Being Private in the Surveillance Society -

The concept of privacy in the age of terror, CCTV and electronic surveillance

Glen Thesslin

SOA 3902

A dissertation submitted in partial fulfilment for the degree:
Master in Human Rights Practice

School of Global Studies, University of Gothenburg
School of Business and Social Sciences, Roehampton University
Department of Archaeology and Social Anthropology, University of Tromsø

Spring 2011

Declaration form:

The work I have submitted is my own effort. I certify that all the material in the Dissertation which is not my own work, has been identified and acknowledged. No materials are included for which a degree has been previously conferred upon me.

Signed: Glen Thesslin ***Date:*** 29/05/2011

Acknowledgements:

I would like to thank my supervisor, Jorun Bræck Ramstad, for her enthusiasm, help and patience!

I am also extremely grateful to my family who have supported me throughout all my studies!

And finally I would like to express my gratitude to my classmates who made these past years as great as they were!

Abstract:

Defending the right to privacy is a growing concern in modern society as surveillance, as a formidable weapon in the "war on terror", becomes more intrusive with every passing year. In order to effectively defend the right to privacy one must know what privacy actually is. Privacy does not have one universal definition, but is a concept that has evolved though varied socio-cultural and historical circumstances, and is constantly being re-contextualised.

This paper aims to discuss and compare various conceptions of privacy, and the right to privacy, with a focus on challenges brought about by technological developments and surveillance. In addition it aims to analyse the implications of surveillance on the right to privacy, with a particular emphasis on video surveillance. In order to reach these goals the paper compares and discusses various academic conceptualisations of privacy, and analyses the discourse surrounding two examples of video surveillance, CCTV coverage of London and the use of covert video surveillance against Arne Treholt, a former bureau chief of the Norwegian Ministry of Foreign Affairs.

Many varied aspects of privacy are considered, with emphasis placed onto two distinct conceptions of privacy; an inherent-value based conception which views privacy as a goal in itself, which is necessary for full human development, and an exchange based conception which views privacy in terms of an exchange, where personal data is disclosed in return for societal goods and benefits. Privacy is conceived as the control of one's own personal data at the most basic level, while surveillance is the process of recording private data; they are antagonistic contradictions.

Using the examples, the paper attempts to reconcile surveillance with privacy; an exchange conception of privacy can accept derogations to the right to privacy in return for more security, although only if based upon a *fair* exchange, something the video surveillance regimes in the example likely do not provide.

The paper concludes with some policy recommendations regarding increased regulation and transparency of surveillance.

Table of contents:

"They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety"

- Benjamin Franklin

1. Introduction:

1.1 *Background:*

The right to privacy is regarded as one of the fundamental human rights as set forth in article 12 of the Universal Declaration of Human Rights (UDHR) and set forth as international law in article 17 of the International Covenant on Civil and Political Rights (CCPR). The understanding of privacy as a distinct right, outwith the public domain, has evolved over a long period of time and has historically encompassed different realms of human interaction and activity throughout different time periods and cultures (Magi 2011, Kasper 2005). Even today the conception of privacy, and congruently also what the right to privacy protects, is neither clear nor taken for granted, and is constantly changing over time and in response to various developments and shifts of technology, and national or international politics.

The conception of privacy not only as an aspect of human life but as a human *right,* pinpoints the importance of protecting that right from *violations*, invasion of privacy is not simply an inconvenience but an important human rights issue. In modern society there are daily many violations of the right to privacy, which civil rights defenders must confront and take into consideration. This thesis aims to contribute to this field and discuss the implications of certain violations to the right to privacy. Due to limitations of scope this thesis will delimit its investigations to the field of surveillance, specifically that of video surveillance.

Surveillance is an increasingly debated topic, coming to the forefront over recent years due in part to the "War on Terror" and the increasingly important role that surveillance plays in security since the events of September the 11th 2001, and partly due to the development of more sophisticated and integrated database and information gathering technology. In addition, many countries have recently altered or added legislation lending increased scope to surveillance, both with regards to the amount of surveillance available to security agencies and the intrusiveness of said surveillance in the post 9/11 era.

Surveillance is in a perpetual state of antagonistic contradiction to the right to privacy, as it necessarily involves an invasion and violation of the right to privacy. But most commentators argue that surveillance is necessary in many different aspects of societal life, be it health care, security against crime or terrorism or even in order to improve customer service (references). Therefore the extent to which surveillance is to be allowed or regulated in society is a current and important, although often controversial, topic. This debate is further complicated by different understandings and conceptualisations of what privacy is, and to what extent it is acceptable to derogate from the right to privacy in exchange for other societal goods.

As such the issue of surveillance and its effect on the right to privacy is an important and current issue, which certainly warrants a deeper investigation. In order to achieve this, the thesis will look at two different cases where video surveillance has been used for the benefit, or protection of public security and what consequences this has for the privacy of the people under surveillance. It will also analyse the media coverage of said surveillance to understand how people and the press react to, and conceptualise such surveillance and the right to privacy in the given cases. The first case is the use of Closed Circuit Television (CCTV) by the authorities in London, arguably one of the sites under most surveillance in the world, to prevent crime and terrorism with particular focus given to the post 9/11 period. The second is the covert video surveillance use against Arne Treholt during the 1980s by the Norwegian . This covert video surveillance was of his house as part of their evidence gathering activities while he was under suspicion of treason. The use of covert video surveillance was kept secret until it was finally revealed in September 2010 leading to cries of outrage from Arne Treholt's wife of the time, Kari Storækre, who had also been monitored despite not being under suspicion (Giertsen 2010).

These cases are appropriate to exemplify the contentious issues at hand as they represent two separate current debates on the violation of the right to privacy, and the appropriate use of video surveillance in the aid of security. They are also examples of different techniques; broad based surveillance on the one hand, and covert, targeted surveillance on the other. In both cases the surveillance is used to aid the authorities in providing security and in both cases involves the surveillance of innocents in addition to the suspects. They have also led to extensive media coverage of the cases in recent years.

1.2 *The aim of the thesis*:

The aim of this thesis is as follows:

To Discuss and compare different conceptions of privacy and the right to privacy, with a focus on challenges brought about by developments in technology and surveillance.

To analyse the implications of surveillance for the right to privacy, particularly with regards to video surveillance.

1.3 *Chapter overview*:

The following chapter will provide a brief overview of the methodology used. Chapter 3 will present a discussion and comparison of different theoretical approaches to the concept of privacy. This will then be followed by a general discussion on the concept of surveillance and its effects on the right to privacy. Chapter 4 presents the two cases of video surveillance in more detail and discusses the media coverage and conceptualisations of the right to privacy versus security in regards to the cases. In Chapter 5 the cases will be discussed in relation to existing academic conceptualisations and theories on privacy and surveillance. Finally Chapter 6 will conclude the paper with a brief overview of the thesis' findings and present the recommendations of the paper.

2: Methodology

In order to achieve its goals this paper will primarily make use of two distinct methodologies; that of a comparative perspective and that of critical discourse analysis. This chapter will discuss the methodological approach used in this paper.

2.1. Discourse analysis as a theoretical context:

The research will use Fairclough's critical discourse analysis, not only as a method to reach its goals, but also as a theoretical perspective on which to base its research (Fairclough 2001). Fairclough's perspective stems from the idea that language is an integral and influential part of social life. Social life itself is composed of interconnected networks of various social practices such as economic, political and cultural practices. These practices constitute a structure within which there is "a relatively permanent way of acting socially" (Fairclough 2001:122), creating a domain of social interaction which reproduces the existing social structures, while having the ability to alter them. Each social practice is comprised of several different elements, such as social relations, social identities, cultural values and semiosis, a concept that includes "all forms of meaning making – visual images, body language, as well as language" (Fairclough 2001:122). All of which are related to each other dialectically, internalising aspects of the others while retaining their individual properties. Critical discourse analysis views semiosis as one of the more significant aspects of social interaction, and therefore focuses on it. In social practices semiosis is used as a tool but also as contextualisation, as it is used to represent the practices both through social construction of other practices, and through self-reflexive construction. In other words the terms used to define a social practice that in turn helps shape the understanding of said practice (Fairclough 2001). Discourses are the representations of social life, which are several diverse practices functioning together. When discourses are networked together they produce a social order, which in turn constitutes a dominant discourse (Fairclough 2001).

Discourses, dominant or not, colour people's conceptions of reality through their use of language, and through the analysis of language one can understand one's reality; how and why it changes in given circumstances. This research is operating on the assumption that the definitions and conceptions of different terms are not constant but are in fact fluid and changing, such as the term privacy. The paper is based on a theoretical perspective where the use of language defines our understanding of society and reality.

2.2. Discourse analysis methodology:

The research will attempt to analyse and reflect over the social problem of derogations to the right of privacy caused by surveillance, in particular, video surveillance. Particular emphasis will be placed upon discourses, which emphasise the link between security-based surveillance and the right to privacy, especially in relation to the "war against terror".

In order to analyse this issue of security-based derogations of the right to privacy, and identify the obstacles to said right, the research will use relevant academic and non-academic texts to analyse the major violations and concerns within the discourse. The research will not analyse the entire semiosis of the social order as described by Fairclough (2001), but due to scope will instead focus on the language aspects. That is; how language is used to shape the discourse and rank the aspects that are important to the different actors, and in what specific ways the language is used in relation to the issue.

To this end the research will first discuss the academic and theoretical literature on surveillance and the right to privacy, in search of various conceptualisations of the concepts "privacy" and "surveillance". This will enable the research to extrapolate some common issues and concerns over the violation of the right to privacy by surveillance. Note that this research is operating on the assumption that definitions and conceptualisations of important terms are neither constant nor universal, but change and evolve over time. Therefore it is not unlikely to find contradicting conceptions of the same idea. Since these conceptualisations inform our perceptions of reality, it is important to be aware of them.

In addition to analysing academic texts, the research will analyse modern media coverage of two examples of video surveillance. They will be analysed for their use of certain keyword expressions and how they relate to the discourse. From this data, it should be possible to determine which definitions and conceptions of the right to privacy, and surveillance, are used by the various actors in the debate. Some examples of these keywords are "security", "privacy", "protection", "fear" and "civil liberty". The research will investigate the occurrence of these and similar keywords, not only for their quantitative use but also for their qualitative properties, to discern if the framing of the terms, and thereby their meanings change depending on the actors involved, their goals or on external events such as 9/11, and if so, how this can take place. Specifically it will attempt to analyse how these keywords and terms dialectically are shaped by, and shape, the various conceptions of privacy and surveillance.

Step 3 of Fairclough's (2001:125) critical discourse analysis urges the researcher to consider if the social order or network of social practices needs the social problem to survive, the social problem in this paper is of course violations of the right to privacy caused by surveillance. While step 4 urges the researcher to suggest solutions to the social problem. This stems from Fairclough's assertion that critical discourse analysis is not purely a method for analysing society, but a theory that plays "an advocatory role" (Meyer 2001: 15), something that falls well within the proposed scope of this paper. As such the issues brought up in Fairclough's step 3 and 4 shall be discussed in chapter 6.

2.3. Comparative perspective:

This research paper will use a comparative perspective on two separate instances; the first of these being the theoretical discussion of previously existing conceptions of the right to privacy and surveillance within academic literature. By comparing the different conceptions, the research will be able to illustrate the subjective and evolving nature of the right to privacy, and highlight basic understanding of surveillance and how this is perceived in light of the unique challenges posed by the "war on terror". The second instance is a discussion on two separate illustrative examples, in which video surveillance has been used in order to promote public security and safety. In each example the research will discuss the media discourse surrounding the intrusive aspects of the surveillance and the concept of privacy. These will then be compared and contrasted to each other in order to determine which concerns and issues are common in relation to the right to privacy and surveillance, which are more contentious, and which are lent most weight. Finally the research will compare the arguments and issues surrounding the examples of video surveillance, with the previously established theoretical conceptions and issues, in order to extrapolate the implications of modern video surveillance on the right to privacy.

As such it is important to choose useful and meaningful examples and instances for comparison, there must be solid reasoning behind the choice and the comparison must be able to add something to the research. In order to reach such goals the research needs to determine several points to be used in comparison; the examples need to be similar enough to enable a proper comparison, while dissimilar enough that comparison provides fruitful insights into the issues at hand. In addition there will be a limitation of scope, as there are far too many aspects that could be investigated; such as electronic interception, full body scanners at airports, covert video surveillance or CCTV cameras on the streets or public transport. This research will be focused primarily on a specific aspect of surveillance. It is important to note that despite this, the research will still discuss the theoretical

aspects of several varying types of surveillance due to their interconnected nature.
The research will also attempt to compare the *qualitative* aspects of surveillance, focusing on technological advancements such as so called "data mining", or face recognition technology, which is replacing human monitoring of surveillance data with computer monitoring, in effect becoming more invasive and comprehensive (Galison and Minow 2006). The research will compare the use of such measures both between countries and between variants of video surveillance, in order to attempt to determine if there has been a qualitative increase in the intrusiveness of surveillance.

Comparing data from two separate countries and conducting a cross-cultural comparison is advantageous to the research, as one can more easily confirm the general applicability of the theories and results reached, if there are similar trends and outcomes visible in both countries. This cross-country comparison could also be applied to the discussion on the concerns and issues that surround the concept of the right to privacy, and that of surveillance, in addition to the obstacles to promoting civil liberty.

2.4 Scope and limitations of comparison:
Due to limitations of scope, the research will focus on one aspect of surveillance in particular, that of video surveillance. This has been chosen both because of the the controversial nature of such surveillance, and the fact that video surveillance has been used extensively in fighting crime and terrorism for many years and in many countries; for example, the current CCTV surveillance regime in the UK has been in operation since 1998, (Gill and Spriggs 2005). It is also an important part of modern counter-terror policies, thus making it useful for discussing the effects of the war on terror on the right to privacy (BBC 2010, 20/07).

The paper will limit the comparison of examples to two distinct instances; using CCTV coverage in London as one of the examples, and the covert video surveillance of Arne Treholt in the 1980s by Norwegian security police as the other. It will pay particular attention to the subsequent debate that erupted in the Norwegian media in 2010, after the covert surveillance became publicly known. These examples were chosen due to their similarities and distinct differences. Both examples use video surveillance in order to maintain and protect national security; both countries' video surveillance practices are controversial, sparking heated debates. These debates both discuss the issue of surveillance of "innocent" members of the public alongside the suspects. The scale of the surveillance is quite different however, UK CCTV is a broad based surveillance that watches practically everyone who passes through London, while the Treholt example is a targeted covert

surveillance operation. The research proposes that the comparison of the UK and Norway, is beneficial to the research as they are countries with similar western and yet distinct cultures which have historically cooperated in security matters, through NATO, and faced the same apparent problems of balancing security and civil liberties. This cross-cultural comparison will aid in reducing the risk of drawing conclusions that appear to be general, but are in reality culturally contextual (Bryman 2008). The research has chosen not be compare other countries' video surveillance due to limitations of space, comparing more examples would lead to overly diluted research.

The results of these comparisons will finally be used to determine what effects the "war on terror" has had on the right of privacy, i.e. whether the concept of privacy has altered in such a way as to encompass less of an individual's life, or if the concerns of national security have led to an acceptance of increased derogations of the right to privacy.

3. Theoretical background of privacy and surveillance:

3.1. Conceptualisation of Privacy:

Included in the UDHR at its adoption in 1948, is the right to privacy, a right later enshrined in international law as article 17 of the CCPR. The conception of privacy as a right, which requires protection from violations, is an important development in human rights history. But the understanding of the definition and meaning of privacy has varied over time and place (Magi 2011, Rosen 2000, Posner 2008). The following section will give a brief overview of the major conceptions of privacy.

The concept of privacy as an individual right was arguably first discussed as a legal issue in the 18th century with private property forming the basis of the right, as exemplified by the US constitution (Rosen 2000). This concept has since then evolved due to technological challenges and changing perspectives on human psychology, rights and philosophy (Magi 2011). One of the first defences of privacy, in the face of its vulnerability to technological change, came in the 1890 article by Louis D. Brandeis and Samuel D. Warren. In this article they discussed the threat posed by the technological advancements in "instantaneous photographs and newspaper enterprise" (quoted in Rosen 2000: 34), which could erode the right to privacy, conceptualised by them as the right "to be let alone" (Quoted in Magi 2011: 189). Such debates over the effects and threats of technology to the right to privacy have only increased in intensity since the seminal 1890 article, gaining further weight with the advent of the "information age", in which our daily lives involve constant interaction with computers and computerised databases. Modern technology has made it possible to collect and analyse enough data to "amount to a picture of your life so complete it's equivalent to somebody following you around all day with a video camera" (Baer quoted in Galison and Minow 2006: 263).

The existing literature on privacy is considerable and broad in scope, covering many different academic fields and focusing on many varied aspects and violations of privacy. There is a spirited debate on how this right may have derived from the other pre-existing rights, such as the right of ownership and the right not to be harmed, or as a unique right inherent to the human condition, (Magi 2011). This paper understands the right to privacy to be a fundamental human right, which has value in and of itself but is also closely linked to other human rights, and acts to a certain extent as an enabling right.

Part of the reason why privacy is such a debated concept stems from the fact that it is "both a

normative and a descriptive notion" (Manning 1997: 820). As such it is quite clear that there is no universal definition of privacy, instead different conceptions emphasise different aspects of human life as private, meaning that a violation of the right to privacy within one definition could be perfectly acceptable in another, depending on how the right is derived (Introna and Pouloudi 1999, Magi 2011). In addition to different academic interpretations of privacy, there is also a documented socio-historic variation of the concept of privacy, which further confuses attempts at defining it. For example, rules limiting entry to houses or to what extent it is acceptable to touch other individuals, vary from country to country. Despite the different cultural conceptions, all cultures have an inherent need for a modicum of individual and group privacy and the norms necessary are present in all cultures, although the norms themselves do vary (Kasper 2005, Magi 2011).

While many theorists attempt to reduce privacy to a single concept, other theorists argue that in today's complex society such simple definitions are too vague to be of use, or are not comprehensive enough to be applicable or easily defended (Magi 2011). Conceptions of privacy that are too vague hamper the defence of privacy, as courts and policy makers "cannot easily articulate the privacy harm" that must be protected against.

Some modern privacy debates have sought instead to outline various distinct aspects of privacy and important similarities, which can then combine as an interlinked whole with privacy as a "shorthand umbrella term for a related web of issues" (Magi 2011: 190). Manning (1997), for example, points out that many a liberal commentator's definition of the right to privacy can be broadly split into two major categories of violations; violations of the right to liberty, and restrictions on a person's development. Interestingly this mimics the debate on how the right to privacy is derived. In the former category privacy is simply a derivative of the more important right to liberty while in the second category the right to privacy has a value in itself as part of a person's development.

Some theorists point out how important privacy is in relation to personal development, maturity and interpersonal relations. To be able to form individual opinions and thought, it is necessary to be able to withdraw from the public sphere to reflect; without some modicum of privacy to reflect individually, society would be entirely homogeneous (Magi 2011). Rosen (2000) argues that in order to create an intimate relationship an individual must be able to gradually and privately reveal their thoughts and feelings, something that would be impossible without a protected private sphere.

While traditional privacy conceptions were based upon a physical conception of one's home and

property, such definitions cannot account for the issues raised through the technological advances of the information age. Instead many theorists emphasise that privacy does not solely relate to the physical aspects or the development of a person, but includes the right to control one's personal data; who has access to it and to what ends it may be used (Rosen 2000, Posner 2008, Introna and Pouloudi 1999). Posner emphasises the aspect of secrecy in relation to personal information. As such he distinguishes between a person's "pure" interest in secrecy and their "instrumental" interest. That is; they fear that the information could be used against them and wish to protect themselves from it. For example a person may not wish to be photographed naked from a pure perspective or may wish to avoid blackmail from an instrumental perspective (Posner 2008: 245). This secrecy is not limited to personal information but includes protected communications. Rosen claims that simply terming privacy as secrecy is an oversimplification, as the concept of privacy includes "the ability to control the conditions under which personal information is disclosed to others (Rosen 2000: 36). Although Posner does not explicitly state that such control falls under the concept of Privacy. His discussion of voluntary disclosure of personal information in order to receive a credit card, driver's license or similar benefits as an issue of privacy, implies that he is in agreement. He further argues that although individuals do care about personal secrecy, they willingly share personal information "at the drop of a hat" creating an odd dialectic between personal benefit and privacy (Posner 2008: 251). It is important to note that Posner's emphasis on instrumental secrecy as a form of concealment has been challenged as presupposing a common and universal value base (Introna and Pouloudi 1999).

Ashworth and Free (2006) focus on online privacy, and describe privacy as an exchange between consumers who freely disclose their personal information in exchange for goods or benefits from firms, although one could apply such a concept to different actors within society, such as between an individual and the government. An example of such an exchange would be giving one's name and address in exchange for the use of an email address, or the opening of a bank account. This exchange theory can complement Posner's conception of voluntary information disclosure and vice versa.

Introna and Pouloudi (1999) argue that since privacy is socially and culturally defined we cannot find any single example of something that is considered private in all cultures. Instead we must focus on a common feature of all privacy conceptions; that individuals wish to retain and protect certain aspects of, or information on themselves from the *judgement* of others. This conception of privacy stems from a form of pluralist understanding of human society where each individual's

values are unique and varied, requiring private control of the de- and re-contextualisation of the data, something that is denied without a private sphere. They claim that privacy has an intrinsic value to individuals by enabling their individual values to develop, and reject claims that there are self-evident universally accepted values (Introna and Pouloudi 1999). They point out that data taken out of context by invasions of privacy or the re-purposing of existing data, can lead to "inappropriate judgement of others" (Introna and Pouloudi 1999: 30).

Prosser uses four types of legal issues that threaten the right to privacy, on which to base his conception. These include; intrusions upon an individual's solitude and private affairs, public disclosure of personal facts, publicity placing an individual in a false light and the appropriation of an individuals likeness or identity (Magi 2011). Solove claims this is too rigid and instead raises six distinct but interrelated categories of privacy definitions. His categories include: "(1) the right to be let alone, (2) the ability to limit access to the self by others, (3) secrecy or concealment of certain matters, (4) the ability to control information about oneself, (5) the protection of one's personhood, individuality and dignity and, (6) control over one's intimate relationships or aspects of life." (quoted in Magi 2011: 189).

Due to the diverse nature of the existing conceptions of the right to privacy, which appears to be much more than simply the right to "be let alone", and instead encompasses and touches upon many different aspects of individual life and societal activities, it is most beneficial to base an analysis of privacy under a broad umbrella conception from which one can dialectically define privacy by relating the violations of, and intrusions on the right to privacy, to the different aspects of such a complex right.

3.2.Overview of issues concerning privacy.

Due to privacy's essential role in human society and development, it is especially important to identify and analyse the potential threats and issues that may occur in society. Due to the varied nature of privacy conceptualisations, the issues facing it are diverse and many-faceted.

It can be derived from the notion of "the right to be let alone" that individuals must be allowed the freedom to create private spaces, both mental and physical, in which they can form independent and unique thoughts and opinions, form intimate relations and be able to relax away from the pressures of public life. It is also important to be able to drop the "mask" or role, which they use in public settings (Magi 2011, Rosen 2000). If individual privacy is eroded within a society it is possible that

one may find a decrease in new and independent thoughts among the population. The information age has also facilitated an exponential increase in available information, which some theorists argue has led to a condition of reduced attention spans among society's individuals, meaning the interpretation of information has been reduced to simply processing sound-bytes. This can lead to more information being taken out of context or misinterpreted (Rosen 2000, Magi 2011).

It is also important to note that an encroachment of the right to privacy could have negative effects on freedom of expression, as the speech and actions of the individual naturally alter if the individual knows he or she is under third party scrutiny, they become more guarded and less spontaneous (Rosen 2000). One could argue, based on this, that surveillance may lead to a more forced and unnatural social interaction in society. It could be argued that the above issues are various forms of "pure" concern for privacy.

The development of information technology and the possibilities it provides for handling and retaining personal information, has led to one of the more complicated privacy issues facing modern society. Modern databases of personal data are used in a variety of fields, from medicine to travel and financial records (Bayer and Fairchild 2000, Haggerty and Gazso 2005). In many cases, such as that of name based surveillance in epidemiological studies, privacy concerns have become more prominent in recent years, predominantly in response to the risk of social stigma should the information gathered by surveillance be revealed. This reflects a growing concern about the use and storage of personal data in modern databases and can be regarded as a form of "instrumental" concern (Bayer and Fairchild 2000, Vleck 2008, Posner 2008). Some databases try to counter this by pledging to keep the data secure and retain it only for the purpose stated, but such pledges are not always believed or adhered to (Bayer and Fairchild 2000). In addition, as electronic data can be more easily retained and accessed than earlier paper records, it is also more easily misappropriated or re-purposed. A recent example is the hacking of PSN (PlayStation Network) (BBC 2011, 07/03).

Given a conception of privacy in terms of exchange, Ashworth and Free (2006) point out two major issues; (1) consumer awareness of information gathering, often consumers will be less concerned about privacy if they are aware of the surveillance and have given permission for it. This is less a contentious issue, rather a way for information gatherers to avoid privacy concerns. The focus here is on a consumer agency releasing their control over their private information. (2) concerns over how the data is used. In many cases information gathered under a particular pretence, such as email addresses for an Internet service, can be sold to other companies for advertising purposes or can be

misappropriated in order to commit fraud (Ashworth and Free 2006).

Ashworth and Free (2006) use theories of justice and fairness judgements to address the concerns regarding how *fair* an exchange is. They claim that individuals will look to both distributive justice and procedural justice in order to judge their exchanges. Comparing the value of the information disclosed to the value of the services or goods gained, will provide the consumer with an understanding of the material fairness of the exchange. In the procedural justice aspect of the judgement, consumers compare the method of the exchange to "normative standards of respectful behaviour" (Ashworth and Free 2006: 115). In relation to information gathering these norms can be; the expectation of a firm's openness about what data is gathered and why, or whether permission is requested beforehand. In many ways the main concern is the "possibility of negative outcomes resulting from the exchange" (Ashworth and Free 2006: 111). With so much data collected in today's databases it is increasingly difficult to regulate how this data is used.

Rosen (2000) argues, using the US as an example, that people are becoming at once both more concerned about privacy and also increasingly exhibitionist, primarily in regards to the Internet in the form of blogs, webcasts and social networking sites such as Facebook or Twitter. One could explain this as a form of voluntary disclosure of information, which could be regarded as given in exchange for fame or online social interaction.

This brief overview of issues concerning the right to privacy, shows that most violations appear to fall into four broad categories. Physical violations of privacy; invasions of the home or person. Intellectual violations; the erosion of an individual's ability to form independent thought and have his or her freedom of expression. Informational violations; the control of one's personal and private information. And finally relational; the ability to form intimate personal relations.

It is interesting to note that most modern theorists focus on non-physical privacy issues, most likely as a reaction to the challenges posed by developments in modern information technology, while they appear to have taken physical privacy for granted and view it as uncontroversial.

3.3. Surveillance and privacy:

Loss of privacy occurs when "others obtain information about an individual, pay attention to him, or gain access to him" (Gavison quoted in Introna and Pouloudi 1999: 29), as such, surveillance can be conceived as the antithesis of privacy and yet surveillance is prominent in almost every aspect of

society. In order to investigate this, one must first briefly investigate what surveillance is and how it is used.

Since the terrorist attacks on September the 11th 2001, several countries have constructed "an intensive surveillance structure" as a major aspect of their counter-terror policies (Haggerty and Gozso 2005: 170). The surveillance employed by said policies includes, but is not limited to, "sensors, bureaucratic documentation, x-rays, satellites, and computerized databases". Surveillance is not limited to purely security usage but is utilised by a myriad of actors including private firms and non-security government agencies. The purposes of such surveillance are as diverse as its methods, encompassing among others; improved governance, profit maximisation, entertainment, health services and security (Haggerty and Gozso 2005, Bayer and Fairchild 2000). The focus of this thesis will be on CCTV surveillance as an aspect of security policies, although a discussion of other surveillance techniques is necessary as modern surveillance is often an interconnected system.

Despite a number of commentators emphasising surveillance as an aspect of the war on terror, many of the techniques used are in fact developments of older surveillance practices, such as financial surveillance used in the war on drugs. What has changed in the post 9/11 era, is the scope and intensity, surveillance is now a much larger focus of security policies and more apparent in society (Vlcek 2008).

Posner (2008) illustrates that private communications are valuable, as much to innocent civilians as to criminals and terrorists, and that a broad-based surveillance of communications or public spaces would lead to criminals and terrorists having their communications or public activities curtailed. This is an important goal for security policy and he argues that surveillance, in coordination with modern data collection and analysis, is an important tool in the fight against terror. For example data mining, that is software which picks out certain aspects within the data such as particular words within communications or irregular travelling patterns, enables security agencies to sort through the frankly enormous piles of data that surveillance can create, in order to identify only the cases that interest the surveillance operators. This can be applied to both the monitoring of communications and travel records, or as an analysis of CCTV data.

A side effect of similar broad surveillance techniques, which target entire populations, could be a reduction of the free idea exchange among the innocents who are aware they are under surveillance. Posner (2008) claims that this is a small cost in relation to the resultant effects on security. Vlcek

(2008) argues that the increased scope and intensity of surveillance measures is in fact counter-productive to security concerns, as the sheer amount of data only further conceals terrorist activities. He points out that while data mining technology can aid security operatives in sifting through the data, it also creates far too many "false positives". That is a data positive, flagged as suspicious by the software, which upon further investigation turns out to be false. This would lead to an increased violation of the innocent individual's right to privacy, as security operatives investigate them without gaining any benefit in security terms. Instead Vleck argues that surveillance could be based upon individual cases where suspicion already exists, something Posner rejects. Warrant based or similar surveillance, which can only target people already under suspicion, cannot find unknown criminals or terrorists. He agrees that while broad based surveillance can cause "false positives" it is infinitely preferable to any "false negatives" that warrant based surveillance could cause. Thus restricting the surveillance to the extent it cannot find hidden terrorists and terrorist plots, as happened in the run up to 9/11. (Posner 2008)

There is an often Hobbesian reasoning behind modern day state surveillance; people will accept certain derogations of their right to privacy by the "state leviathan" in exchange for the protection it can offer (Vlcek 2008: 23). One can argue that it is part of the social contract between the state and the people or that it is a conscious exchange of individual privacy for increased security. This conception of the right to privacy as an antagonistic contradiction to security, and terming the balance between the two as an exchange, is common among many commentators on surveillance and security. As such the debate is often focused on how much privacy we can actually afford to give up in the name of security, and rather less on whether we need to give up privacy (Posner 2008, Bayer and Fairchild 2000, Haggerty and Gozso 2005).

A major aspect of modern surveillance is the process of previously disparate databases becoming increasingly interconnected due to digitalisation, previously innocuous information can now be combined into a rather complete picture of a persons life (Posner 2008, Introna and Pouloudi 1999). Haggerty and Gozso (2005: 172) define this as a "surveillant assemblage", which is characterised not as a single system but as a *potentiality.* The assemblage consists of a decentralised group of distinct databases, which can potentially be combined into a centralised search. State actors often incorporate this assemblage in their surveillance operations, to take advantage of the "surveillance and informational capacities of ostensibly non-state organisations" (Haggerty and Gozso 2005: 174). This is a growing trend where many non-state or police actors are being urged to or legally required to increase surveillance, for example bank tellers becoming in effect "little brothers"

(Vlcek 2008). Another concern raised by the use of modern databases is the fact that such information can be retained almost indefinitely (Monmonier 2002), there is a threat that data collected for a given purpose is retained and available long after it has served it's initial purpose.

Since not only the data is retained but the surveillance regimes themselves, once implemented, are difficult to remove, the issue that "surveillance regimes instituted and justified for one purpose now rapidly assume other uses" (Haggerty and Gozso 2005: 170) is quickly pressing to the forefront of the debate. Vlcek (2008) points out that some surveillance originally created to combat terrorism has since been used against "garden-variety" crime, highlighting the possible negative ramifications of implementing an extensive and invasive surveillance regime. Posner (2008) explains that trust is an important aspect for successful surveillance regimes, and can counter privacy concerns. If the public trust the security agencies to be professional and impartial with the data, including in what way the data is used and that it will not find its way into other databases or be otherwise misappropriated, then they would be more likely to accept intrusive surveillance. It is similar to people being willing to disrobe in front of a doctor, as they believe that a doctor's interest is purely professional. It is important to note that such reasoning only addresses individual's instrumental interests in privacy, but cannot satisfy their pure concerns.

A similar instrumental justification for broad-based surveillance is that invasions of privacy should not be of concern to the general law abiding public and should only be of concern to criminals and terrorists. It can be argued however, that this is based on a basic conception of privacy as the right to be "let alone" and as such does not take into account any inherent values of privacy that can be found in other conceptions of privacy (Vlcek 2008).

An interesting aspect of surveillance is that it can, in some cases, be self-replicating, CCTV is a good example; if a certain neighbourhood has a high CCTV camera coverage then residents in other surrounding neighbourhoods often feel less secure and call for CCTV coverage of their own area. Haggerty and Gozso (2005) claim that this would not necessarily help security but simply displace crime and terror threats. It is also unlikely to lead to an, in their opinion, re-evaluation of how we understand surveillance, but simply lead to calls for more surveillance.

There is a general acceptance of the necessity of surveillance in modern society and there are several different approaches that attempt to reconcile surveillance with the right to privacy. These approaches are then employed as a measuring stick or filter when discussing how and when

surveillance can be used. The argument that surveillance should only be a concern if one has something to hide, justifies surveillance in terms of the benefits it brings to society, and a conception of privacy as non-interference. CCTV, for example, intrudes on personal interactions and can be used to compile data about an individual's location and their habits, information that is necessary for observers to piece together a meaningful picture (Monmonier 2002). The above conception would argue that this does not pose a problem to the right to privacy per se, but the conception rejects notions of the inherent value of privacy and it's necessity to human development. In effect it does not consider broad surveillance such as CCTV coverage, which can be so complete that it is in essence impossible to function in modern society and avoid being under surveillance, as violating the right to privacy (Vlcek 2008, Posner 2008). Other commentators argue that surveillance inherently reduces an individual's worth, changing them into objects, not people. The knowledge that we are under surveillance changes the way we act and takes away our personal spaces in which we can form private thoughts and opinions (Ashworth and Free 2006).

Ashworth and Free's (2006) approach to surveillance and privacy uses the conceptualisation of privacy as a good that can be exchanged in return for societal goods or benefits, such as increased security. This conception would allow derogations of the right to privacy as one end of an exchange. Their conception provides a format in which one can analyse the costs and benefits of such an exchange through fairness judgements. This is only applicable in cases where the judgements are made in situations where access to the relevant information is available and trustworthy. The consumers, the populace who will be under surveillance, must know to what ends their personal data will be used and be able to trust it will not be re-purposed. Data aggregation is quickly becoming a growing threat by collecting innocuous data and compiling it for purposes other than those originally intended (Magi 2011).

The focus of such an exchange is on an individual level and presupposes a degree of agency. Can it truly be said that every individual in society has agreed to an exchange of personal information, in return for increased security with regards to broad based surveillance? CCTV coverage can be so comprehensive that it is essentially impossible to avoid while participating in modern society, thus representing an *involuntary surveillance* (Posner 2008). One could argue that individuals who have not voluntarily agreed to the surveillance are in fact having their right to privacy violated. It is difficult to justify covert surveillance in terms of an the exchange approach, since the inherent secrecy of covert surveillance implies that the individuals involved are not aware of their disclosure of personal data and as such have not agreed to the exchange, no matter what benefits they receive.

Ashworth and Free (2006) point to the secret selling or transfer, for other purposes, of data given in a particular setting, as one of the major barriers to fair exchange judgements. Social contract theorists may argue that the acceptance of any derogations or violations of the right to privacy, was implicit in a member's participation in society, but such reasoning is valid only together with an acceptance of social contract theory.

Many commentators, who accept that a certain amount of derogation of the right to privacy must take place in order to increase security, are in disagreement over how much focus should be put on security. An important aspect of surveillance regimes is that the mechanics are difficult to remove once in place. If the immediate terror threat and the fear it brings, which causes populations to place more weight on security than privacy, passes, it may no longer be necessary but may still exist. This is equally applicable to data, since modern information technology can retain data more or less indefinitely (Vlcek 2008, Haggerty and Gozso 2005). Repurposing of surveillance regimes and databases is certainly one of the greatest privacy concerns in modern society. The question then becomes "Quis custodiet ipsos custodes?" or "who guards the guardians" perhaps better understood as "who guards us *from* the guardians" (Vlcek 2008: 23).

4. Illustrative examples of video surveillance:

This chapter will give a brief overview of two examples where video surveillance has been implemented in order to strengthen national security; the first instance is the usage of CCTV cameras by council or police authorities in London, the second instance is the usage of covert video surveillance in the Arne Treholt case by Norwegian PST (Politiets Sikkerhetstjeneste, or the Police Security Service[1]). Following each overview, the chapter will continue with a discourse analysis of some of the media coverage surrounding the examples, focusing primarily on the conceptualisations of surveillance and the right to privacy used by the concerned actors. It will also consider the question of how the surveillance is justified in each example.

4.1. CCTV coverage in London:

The UK citizens are often referred to as one of the world's most watched, and London as its most observed city where there are more CCTV cameras per capita than anywhere else in the world, with figures as high as one camera "for every 14 citizens" (David Davis quoted on BBC 2008, 12/06). London is thought to have more than 7000 operative CCTV cameras in total, while the borough of Wandsworth alone has over 1000 cameras, the latter representing more CCTV coverage than Dublin, San Francisco, Johannesburg and Boston combined (BBC 2009, 20/07). CCTV coverage has, since the 1960s, become a major aspect of UK counter-terror policies, especially after the London bombings on the 7th of July 2005. The number of cameras in use continues to mount as police and councils rely more and more on video surveillance (BBC 2010, 11/05).

CCTV coverage can be said to have two different, but interlinked purposes; that of fighting terror, and that of fighting crime, and has a history of both since the 1960s (BBC 2006, 3/11). Although there are many instances where CCTV has been instrumental in solving or preventing crime, other statistics have led to increased concerns over the effectiveness of CCTV. Statistics such as "Fewer than one crime in 30 is solved through CCTV" (McSmith 2008) or "1,000 cameras solve one crime"' (BBC 2009, 24/08) have added to the anti-CCTV debate. Concerns over what other possible purposes are served by CCTV coverage are strengthened by cases of city councils using CCTV to monitor parking violations or firms allowing private persons access to CCTV coverage of public areas, have added another dimension to the debate (BBC 2011, 20/01, Allen 2006).

1 Known as POT at the time of his arrest.

4.2. Discourse analysis regarding CCTV coverage in London:

There is a huge amount of media interest regarding the use of CCTV in London, within which one can find a varied berth of perspectives ranging from journalistic reports on the statistical implications of CCTV surveillance, to quotes from politicians and privacy activists, to opinion columnists. The discourse is split between those in favour of a more comprehensive CCTV system and those that oppose it, each side of the discourse have their own arguments and language to convey their messages. The paper will present and discuss these arguments and its language.

Proponents of a comprehensive CCTV surveillance system often use arguments focused on the benefits of surveillance, generally in regards to security or safety. Both politicians and the general media remark upon how CCTV coverage has played a prominent role against terrorist threats in London, especially when discussing the role it played in the investigation of the London bombings of 2005. (BBC 2010, 11/05). Karl Powell, a Westminster city council member, explained that increased CCTV capacity, while not the ultimate solution to crime and terror, was "a very powerful tool which we are able to link to our other anti-crime initiatives." (BBC 2002 18/09). However it is not only policy makers who discuss privacy and surveillance in terms of security or safety, many local residents are also in favour of video surveillance. In Shoreditch, for example, a novel programme has been initiated, where CCTV cameras are connected directly to the television channels of local residents, in order for them to monitor their neighbourhood and alert the police if they observe anything suspicious. Local residents have been quoted as saying that CCTV; "will mean they feel a lot safer" (Allen 2006). Privacy campaigners have condemned such moves as promoting fear and suspicion in society, and have raised concerns regarding vigilantism (BBC 2006, 10/01, 2009, 18/11).

Hari (2008) argues in favour of the use of CCTV surveillance in a similar form to that of those focused on protecting the right to privacy from intrusion, by focusing on the human rights aspects of the discourse. She points out how the individual liberty of the person can be protected by CCTV surveillance, that by protecting the security and safety of an individual their liberty is preserved and their other rights enabled. This is a notable deviation from most language used in defence of a comprehensive CCTV surveillance regime. She goes on to discuss how anti-CCTV proponents use "bombastic" language to paint CCTV as a totalitarian threat to society, claiming that that is unreasonably diverting the discourse away from the more important issues of how to balance privacy with security. In addition she points out that the cameras are in any case monitoring public spaces and therefore cannot intrude on privacy.

Many privacy defenders, particularly columnists and campaigners, use the term “Orwellian” about the surveillance regime, and compare the state to “Big Brother” from Orwell's dystopian novel when discussing privacy concerns and CCTV surveillance. Of course the use of “Orwellian” does not refer only to video surveillance but it is one of the more prominent aspects of the novel. The use of the term does not appear to imply that the commentators view London and the UK CCTV surveillance regime as totalitarian, more that it has the *potential* to become so. This type of terminology is particularly common in connection with texts discussing increase in surveillance or articles about its ineffectiveness (Goodchild 2007, Walsh 2010, Duffy 1999, BBC 2009, 6/02).

Such terminology is often found when privacy campaigners are questioning whether the benefits of CCTV outweigh the concerns that arise when the surveillance is re-purposed, from its major goals of “security and safety”, to be used instead in combating minor infringements such as parking infringements or dog fouling. The campaigners often paint such re-appropriation of CCTV data in negative terms; such as “policing by remote control” and CCTV or surveillance “creep”, describing how video surveillance is spreading into more areas than originally conceived (BBC 2009, 06/02, 2011, 20/01). Terming CCTV as remote control policing evokes images of machines replacing human interaction, while the idea of CCTV creeping make it seem like an underhand development. Others however view the spread of CCTV surveillance to other fields as a positive development, claiming it will help combat minor infractions, and that most people are reassured by the presence of more CCTV (BBC 2011, 20/01).

Similar emotive language is most common when used by privacy rights campaigners rather than CCTV surveillance defenders, as in expressions such as the UK “committing slow social suicide” through unwittingly allowing such a steady increase in surveillance (Goodchild 2007). This kind of language in particular, mimics concerns by privacy rights theorists who are concerned with the inherent values of privacy. CCTV proponents do of course use emotive language, although it rarely paints such a sombre picture as the above. Instead it is generally focused on the need for security and the abolition of citizen’s fear. But it is worth noting that both proponents for and against CCTV, use arguments based upon fear, in the discourse. Privacy proponents often ascribe requests for extended CCTV surveillance by local residents to a “culture of fear and mistrust driven by a failure on the part of the borough and the police to have proper law enforcement” in the area (Alex Deane quoted in BBC 2009, 18/11). It must be noted that this development is not universally lauded by policy makers and advisers; The Department for Communities and Local Government had asked

councils to ensure their video surveillance was “proportionately” used, the overuse on minor infractions could lead to a loss of trust in CCTV surveillance (BBC 2009, 06/02).

The discourse touches upon the issue of CCTV effectiveness, a particularly complicated issue as there are no conclusive studies of the CCTV's effect on crime rates; the estimates vary from a 95 percent reduction in crime, to solving only 1 in every 1000 crimes (McSmith 2008, BBC 2009, 24/08). There are however two general trends within the discourse; that of promoting CCTV as a valuable tool for the protection of citizens from crime or terror, and that of deriding CCTV as expensive, infective and poorly operated. Police officials have conceded that CCTV operation is not optimal and ought to be improved. But, as opposed to privacy campaigners, they argue that putting more resources into CCTV training and equipment to optimise surveillance is a better option (BBC 2009, 24/08, McSmith 2008). The language used in positive reports on CCTV refers often to the professional and scientific usage of the surveillance regime, and that there is a strong commitment to investing in a functioning surveillance operation. There is also a strong focus in these articles stressing that crime has in fact been reduced (BBC 2010, 26/12). The Mayor of London, Boris Johnson, exemplified this stating; “sustained investment in policing and CCTV - is helping us make significant strides along the road of tackling crime in our city” (BBC 2010, 11/05).

There is one certain similarity between the discussion of opinions on both sides of the discourse; they almost always use lists of examples to strengthen their arguments, either by showing statistics of ineffective CCTV coverage or examples where CCTV has indeed been effective (McSmith 2008, BBC 2009, 24/08, Hari 2008). The debate can be quite heated with both sides of the discursive divide using emotionally charged language, painting pictures of the need for security and safety, or the risks of a bleak Orwellian future that surveillance represents.

One can extrapolate some common arguments from the discourse surrounding CCTV surveillance and the right to privacy; those who are in favour of a comprehensive CCTV surveillance regime tend to use arguments that justify CCTV based derogations on the right to privacy in terms of CCTV's use as an effective tool. A tool that perhaps may need more resources or development, but a necessary one none the less. The issue at hand in these arguments is almost always the increase in security and safety through a decrease in fear.

This argument is often met with arguments regarding the lack of impact CCTV purportedly has on crime and terror. But most of the counter CCTV arguments are derived from the fear of a

surveillance “creep” and of the alternative uses for said surveillance. Even though it is not explicitly mentioned in the media sampled in this paper, one of the major issues is that of trust, can the CCTV operators be trusted?

4.3. Covert video surveillance of Arne Treholt.

Arne Treholt is a former Bureau chief of the Norwegian Ministry of Foreign Affairs, who was arrested by the Norwegian Police Security Service in January 1984 under suspicion of disclosing national secrets to the Soviet Union. He was tried, convicted and served 9 years in prison before being pardoned in 1992 (Kolsrud 2008). Treholt claims he is innocent and has made several appeals to have his conviction overturned, all of which have been rejected.

In 2010 the “Treholt-case” came into media focus yet again as a result of two new revelations. First; claims were made that some of the evidence against Treholt was in fact falsified, and second; it was revealed that Arne Treholt had been under covert surveillance for a year and a half, which included covert video and audio surveillance of his private family residence, a security measure that was illegal under Norwegian law at the time. Understandably this caused quite an outcry in the Norwegian media although not solely due to issues of legality but also on grounds of principles related to the right to privacy. The fact that unbeknownst to her Treholt's wife at the time, Kari Storækre, and their son were by extension also under constant surveillance, was an important aspect of the media coverage. Indeed it has been argued that Storækre and her son should have reparation made to them, and some argue that Treholt should also be compensated. The debate is of interest to this thesis as it illustrates how the right to privacy is conceptualised by media commentators surrounding, and the actors involved in, an actual application of video surveillance. It is particularly interesting to note that these privacy concerns are discussed as an independent question regardless of Treholt's guilt or innocence.

4.4 Discourse analysis regarding covert video surveillance of Arne Treholt:

On the 27th of September 2010 the Lund-commission, a commission that monitors illegal surveillance of Norwegians, confirmed that Arne Treholt had been under illegal covert video surveillance for almost two years until his arrest in 1984. A fact that the commission had previously withheld from the public and the various actors related to the case (Aalbu 2010).

“We could see when Treholt had a nap on the sofa, played with his son in the living room or when

the couple had friends visiting[2]" A former POT surveillance operator describing the extent of the surveillance Jonnassen, Staveland and Gjerde 2010). In fact the surveillance was much more invasive and comprehensive than initially revealed, with the Lund-Commission explaining that they had received reports from the POT stating that there were several more cameras around the house, including inside the bedroom (Gjerde 2011).

There is an overwhelming consensus amongst the media and commentators that the covert surveillance of Arne Treholt and his family was an objectionable action. The discourse rarely seems to contest this assumption, instead there appears to be a split between those commentators who discuss the covert surveillance in terms of the loss, or the abuse, or the violation of the right to privacy, or a persons integrity on the one hand (Giertsen 2010, Aune and Hessevik 2010, Døvik and Granbo 2010), and those who focus on the illegality of the surveillance on the other hand Jonnassen, Staveland and Gjerde 2010, NRK 2010 27/09, Stanghelle 2010).

While the difference may appear to be solely of the semantic kind, it may help shed some light on the conceptions of privacy and surveillance that are dominant in the discourse. Those who contextualise the problematic as a question of rights, obviously see a clear violation of the Treholt family's rights; with many commentators explicitly mentioning that despite any guilt on Treholt's part, the surveillance was most certainly an unacceptable violation of the right to privacy (Giertsen 2010, Døvik and Granbo 2010).

Treholt himself claims that, "This [the surveillance] is pure abuse which has nothing to do with national security" (Aune and Hessevik 2010). The surveillance was solely an invasion of his private sphere, where he and his wife were victims of a "witch-hunt".

The human rights specialist Anine Kierulf, from the University of Oslo, referred to legal norms when discussing the case in relation to the right of privacy. She pointed out in an interview with NRK that the covert video surveillance of Kari Storækre is a clear violation of the EU Charter of Fundamental Rights and Norwegian personal integrity laws, concluding that Storækre should receive some form of compensation for the surveillance (Døvik and Granbo 2010). Similarly Gierstsen (2010) also used legal reasoning to question whether the Lund-commission, who had withheld information about the surveillance from the actors since 1984, should be liable to Treholt and his family.

2 All translations from Norwegian to English by the author of this paper.

Several commentators have questioned the Lund-commission over their apparent willingness to cover up illegal surveillance activities, these include the Justice Minister who asked why the Lund-commission did not come forward with this information earlier, since they had already reported illegal investigations which had been employed during the Treholt case (Aftenposten 2010). The Lund commission has explained their omission of the information, by pointing out that their mandate and focus was on mapping politically motivated registrations and surveillance of Norwegians by Norwegian authorities, while counter-intelligence cases were in the "periphery". (NRK 2010 27/09) This could imply that since the surveillance of Treholt fell under national security, it is not afforded the same protection as politically motivated cases of illegal surveillance, i.e. that national security trumps privacy in this case.

Admittedly there have been no explicit statements using such reasoning, but there does seem to be such a mentality. According to a former POT employee who worked on the Treholt case; the POT were willing to go as far as to falsify evidence to get Treholt convicted for treason, and the POT leader in charge of the surveillance was reported to have said that there are "other rules in play for POT" Jonnassen, Staveland and Gjerde 2010).

Some newspaper commentators pointed out that there appears to have been a mental attitude that POT operatives could get away with anything. This can possibly be observed in the fact that the Lund-commission did not mention to their "employers", the Norwegian Parliament, that illegal surveillance had been used (Stanghelle 2010). It could also be argued that it was simply a case of "the ends justify the means" mentality applied to surveillance and privacy.

In the general discourse the issue of trust is not explicitly mentioned by media or commentators but it is certainly *implied* by the texts. Stanghelle (2010) is an exception and does mention that this could lead to a sense of mistrust regarding PST, the modern version of the POT, and surveillance regimes in general. Interestingly the commentators appear to be unanimous in regarding covert surveillance as objectionable. Some go as far as to argue that the silence of the Lund-commission was in fact a violation of the right to privacy, even though Treholt and his family were no longer under surveillance. Treholt and his family could not take action in response to the surveillance without being aware of it (Giertsen 2010). This is interesting as it implies that privacy has an inherent value that is violated even when the observed are not conscious of the surveillance.

5: Privacy and video surveillance:

5.1. The development of Privacy and Surveillance:

In previous chapters the conception of the right to privacy has proven to be elusive, privacy does not have a set definition, the meaning of the word changes, depending on cultural and historical context. While the meaning changes, so does its effect on society, the way we conceptualise privacy affects what is and what is not an acceptable intrusion on our solitude, life or interests. Privacy is an inherently individual right, it entails a certain withdrawal from society; the individual does not participate in society with the private aspects of their being, while the public society cannot enter nor intrude in these aspects. The private aspects of an individual can be defined in terms of information; at the most basic level we can reduce privacy to the control over an individual's own personal data (Posner 2008, Rosen 2000, Ashworth and Free 2006). How much or how little of a person's data should be under this control, is of course less clear. The threat to privacy is in the collection of data or surveillance. Surveillance and privacy are in an antagonistic contradiction, they cannot co-exist.

Out of the threat posed by surveillance through the information gathering capabilities of the photographic camera, evolved the original conception of privacy as the right "to be let alone" (Rosen 2000). As a definition of privacy it entails a certain control of personal information, but is incapable of protecting personal data from modern technology. Many different conceptions have since developed in order to face the threats posed by modern surveillance technology. It can be argued that there are two broad types of modern conceptions of privacy; those that focus on the inherent value of privacy to both the individual and society, (Rosen 2000, Introna and Pouloudi 1999) and those that focus on an individual's agency to control their personal data in order to create beneficial exchanges (Ashworth and Free 2006, Posner 2008).

The conceptions that emphasise an inherent value of privacy, appear to focus on the *protection* of privacy, that no matter what other benefits one can procure in exchange, the value of privacy is too great to squander. These conceptions are inherently defensive and, it could be argued, a response to evolving surveillance threats. As surveillance technology stretches to more fields of human life and interaction, these privacy conceptions redefine themselves and throw up barriers in response. An example could be an imagined response to the collection of data for a medical database. An inherent value based approach to privacy would contend that such data must be properly regulated and the

stakeholder, that is, the individual involved, must be protected from data misuse or misappropriation (Introna and Pouloudi 1999).

Exchange based conceptions, focus on how individuals can enjoy the freedom to disclose their personal data unhindered in order to benefit from the exchange. They could be said to internalise the threats posed by modern informational technology, instead of directly confronting them. In response to the medical database situation above, an exchange conception of privacy might instead advocate an active participation in the database, after judging whether the exchange is free (Ashworth and Free 2006).

There are of course more varied conceptions of the right to privacy, but these two provide the optimal starting point when discussing the pertinent values and concerns while discussing surveillance as an aspect of security.

5.2. Privacy and modern video surveillance as an aspect of security:

In today's society, security is a major concern of policy makers, citizens, academics and media commentators alike, and surveillance is a major aspect of modern day security policies. Surveillance is an integral tool in the policy maker's arsenal in the "war on terror", and is becoming a more important tool as technology develops. As such, it is becoming increasingly important to address the implications of security surveillance on the right to privacy. As one of the more controversial, but valued aspects of surveillance (BBC 2006 20/07, 2011 20/01), this paper has chosen to focus on video surveillance.

The two illustrative examples chosen; CCTV coverage of London and the targeted video surveillance of Arne Treholt, are similar enough to enable us to compare the privacy concerns they arouse, while still being different enough to provide a discussion with different perspectives.

5.2.1: CCTV:

The idea of a *voluntary* exchange, is a basic and important aspect of many exchange-based conceptions of privacy. Voluntary surveillance implies an active volition to undergo the surveillance in question, something arguably lacking in London's CCTV network, in order to exchange ones personal data for a good or benefit. CCTV coverage as comprehensive as the surveillance regime in London, ensures that there is no plausible method of avoiding surveillance and still participating in society at a normal level, therefore, as opposed to other types of surveillance, CCTV cannot be

considered voluntary (Ashworth and Free 2006, Posner 2008).

Of course one can argue that as a member of a democratic society, that one has implicitly accepted that governments have the duty and authority to protect their citizen's security and safety. As a member of society, one has made a Hobbesian social contract whereupon one accepts that the state has the right to derogate from ones individual rights in order to protect the society. In effect: "the public will be compensated for the costs of diminished privacy in increased security from terrorist attacks" (Posner 2008: 251). This is of course a form of an exchange conception of privacy, except that the agency has been removed from the individual and placed in the hands of the state or society.

Inherent in any exchange of privacy, is the concept of a fairness judgement. The exchange must be considered a fair exchange from both a retributive and a procedural justice perspective (Ashworth and Free 2006). The first involves a value judgement, the value of the good received, increased security, must be equal or more to the value attributed to the loss of privacy, i.e. the data disclosed. In regards to CCTV this is a controversial question; it is near impossible to definitely establish the effectiveness of the surveillance, making it increasingly hard for an individual to make a satisfactory judgement. In addition, the data disclosed may be used for more than was originally assumed, such as CCTV cameras being used against dog foulers (BBC2009 06/02). Procedural judgement involves an individual feeling that they have been treated with respect in the exchange (Ashworth and Free 2006). If the citizens of London do not feel they are treated with respect, such as if they are not consulted prior to the re-purposing of CCTV cameras to track parking violations, the exchange may no longer be fair to them.

From a purely inherent value based conception of privacy, CCTV is difficult to accommodate due to the obvious violation of privacy, and the "chilling" effect that it has on human development and interaction. The evaluation of CCTV would be based upon an evaluation of the intrusiveness; are there still enough areas where one can as yet enjoy privacy? With the CCTV "creep" it is becoming increasingly difficult to reconcile CCTV surveillance with an inherent value based conception of privacy.

5.2.2: Covert video surveillance:

One major difference between London's CCTV surveillance regime, and the covert video surveillance of Arne Treholt's house, is the scope. CCTV is a broad-based surveillance technique capable of monitoring millions of people every day while the video surveillance used in Norway in

the 1980s, was very specific. They share the similarity that both techniques have negative externalities in the targeting of people who are not yet suspects.

An analysis of the media surrounding the revelation that Treholt's house was under video surveillance, shows that although the surveillance was condemned as objectionable, it may not have been considered a violation of the right to privacy by all commentators.

Obviously commentators who consider privacy to hold an inherent value, could not reconcile their views with such an invasive surveillance. As opposed to CCTV, the video surveillance that Treholt and Kari Storækre were under, showed an almost complete picture of their lives, especially when coupled with the other forms of surveillance used at the time, Treholt was almost never outwith his watchers sight (Jonnassen, Staveland and Gjerde 2010). The surveillance was particularly invasive due to the fact that it was centred on his home, a concept from which the original conceptions of privacy arose (Magi 2011). Proponents of privacy, as having an inherent value, would certainly argue along with many of the commentators, that the issue of Treholt being guilty or innocent is irrelevant, it was none the less a violation of his right to privacy (Gierstsen 2010, Døvik and Granbo 2010).

Some commentators may perhaps argue that in order to ensure national security and safety for Norwegian citizens, it may be necessary to derogate the right to privacy of certain individuals. While one could support this approach from an exchange conception of privacy, it is hard to justify, due to the invasiveness and huge consequences for innocent bystanders. A derogation of one individual who has committed a crime, or is under strong suspicion, is much more easily accepted in exchange for increased security for the other members of society (Posner 2008).

It is interesting that many commentators appear to object to this video surveillance, not due to concerns about privacy, as anti CCTV campaigners in the UK are known to do, but with concerns about the legality of the action. There is certainly a much stronger acceptance of warrant based surveillance, such as targeted wire taps, than broad-based surveillance, data mining of all telephone communications for example, among privacy campaigners (Vlcek 2008, Posner 2008). But it is difficult to reconcile such an invasive surveillance operation when it violates the privacy of innocents. The fact that it was an illegal surveillance operation, most likely ensures that any proponent of an increased surveillance regime will have a more difficult time as a result of the lack of trust in the security forces.

5.3. Common challenges to privacy in video surveillance:

One concern raised against both of the video surveillance regimes, is the question of justification. As surveillance is an inherent threat to privacy, any surveillance must be justified in order for it to have a chance to be reconciled with the right to privacy. A surveillance regime must be necessary in order to be justified. An unnecessary surveillance regime is simply a violation of the right to privacy. Both examples of video surveillance claim to be justified in terms of security and safety, this can be reconciled relatively smoothly with an exchange-based conception of privacy. Of greater concern is how effective the regime is. If, as some statistics portray it, the London CCTV regime is expansive, intrusive and inefficient, then the regime will have an extremely hard time to reconcile itself with any conception of privacy.

Several theorists have pointed out the seeming contradiction that we, as individuals in modern society, are becoming increasingly open with our personal information, as can be seen by the proliferation of social networking sites and blogs, while simultaneously becoming increasingly concerned with privacy (Rosen 2000, Posner 2008, Magi 2011). This can be reconciled through trust, that one trusts that the data disclosed for a given purpose is *solely* used for that purpose.

Trust is a necessity, if surveillance regimes are to be successfully implemented, an individual will not disclose data without trust, an exchange will not be judged fair if it is not judged trustworthy, and covert surveillance will not be reconciled with the general populace if they cannot trust the surveillance operators. This is particularly important in regards to security surveillance. If individuals can trust the CCTV operators to keep all personal data secret, and only use the data gathered for the stated purpose, they are less likely to be opposed, especially when they are aware of the possible security that may be exchanged (Posner 2008, Haggerty and Gazso 2005). Covert video surveillance can, if legal, be accepted under the same reasoning, if there is a trust in the operators. Of course these kinds of surveillance regimes are controversial, simply pledging to keep the data safe and to use it for its original purpose, will likely not be enough. Increased and transparent regulation is necessary to create trust.

6. Conclusion:

The right to privacy is a fundamental human right set forth in both the UDHR and the CCPR. In order for it to be adequately protected as a right, human rights defenders must understand what the right actually is. This paper set out to discuss and compare different conceptions of the right to privacy, and how developments in technology and surveillance are challenging that right.

The events of 9/11 and the "war on terror" have ushered in an age where security is the predominant concern of policy makers and governments, where they struggle to balance the apparently antagonistic values of security and civil liberties, among which, is privacy (Goldstone 2006). Surveillance has become one of the favoured tools of policy makers in their counter-terror tactics, and has grown as an aspect of society. As surveillance has become more prominent, so have the threats it presents to privacy.

The paper has discussed several different conceptions of privacy, and how the conception used can alter the way we view our society, and our priorities, particularly in regards to surveillance. Privacy is not a constant and universal principle, but changes due to socio-cultural and historical circumstances. Even today the conception of privacy is changing in response to recent developments, in particular, technological developments. The innovations within communications, prompted by the information age, have helped evolve the conception of the right to privacy further. Any conceptions of the right to privacy can no longer be solely based upon property or the "right to be let alone". The various issues that concern privacy in modern society, mean that one can no longer give privacy a single definition, but must instead use it as an umbrella phrase that encompasses the many varied aspects of the concept.

On the most basic level, privacy is simply the control of one's own personal data. The antithesis to that is surveillance. Surveillance is, at its most simple level, the collection of personal data. As such, surveillance is an antagonistic contradiction to privacy and the greatest threat to the right to privacy. Surveillance is perhaps a necessary part of any definition of privacy, as privacy is shaped and often defines the threats it faces.

Among the various understandings of privacy, two were particularly beneficial to this paper; the inherent value based conception, which focuses on how privacy has an inherent value, and is a goal in itself, and the exchange based conception, which portrays privacy in terms of exchanges of personal data for societal goods or benefits.

The original threat to privacy in Louis D. Brandeis and Samuel D. Warren's article, was that of the "instantaneous photographs" (quoted in Rosen 2000: 34). In today's security minded society one of the greatest threats to privacy is that of video surveillance. This paper has analysed the discourses surrounding CCTV usage in London, and the use of covert video surveillance on Arne Treholt in Norway, in order to better understand how surveillance affects different conceptions of privacy and vice versa. How video surveillance could be reconciled with various conceptions of privacy was also investigated.

Most of the discourses were variants of the two main conceptions of the right to privacy previously described. Surveillance was as such, difficult to reconcile with most conceptions, due to the inherent antagonistic contradiction between the two concepts. It was found that an exchange conception of privacy could be reconciled with surveillance, if certain conditions were met. Specifically that the trade of personal data for societal goods is beneficial for the individual.

The surveillance has to be justified; individuals in society must be able to make a *fairness judgement* regarding their loss of privacy and what they receive in exchange. The surveillance has to be efficient, it has to be a fair exchange of values, and the individual must be able to trust that their personal data will not be misused or re-purposed. This is an increasing problem in modern society, as more and more data is stored in electronic databases and left vulnerable to become a "surveillant assemblage".

For a security surveillance regime to be able to attempt to reconcile itself with the right to privacy, it must be able to guarantee that the data is not re-purposed, the surveillance operators must gain the trust of the individuals. This is most simply done by clear and transparent regulation, ensuring that data is used properly. If these conditions are met in an individual's evaluation, then it is possible to reconcile his/her privacy as an exchange for increased security through surveillance. In most cases individuals and commentators have a conception of the right to privacy where derogations can be made in exchange for security, but only to a certain extent, privacy does have inherent values.

It will never be possible to reconcile a surveillance regime that encroaches too far into our privacy, but as the conception of privacy changes in response to outer circumstances, it may lead to an eventual weakening of the right to privacy as our conceptions accept more and more derogations.

6.1. Recommendations:

The paper has the following recommendations to make:

Surveillance has become an important part of modern society, almost an integral one, which we use in trade, communication and security; we cannot simply do away with it. At the same time we cannot allow it to run rampant and intrude more than necessary into our privacy.

At this moment in history we are in a paradigm where security is the emphasis of policy, and fear is on the minds of many. Eventually this mindset will pass and we will be left with a surveillance regime that is no longer necessary but institutionally difficult to remove (Haggerty and Gozso 2005). In order to combat this we must be aware of the risks, and develop regulation that will both minimise the amount of surveillance used, and prevent the misappropriation of databases into surveillant assemblages. This regulation ought to be developed on an international level, perhaps in the form of a treaty. The retention and spread of data in databases, which are constantly being merged, may pose the greatest threat to the right to privacy in the coming years. Such regulation could potentially increase individual's trust in surveillance operators and their ability to aid the populace.

This paper recommends that further research be made into other aspects of surveillance, particularly in regards to data aggregation and mining, and how that affects the right to privacy and its protection. Another interesting direction for potential research could be investigating the efficiency of CCTV coverage; it is still something of a mystery.

On a final note, this paper opened with a quote from Benjamin Franklin reminding us that we do not deserve liberty if we give it up for safety. This paper agrees in principle, although modern society necessitates a certain loss of privacy. Instead we must remain vigilant to minimise the encroachment into our privacy. The surveillance that is now part of our lives must be kept under scrutiny. In order to defend our right to privacy we must ask ourselves: “Quis custodiet ipsos custodes?”

Word count: 13960

References:

Aalbu, **Anders. (2010).** "Storberget ber om svar om Treholt-overvåking". *NRK.* [Online] 28 September. Available at:http://www.nrk.no/nyheter/norge/1.7311718 [Accessed 26/05/11]

Aftenposten. (2010). "Storberget ber om svar om Treholt-overvåking". *Aftenposten.* [Online] 28 September. Available at: http://www.aftenposten.no/nyheter/iriks/article3830538.ece [Accessed 26/05/11]

Ashworth, Laurence. and Free, Clinton (2006). "Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy concerns" *Journal of Busines Ethics* Vol 67 (2).

Allen, **Liam. (2006).** "Is 'reality CCTV' a step too far?". *BBC News.* [Online] 8 May. Available at: http://news.bbc.co.uk/2/hi/uk_news/4752167.stm [Accessed 26/05/11]

Bhatt, Chetan. 2008. "Doing a dissertation" in "*Researching Society and Culture*" **Seale, Clive. (ed.).** Sage Publications Ltd. London.

Aune, Oddvin. (2010). "PST finner ikke overvåkningsvideo". *NRK.* [Online] 18 September. Available at: http://www.nrk.no/nyheter/norge/1.7342932 [Accessed 26/05/11]

Aune, **Oddvin. and Hessevik, Jørund. (2010).** "Treholt: - Jeg er forbannet og oppgitt". *NRK.* [Online] 18 September. Available at: http://www.nrk.no/nyheter/norge/1.7298203 [Accessed 26/05/11]

British Broadcasting Company BBC. (2002). "West End surveillance stepped up" *BBC News.* [Online] 18 September. Available at: http://news.bbc.co.uk/2/hi/uk_news/england/2267359.stm [Accessed 26/05/11]

British Broadcasting Company BBC. (2006). "Rights group criticises 'Asbo TV'" *BBC News.* [Online] 10 January. Available at: http://news.bbc.co.uk/2/hi/uk_news/england/london/4597990.stm [Accessed 26/05/11]

British Broadcasting Company BBC. (2006). "How We are being watched." *BBC News.* [Online] 3 November. Available at: http://news.bbc.co.uk/2/hi/uk_news/6110866.stm [Accessed 26/05/11]

British Broadcasting Company BBC. (2008). "Q&A: Loss of Freedoms?" *BBC News.* [Online] 12 June. Available at: http://news.bbc.co.uk/2/hi/uk_news/7451552.stm [Accessed 26/05/11]

British Broadcasting Company BBC. (2009). "Warning over 'surveillance state'". *BBC News.* [Online] 6 February. Available at: http://news.bbc.co.uk/2/hi/uk_news/politics/7872425.stm [Accessed 26/05/11]

British Broadcasting Company BBC. (2009). "The statistics of CCTV"**.** *BBC News.* [Online] 20 July. Available at: http://news.bbc.co.uk/1/hi/uk/8159141.stm [Accessed 26/05/11]

British Broadcasting Company BBC. (2009). "1,000 cameras 'solve one crime'"**.** *BBC News.* [Online] 24 August. Available at: http://news.bbc.co.uk/2/hi/uk_news/england/london/8219022.stm [Accessed 26/05/11]

British Broadcasting Company BBC. (2009). "'Hidden CCTV' installed in homes". *BBC News.* [Online] 18 November. Available at: http://news.bbc.co.uk/2/hi/uk_news/england/london/8366317.stm [Accessed 26/05/11]

British Broadcasting Company BBC. (2010). "New York mayor Bloomberg views London CCTV measures". *BBC News.* [Online] 20 July. Available at: http://news.bbc.co.uk/2/hi/uk_news/england/london/8674181.stm [Accessed 26/05/11]

British Broadcasting Company BBC. (2010). "'Six crimes a day' solved by CCTV, Met says". *BBC News.* [Online] 26 December. Available at: http://www.bbc.co.uk/news/uk-england- london-12080487 [Accessed 26/05/11]

British Broadcasting Company BBC. (2011). "Is CCTV creeping too far?" *BBC News.* [Online] 20 January. Available at: http://www.bbc.co.uk/news/magazine-12224075 [Accessed 26/05/11]

British Broadcasting Company BBC. (2011). "PS3 hacking case: Sony gets downloaders' information" *BBC News.* [Online] 7 March. Available at: http://www.bbc.co.uk/news/technology-12663410 [Accessed 26/05/11]

Bryman, Alan. 2008. "*Social Research Methods*" Oxford University Press. Oxford.

Bayer, Ronald. and Fairchild, Amy L. (2000). "Surveillance and Privacy" *Science, New series* Vol 290 (5498).

Duffy, Jonathan. (1999). "Something to watch over us." *BBC News.* [Online] 4 May. Available at: http://news.bbc.co.uk/2/hi/uk_news/334853.stm [Accessed 26/05/11]

Døvik, Olav. and Granbo, Kristin (2010). "–Staten bør gi Storækre oppreisning" *NRK* [Online] 20 November. Available at: http://www.nrk.no/nyheter/norge/1.7390381 [Accessed 26/05/11]

Fairclough, Norman. 2001. "Critical discourse analysis as a method in social scientific research" in "M*ethods of Critical Discourse Analysis*" **Wodak, Ruth and Meyer, Michael. (ed.).** Sage Publications Ltd. London.

Galison, Peter and Minow, Martha. 2006. "Our Privacy, Ourselves in the Age of Technological Intrusions" in *"Human Rights in the 'War on Terror'"* **Wilson, Richard Ashby. (ed.).** Cambridge University Press. Cambridge.

Giertsen, Johan. (2010). "Krenkende taushet". *Aftenposten.* [Online] 10 October. Available at: http://www.aftenposten.no/meninger/article3835925.ece [Accessed 26/05/11]

Gill, Martin and Spriggs, Angela. 2005. "*Home Office Reasearch Study 292 – Assesing the impact of CCTV*". Home Office Research, Development and Statistics Directorate. London.

Gjerde, Robert. (2011). "Også soverommet avlyttet". *Aftenposten.* [Online] 09 February. Available at: http://www.aftenposten.no/nyheter/iriks/article4055763.ece [Accessed 26/05/11]

Goldstone, Richard. (2006). "Combatting Terrorism and Protecting Civil Liberties" in *"Human Rights in the 'War on Terror'"* **Wilson, Richard Ashby. (ed.).** Cambridge University Press. Cambridge.

Goodchild, Sophie. (2007). "Britain becoming a Big Brother society, says data watchdog" *The Independent.* [Online] 28 April. Available at: http://www.independent.co.uk/news/uk/this-britain/britain-becoming-a-big-brother-society-says-data-watchdog-446700.html [Accessed 26/05/11]

Haggerty, Kevin D. and Gazso, Amber (2005). "Seeing beyond the Ruins: Surveillance as a Response to Terrorist Threats" *The Canadian Journal of Sociology* Vol 30 (2).

Hari, Johann. (2008). "This strange backlash against CCTV - There is a danger that the debate about civil liberties is driven into a right-wing ditch" *The Independent.* [Online] 17 March. Available at: http://www.independent.co.uk/news/uk/crime/the-big-question-are-cctv-cameras-a-waste-of-money-in-the-fight-against-crime-822079.html [Accessed 26/05/11]

Introna, Lucas D. and Pouloudi, Athanasia (1999). "Privacy in the Information Age: Stakeholders, Interests and Values" *Journal of Business Ethics*Vol 22 (1).

Jonnassen, Arild M. Staveland, Lars I. and Gjerde, Robert. (2009). "Treholt-spaner: Bevis ble forfalsket"**.** *Aftenposten*. [Online] 18 September. Available at: http://www.aftenposten.no/nyheter/article3816677.ece [Accessed 26/05/11]

Kasper, Debbie V. S. (2005). "The Evolution (Or Devolution) of Privacy" *Sociological Forum* Vol 20 (1).

Kolsrud, Kjetil. (2008). "En spions historie". *Aftenposten.* [Online] 7 December. Available at: http://www.aftenposten.no/nyheter/iriks/article2810540.ece [Accessed 26/05/11]

Magi, Trina J. (2011). "Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature" *The Library Quarterly* Vol 81 (2).

Manning, Rita C. (1997). "Liberal and Communitarian Defenses of Workplace Privacy" *Journal of Business Ethics* Vol 16 (8).

McSmith, Andy. (2008). "The Big Question: Are CCTV cameras a waste of money in the fight against crime?." *The Independent.* [Online] 7 May. Available at: http://www.independent.co.uk/news/uk/crime/the-big-question-are-cctv-cameras-a-waste-of-money-in-the-fight-against-crime-822079.html [Accessed 26/05/11]

Meyer, Michael. (2001). "Between theory, method, and politics: positioning of the approaches to CDA" in "M*ethods of Critical Discourse Analysis*" **Wodak, Ruth and Meyer, Michael. (ed.).** Sage Publications Ltd. London.

Monmonier, Mark. 2002. "*Spying with Maps*" The University of Chicago Press. Chicago.

Norsk Rikskringkasting NRK. (2010). "Lund bekrefter videoovervåking" *NRK.* [Online] 27 September. Available at:http://www.nrk.no/nyheter/norge/1.7311460 [Accessed 26/05/11]

Posner, Richard A. (2008). "Privacy Surveillance and Law" *The University of Chicago Law Review* Vol 75 (1).

Rosen, Jeffery. (2000). "Why Privacy Matters" *The Wilson Quarterly* (1976-) Vol 26 (4).

Stanghelle, Harald (2010). "Hevet over loven" *Aftenposten.* [Online] 29 Spetember. Available at: http://www.aftenposten.no/meninger/kommentatorer/stanghelle/article3832490.ece [Accessed 26/05/11]

Walsh, John. (2010). "Big Brother: the series that made surveillance acceptable" *The Independent.* [Online] 18 August. Available at: http://www.independent.co.uk/opinion/commentators/big-brother-the-series-that-made-surveillance-acceptable-2055154.html [Accessed 26/05/11]

Vlcek, William. (2008). "A leviathan Rejuvenated: Surveillance, Money Laundering, and the War on Terror" *International Journal of Politics, Culture, and Society* Vol 20 (1).