THE ETHICS OF WORKSPACE SURVEILLANCE

Elin Palm

STOCKHOLM 2007
Abstract


The general framework of this thesis is that of ethical Technology Assessment (eTA). Whereas the first essay proposes an inclusive approach to technology assessment by delineating an ethical checklist, the following essays focus on two of the checklist points, i.e. “privacy” and “control, influence and power”, in relation to workspace surveillance.

The core idea of *Essay I* (written in collaboration with Sven Ove Hansson) is that, due to its strong social impact, new technology and novel use of existing technology should be considered from the perspective of ethics. We suggest that assessments should be conducted on the basis of nine crucial ethical aspects of technology.

In *Essay II* an in-depth analysis of the meaning and value of privacy in the realm of work is undertaken. The meaning and value of privacy is explained as well as why it should be protected. It is argued that two dimensions of privacy should be safeguarded; “informational privacy” and “local privacy” for the reason that workers’ personal autonomy is protected thereby.

*Essay III* is concerned with how workspace surveillance requires that job-applicants claim their privacy interests in employment negotiations to a much larger extent than what was previously the case. In most cases however, a dependency asymmetry between employer and job-candidate makes the latter ill-equipped for doing so. This asymmetry serves as the point of departure for an analysis of the conditions under which consent should be considered a criterion on moral acceptability with regard to employment contracting. The analysis suggests ways of rectifying this imbalance, raising demands on the quality of contractual consent.

*Essay IV* discusses the extent to which it should be morally permissible for current or prospective employees to trade off their privacy in employment negotiations. The analysis starts out from, and questions, a libertarian case for voluntary self-enslavement. It is concluded that not even an orthodox libertarian can justify trade-offs of a social good like liberty. Neither should employees be allowed to abstain informational privacy for the reason that such a trade-off could harm their future selves.

In *Essay V* a dimensional analysis is proposed as a means to identify actually or potentially privacy invasive surveillance practices. It discusses ways in which different types of surveillance intrude upon employees’ privacy in order to guide the evaluation of such practice. Even though negative implications cannot be avoided altogether, by means of the proposed analysis, minimally intrusive means of monitoring can be identified.

**Key words:** asymmetric relations, autonomy, consent, contract theory, contractualism, employment, ethical technology assessment, ethics, monitoring, reasonable interests, privacy, surveillance, technology assessment, work, workspace, workspace surveillance.
List of essays

This doctorate thesis consists of the following introduction and:


Elin Palm, Department of Philosophy and the History of Technology, Royal Institute of Technology (KTH), 100 44 Stockholm, Sweden.
Acknowledgements

First and foremost, I wish to express my gratitude to my supervisor Professor Sven Ove Hansson for his helpful guidance throughout the process of writing this doctoral thesis. Without his support this work would not have come about. I also want to thank all of my colleagues at the Division of Philosophy who, in various ways, have assisted and encouraged me over the years. In particular, I would like to thank Lars Lindblom, Barbro Björkman and Drs. Anders Persson and Martin Petersson for their careful reading of my manuscripts, inspirational discussions and constructive criticism. Furthermore, I want to acknowledge Professor Dag Elgesem, who served as a discussant on my Licentiate thesis in 2005 – his feedback has been of great value for my subsequent work.

I have also benefited immensely from two extended academic visits: one at the Department of Philosophy, University of Amsterdam (UvA) where Professor Beate Rössler served as my supervisor, and the other at Queen’s University, Canada working with Professor David Lyon and The Surveillance Project. These visits were made possible by generous scholarships from the Swedish Foundation for International Cooperation and Research in Higher
Education (STINT) and the Swedish Council for Working Life and Social Research (FAS) respectively. I gratefully acknowledge Beate Rössler’s generosity with time, comments and support. Her thoroughgoing work on privacy and her enthusiasm for the subject have been truly inspiring. In turn, working within the Surveillance Project has been an immensely rewarding experience. I wish to thank David Lyon for welcoming me into his research group and Professor Emeritus Elia Zureik and Emily Merz Smith for fruitful discussions on work-related surveillance.

All essays in this thesis have been presented in various conferences and workshops where I have also received many valuable comments. In particular I would like to thank the researchers at the Tilburg Institute of Law, Technology and Society for inviting me to a very inspirational discussion on privacy at work. In addition, I would like to thank the participants of the one-week ECPR workshop on “Privacy and Information - Modes of Regulation” in Helsinki 2007. I am particularly thankful for the discussant Professor Dag Wiese Schartum and for his useful comments.

Beyond these various academic stimulations, I also want to acknowledge that the work in this thesis has been financially supported by Vinnova and by SALTSA; A joint Programme for Working Life Research in Europe run by the former Swedish National Institute for Working Life (NIWL/ALI) and the Swedish Confederations of Trade Unions (LO), Professional Employees (TCO) and Professional Associations (SACO). My sincerest thanks go to
Programme Secretary Charlotta Krafft for her keen interest in this research project.

Finally, and certainly not least, the moral support from friends and family has been essential for accomplishing this thesis. Above all, I would like to thank Professor Göran Collste for planting the idea of doctoral studies in my mind and for his encouragement throughout this endeavour. Without his support I would never have embarked on this journey.

Stockholm

Elin Palm

November 2007
Contents

ABSTRACT

ACKNOWLEDGEMENTS

1. INTRODUCTION

2. AIM AND SCOPE
  2.1 Key concepts
  2.2 Reasons for surveillance
  2.3 Why ethical analysis?
  2.4 Preview of Essays I-V

4. A DESCRIPTIVE ANALYSIS OF PRIVACY
  4.1 Surveillance at work
  4.2 The legal framework

5. A NORMATIVE ANALYSIS OF PRIVACY
  5.1 The value of privacy
  5.2 Privacy in public
  5.3 Privacy as a social good
  5.4 Reasonable expectations of privacy from a moral perspective
  5.5 Securing privacy - contractual procedure and content

6. A THEORETICAL FRAMEWORK FOR FAIR CONTRACTING

7. ISSUES FOR FURTHER RESEARCH

8. CONCLUSION

REFERENCES
1. Introduction

As a result of modern surveillance technology individual workers and their dealings grow more and more transparent. An employee carrying an ID-card equipped with biometric information and Radio Frequency sensors - a so called Smart-ID - can, upon her arrival at work, be authenticated and registered. Once the card is authenticated, the employee’s movements throughout a factory building can be followed in real time and/or tracked. Simultaneously, strategically placed close-circuited cameras may provide images and software can be used to monitor her movements. Company computers and electronic equipment can record activities and software like computerized performance monitoring (CPM) can be used to assess her work on a computer e.g. by measuring the number of keystrokes per time unit (Ball, 2003). Interaction with clients, customers and co-workers can be video recorded, intercepted and listened in on. Moreover, geographical positioning system (GPS) device in company owned vehicles can reveal an employee’s position and path through areas outside the work-site (cf. Bennett in: Hansson and Palm, 2005). Yet another dimension of supervision and control
in the realm of work involves extensive medical checks such as drug- and pregnancy tests (Borg and Arnold, 1997) and in some cases, health surveillance in the form of genetic screening and monitoring (Regan in: Zureik and Lyon (Eds), 1995, Sorsa and van Damme in: Hansson and Palm (Eds), 2005).

Not only has novel technology expanded the arsenal of tools, it has altered the nature of surveillance and the modes of gathering and processing information. Of course, observation and control have always been a part of the hiring process and employment conditions. Assessments have played a key role in efforts to control systems of transportation, communication and manufacturing (Beninger, 1986). But increasing availability of relatively inexpensive and easy to use surveillance devices is enabling employers to expand the range and scope of their control over their employees’ activities. It also allows constant and more detailed surveillance than has been possible with traditional methods (Fairweather, 1999) and the process of information gathering has become more surreptitious (Bennett in: Hansson and Palm, 2005:73).

Even if employers have traditionally considered it within their right to monitor their employees and even though they have had various techniques at their disposal, the ways in which surveillance can be conducted have changed significantly in the past few decades. Traditional means of control such as human supervisors, cash registers, log books and punch clocks (cf. Sewell,
1999, Marx, 1995) enabled employers to identify the doings and productivity of a group of workers. Today however, employers can single out individual workers, continuously scrutinize their activities and obtain detailed reports on their work. Computerized surveillance technology allows for an unprecedented accuracy, continuity and scope of monitoring (cf. Marx, 1985) and medical surveillance can reveal a previously unavailable type of data – genetic information (Alpert, 2003).¹

Historically, surveillance often involved distrust, coercion and asymmetrical power relations (Sewell, 1999:9) and most certainly, modern surveillance technology can imply an opaque, oppressive and unequal form of control. However, even if surveillance makes for an instrument of power, it will not automatically invite resistance (Zureik in:. Lyon, 2003:52). Rather, the context, implementation and technology employed in the application determine how it is received. This doctoral thesis contributes to the identification of morally acceptable forms of workspace surveillance. It teases out conditions for reasonable surveillance by explicating the meaning and value of privacy at work and by investigating ways of securing this value.

¹ More to the point, computer-based technology fundamentally changes the cognitive and organizational aspects of work and new management techniques have been adopted that involve workers more substantively in the production process (Zureik, in:. Lyon, 2003:46-52). The case has been made that surveillance technologies are increasingly combined with team based management (cf. Sewell, 1998). That is, management hierarchies are flattened out into teams creating vertical surveillance by management and horizontal surveillance by peers relying on mutual supervision and self-discipline (cf. Sewell, 1998).
2. Aim and scope

In this thesis ethical implications of work-related surveillance will be analyzed. My primary aim is to contribute to the identification of conditions under which surveillance capable technology and surveillance conduct may be considered morally acceptable.

I start out by emphasizing the need to bring in ethical aspects to technology assessment, suggesting an ethical checklist to be applied to new technology or to novel use of already existing technology. Two of the checklist entries; privacy and control, are the main components to be analyzed throughout this thesis. It should be noted though, that the discussion of these two aspects will, to a rather large extent, overlap. The analysis of privacy will be conducted in two steps:

First, I will provide a descriptive account of privacy, high-lighting some general features of surveillance and privacy intrusions based on sociological theory of surveillance. I will also exemplify actual reactions to work-related surveillance as conducted within call-centers, informed by empirical sociological studies (Lankshear et al, 2001, Ball, 2003, Merz Smith, 2004). This
section also contains a rough overview of existing privacy protection, indicating how privacy is viewed from a legal perspective.

Second, in a normative analysis I investigate the meaning, value and scope of privacy in the context of work. Here, I discuss how workers’ privacy should be understood. This section addresses the questions of why privacy is valuable and what expectations employees reasonably may have. I also examine the employees’ chances of securing these expectations in employment negotiations and the extent to which they should be at liberty to do so. That is, I first consider the contractual form, then the contractual content. Although the literature on privacy is extensive, little unity is found and no real attempts have been made to show how privacy should be understood in the realm of work.

This section draws on the discussions of privacy in my essays and synthesizes the most essential aspects to a unit. Certain aspects are further explicated by additional material. Drawing on three important contributions to the philosophical discussion of privacy I will present a framework of privacy suitable for the context of work. The three sources are; Beate Rössler’s analysis of the value of privacy (2001, 2005), Helen Nissenbaum’s emphasis of privacy as contextual integrity (Nissenbaum, 1998, 2004) and Priscilla Regan’s work on the social importance of privacy (Regan, 1995).

A strong reason for undertaking this analysis is that once we have a clear understanding of what privacy means within the realm of work and why it
should be protected, we have a better normative foundation for a satisfactory privacy protection legislation. Having a conception of workers’ privacy would enable us to assess the extent to which existing laws and codes accommodate workers’ privacy and, from there, work towards adequate legislation. At present, no such basis exists. Rather, protection of workers’ privacy primarily draws on general data protection legislation. Likewise, a better understanding of the meaning and importance of contractual consent in employment negotiations can aid the protection of workers’ privacy. Both aspects become highly relevant in the light of increased work-related surveillance.

2.1 Key concepts and scope

Before entering the discussion proper, a few key-concepts require explanation. Under “surveillance” I include practices that involve the gathering of information about individuals in order to influence their behaviour or control them. These activities may be technologically instrumented but not necessarily. The definition is intended to capture methods ranging from the sophisticated, such as interception of communication and location-based surveillance to the very rudimentary, such as standard enforcement of dress codes and codes of conduct. Traditional and novel forms of surveillance, health-surveillance and computer-based surveillance are all included. In addition I rely on a distinction between surveillance and monitoring where the latter is considered a
precondition of the former. Monitoring refers to information-gathering activities in general whereas surveillance refers to data collection for a certain purpose (Rogerson and Prior, 2005). Although not clear-cut, this distinction fits well with the intuition that there is a significant difference between data collection motivated by a general aim of deterrence in public and data collection motivated by a specific reason such as identifying how many key strokes an employee makes per time unit. In some cases it may be difficult to establish whether an employee is under surveillance or only monitored, especially where several interests are at play simultaneously. Cameras in taxis for example, serve the general aim of enhancing public safety, of protecting the company asset (the car) and the health and safety of employees. They also serve to track every movement of the driver, which can go beyond monitoring in some circumstances.²

By privacy, I understand the relative ability of individuals to exercise control over personal aspects that she reasonably wishes to control. Importantly, privacy is a spatial and intellectual sphere that allows individuals to control others’ access to their personal information (both direct sensory access and stored data). Control over one’s self-representation is key to establishing and developing different types of relations. Individuals’ privacy expectations and

²The ambiguity of the concept of surveillance has been highlighted by David Lyon using parenting as an example of surveillance and control (Lyon, 2007:14). The question is however, under what conditions surveillance practice is morally acceptable and not.
the legitimacy thereof vary with context and privacy is a context dependent notion. The concept of workers’ privacy will be further developed in section.\textsuperscript{5}

It should also be mentioned that when discussing a current or prospective employee’s chances and rights to secure her privacy interests in employment negotiations, I deliberately use a rather simplistic model of the contract relation, namely one which includes only two contracting parties. Reduced to its most essential elements, the employment relation is taken to consist of employer and employee. In the normative part, I use this minimal model both to describe surveillance conduct at work\textsuperscript{3} and to discuss the interests and obligations of the employer and the current or prospective employee, leaving aside the role of unions, collective bargaining and worker councils such as those at the European labour market. Such a minimalist backdrop teases out the morally problematic issues at hand.

Moreover, the employment context considered is that of the European labour market and the type of work to be discussed is work conducted by employees in exchange for remuneration either from public or private employing entities - and more precisely - work that is regulated by an employment contract that specifies certain conditions, duties and obligations.

\textsuperscript{3} Modern theories of surveillance typically emphasize surveillance as an assemblage rather than as a top-down activity. In the context of work, multilayered surveillance is discussed. Although I am sympathetic with such descriptions, the moral implications regarding surveillance are primarily tied to the uneven relation between employer and employee. Hence, the simplistic model will be used to discuss work-related surveillance as a “one-to-one activity” or “one-to-many activity”
This includes temporary and freelance work as well as long-term employment. Excluded from the discussion is paid work carried out in the household by members of the household. Work conducted in a household by outsiders could be regulated by formal employment contracts but generally is not.
3. An ethical analysis of work-related surveillance

Before embarking on a more in-depth explanation of the reasons for subjecting work-related surveillance to ethical assessment, the reasons an employer might have for implementing surveillance technology and for subjecting workers to control deserve some attention.

3.1 Reasons for surveillance conduct

Employers mainly adopt surveillance capable technology at work for efficiency, productivity and security. Perhaps unsurprisingly, employers are primarily interested in improving the efficiency and profitability of an organization. However, they are also responsible for the health and safety of workers, consumers and the public. These interests and obligations can explain most cases of implementation and use of work-related surveillance. Surveillance is used to control the employees’ behaviour and performance, to protect work premises, stock and means of production and to deter and control abuse of the employment relationship (Miller and Weckert, 2000). Moreover, it is used to comply with regulatory requirements and to promote
certain public interest considerations. A rather clear-cut example of surveillance used for reasons of efficiency and productivity would be call-center surveillance where computerized data-collection is used to obtain information about workers’ capacity, skills, performance, attendance and knowledge. This information is analyzed and categorized to align worker performance with organizational goals and also to compare workers to each other in terms of work performance. It may also be used to predict optimum staffing level, skills and capability combinations (Ball, 2003). Furthermore, surveillance cameras may be employed to protect property against damage, misuse and theft (Miller and Weckert, 2000). Surveillance technology may also be used to reduce risks associated with certain types of job. Close Circuit TV can be used to reduce risks to employees and third parties as in the case of cameras in public transport and taxis. Medical surveillance is typically used in industries where employees are subject to hazardous exposure. To the extent genetic screening is used, it is most likely intended to lower health-related costs, especially in countries with a private health insurance system (Sorsa and van Damme in: Hansson and Palm, 2005:41).

Surveillance may be welcomed not only by employers and owners of the means of production but also by those subjected to surveillance. It can be seen as a more objective form of productivity assessment than traditional direct supervision by a manager whose personal view of the worker may influence a
performance evaluation. It may help to reduce the problems of favouritism (Merz Smith, 2004:19). Moreover, computerized surveillance technology may be seen as having a higher degree of accuracy than manually conducted observations. Computerized performance monitoring can validate employees performance, differentiating hard-working employees from “free riders”. Most importantly though, certain types of surveillance technology are applauded for their (allegedly) safety-enhancing effects.

3.2 Why ethical analysis?

As we have seen, there are several benefits to work-related surveillance and, clearly, “the transparent employee” canvassed in the introduction is an exaggeration. Most likely, single employees would only in exceptional cases be subject to such encompassing surveillance. Nevertheless, technologies that collect and store data about work performance are becoming routine features in the context of work (Lankshear et al., 2001). The proliferation of surveillance capable technology indicates that surveillance practice can be employed in many different work-settings. While call-centers have been the focal point of most empirical studies on surveillance at work, the use of computerized performance monitoring has spread from call-centers to banking, insurance and health care. That is, call-centers are no longer the extreme exception. Indeed, the case has been made that no occupation is
immune to surveillance at work given the prevalence of computerized work (Lyon, 1993:244).

My reasons for subjecting surveillance technology to ethical analysis are rather straightforward. The plethora of surveillance capable technology available merits ethical consideration due to its privacy invasive capacity. Technology that enables continuous and systematic collection of personal data possesses a potential to influence the data subjects in a most profound way. More to the point, surveillance and monitoring are likely to become particularly problematic in the context of work. One reason for this is that the majority of the surveillance capable devices used in public, such as various forms of monitoring cameras, biometrics, location based technologies or Information and Communication Technologies (as well as combinations of these), are in use or can be used within the area of work as well. In addition, there are surveillance forms that are almost exclusive to work such as genetic screening used to detect dispositions to genetic disorders and smart IDs like the Hygiene Guard®.

The following four aspects of work and the areas where work is conducted tend to make work-related surveillance particularly problematic from an ethical perspective: 1) the unavoidability aspect, 2) the continuity aspect, 3) the dependency aspect and 4) the identification aspect.
Firstly, by the *unavoidability aspect* I mean that job-applicants can seldom avoid surveillance simply by strategically choosing a position. Although avoiding surveillance in public can be rather difficult as for instance when traveling by air and when surfing the Internet, in order to avoid surveillance at work individuals may have to abstain from working. Given the social importance of work i.e. the most important means of securing ones living and an ever so important way of self-realization, a freedom of choice argument is not as readily applicable in relation to work as it might be in other cases.

Secondly, within the workplace, individuals can be subjected to monitoring over a longer period of time than what, in most cases, would be possible in other areas of society. The *continuity aspect* bears relevance for privacy intrusiveness. Most likely, data generated by long-term camera surveillance in a work setting is more privacy sensitive than information about occasional bypassers as in the case of camera surveillance in public spaces.

Thirdly, the *dependency aspect* refers to the importance of the relation between the observer and the observed. In a situation where the data subject is dependent on the observer’s acceptance and liking, she may alter her behavior accordingly even if this would be against her reasonable interest. An asymmetric dependency relation like the one which is typically in place

---

*Although used here, it should be noted that the distinction between a public and a private sphere is found problematic and that it will be questioned later on.*
between employer and employee may make the latter alter her behavior in ways she would prefer not to (Miller and Weckert, 2000).

A final significant difference between general surveillance and work-related surveillance is the *identification aspect*. As opposed to camera monitoring in public places, the individuals subjected to surveillance at work are typically known to the observer in advance or at least they are readily identifiable. Already existing personal files i.e., employment records, facilitates storage and processing of data collected by monitoring. Different types of personal data may be combined from which certain patterns or profiles may be extracted.

Taken together, these four aspects indicate that employees, in most cases, are more vulnerable to privacy intrusions than individuals in general with regard to public surveillance. Thus, work-related surveillance tends to have a greater impact on single individuals than what general surveillance has (at least in the absence of an omnipresent Big Brother). Apart from the ethical issues that immediately appear to be of particular relevance i.e. privacy and autonomy, certain features of work such as the areas within which work is conducted ought to be subject to analysis, e.g. the dependency relations mentioned and the broad variety of jobs and work-sites.
3.3 Preview of Essays I-V

In the following sections, I briefly introduce the most central aspects of my five essays. It should be noted that these essays are intended to be published separately and to stand on their own. As a consequence, certain overlaps have been unavoidable. Some discrepancies between these essays may be noted as my views have evolved on several points throughout the course of writing this dissertation.

Essay I. “The Case for Ethical Technology Assessment (eTA)”

The first of the essays was written together with Sven Ove Hansson. This essay advocates an inclusion of ethical analysis in the well-established tradition of Technology Assessment (TA). Whereas traditional TA primarily aims at identifying adverse effects of novel technology at an early stage, eTA intends to bridge a ‘cultural lag’ that comes with new technology. By this is meant that, the time it takes for a technology to fully integrate in society - before a legal and normative framework have emerged. A principal task of eTA is to identify and characterize the ethical aspects of an emerging technology and to stage reasoned discussions on ethical dilemmas before the technology is too entrenched in society. Instead of pointing to the negative effects after the technology has been taken in use, ethical discussions should be part of the
design process where the chance of constructive reasoning lies. By addressing ethical issues, norms and values, at an early stage of the technological development and implementation, the gap may be bridged. Importantly, eTA should not be conducted from the perspective of one clear-cut normative position. Rather, nine groups of issues are set forth in the form of an ethical check-list, intended as a basis for assessment conduct; 1) Dissemination and use, 2) Control, influence and power, 3) Impact on social contact patterns, 4) Privacy, 5) Sustainability, 6) Human reproduction, 7) Gender, minorities and justice, 8) International relations and 9) Impact on human values.

This essay serves as the starting point for this thesis. The subsequent essays provide a limited assessment based on the entries “control, influence and power” and “privacy”. Importantly, the assessment is undertaken with the aim of contributing to an enhanced understanding of the meaning and significance of these aspects in relation to surveillance conduct.

Essay II. “Expectations of Privacy at Work – What is reasonable and why?”

The second essay introduces the investigation of privacy and the corner-stone of this dissertation; the concept of workers’ privacy. To the extent that privacy is discussed in a work setting, privacy claims are typically dealt with in the same way as they are in society at large i.e. in terms of informational privacy. Based on Beate Rössler’s triptych model of privacy in “The Value of Privacy”
(2005), I introduce a model of privacy suitable for the context of work. This essay explicates why workers’ privacy is important and why it should be protected. The main thrust is that privacy at work encompasses more aspects than what has traditionally been recognized in general privacy protection legislation. The circumstances in which individuals should be granted freedom from intrusion have typically been equated with the indisputably private domestic sphere. In consequence, privacy claims in the semi-public area of work have been overlooked. Here, the case is made that employees have reasonable expectations on privacy at work.

First, in a descriptive analysis, I provide some examples of actual reactions to privacy in the context of work. Second, I present a normative analysis to show why privacy is expected and the extent to which it should be protected. Arguments are given to the effect that employees need both informational privacy and local privacy. “Informational privacy” refers to the ability of employees to control certain aspects of themselves – to protect their personal data against unwanted access. “Local privacy” refers to the opportunities workers have to avoid observation by withdrawing to certain areas, and by using certain areas as if private. Employees need to control personal aspects and information so they can influence how others perceive them and to manage their relations with others. Moreover, workers need access to areas where they can relax from public exposure and observation. The way individuals define and express
themselves differs between private and public settings and seclusion is essential for employees to be able to prepare for their “public performance”. Workers’ privacy should be protected for the reason that we thereby secure personal autonomy. In essence, employees have a need to decide what to expose of themselves as well as when and to whom. By securing the two aspects of privacy, personal autonomy is protected. This explains why privacy should be protected.

The ambition in this essay is to provide a concept of privacy suitable for the context of work, recognizing the particular conditions that employees face.

Essay III. “Strengthening Employees’ Negotiating Power
– The importance of contextualized consent”.

Drawing on the meaning and value of workers’ privacy developed in the previous essay, in this essay I move on to investigate workers’ chances of securing this interest in employment negotiations. I assume that an increase in work-related surveillance will, to a larger extent than ever before, require job-applicants to negotiate their privacy interests during employment contracting. My starting point is the existence of a morally significant dependency asymmetry between the contracting parties i.e. between the employer and the current or prospective employee. In most cases the employees are in a rather weak position when advocating their privacy interests in employment
negotiations. Employers are typically in a better position to reach beneficial contracts with workers than *vice versa*. Arguably, this has bearing on the quality of employees’ consent. According to Jon Elster’s discussion on preference adaptation in “The Subversion of Rationality – Sour Grapes” (1985), preferences are conditioned on the extent to which these can be realized. Just as the fox in the fable discounted the grapes beyond his reach as being sour, individuals are likely to adjust their preferences to what they consider feasible. In employment negotiations this may mean that employees downplay their privacy interests because they seem unattainable. Given that consent normally functions as a criterion in morally acceptable contractual agreements, the dependency asymmetry gives us reason to pay attention to the quality of employee consent in employment negotiations. Importantly, a current or prospective employee’s *de facto* consent should not be sufficient for the moral acceptability of a contract. It is argued that conditions under which both parties’ consent to an employment contract may be considered morally acceptable should be established. A remedy is suggested based on John Rawls’s idea of background justice (Rawls, 1971). The case is made that fair conditions must be in place before the contracting parties’ consent can serve as a criterion of a morally justifiable employment contract.
Essay IV. “Is There Anything Wrong With Voluntary Slavery?”

Whereas the previous discussion concerned current or prospective employees’ chances of securing their privacy interests (the contractual procedure), this essay investigates what kind of contracts they should be free to enter and based on what (contractual content). In order to establish the extent to which current or prospective employees should be at liberty to enter contractual agreements, I start out from a libertarian case for individuals’ right to self-enslavement. Based on the libertarian principle of self-ownership, proponents of voluntary slavery argue that individuals should be at liberty to enter any contracts, even such that renounce basic liberties. In this essay, the libertarian arguments in favour of self-enslavement are used as a starting point for an analysis of morally permissible contractual content. By critically assessing the libertarian case for voluntary slavery a better understanding is reached of why we should treat liberty and privacy as non-waivable. Whereas proponents of voluntary slavery hold that all rational individuals should be allowed to carry out their autonomously chosen alternatives irrespective of content or consequences, an investigation of some of libertarian key-assumptions shows that the arguments offered in favour of voluntary slavery are inconsistent. Neither an orthodox Nozickian view, nor a modified notion of slavery provides us with convincing arguments for the acceptance of self-enslavement. Rather, proponents of voluntary contractual slavery must recast the notion of
self-ownership and adopt a broader view on liberty. Most importantly, they must consider that a slave aspirant may harm her future self by entering an irreversible contract. For those reasons, and since privacy is crucial for the protection of personal autonomy, individuals should not be at liberty to enter employment contracts in which their privacy is seriously impaired. They should not be allowed to waive their control over personal aspects that, now or in the future, may hinder them from managing their public persona and from influencing important relations like that to the employer.

**Essay V. “The Dimensions of Privacy”**

This essay is intended as an application, providing a tool for employers to reduce the privacy invasive nature of surveillance conduct. Since it was written at an early stage the reader will find the concept of privacy to differ somewhat from the notion of privacy suggested in essay II.

The starting point is that employees have reasonable expectations on privacy and that most surveillance practices are, under certain conditions, likely to constitute privacy invasions. While at times monitoring may be justified, restraints are required in order to safeguard employees’ reasonable expectations on privacy at work. It is shown how privacy intrusions may be avoided in cases where surveillance technology is to be implemented or when surveillance conduct is to be changed within a work-site. Seven factors of
importance for perceived privacy intrusiveness have been identified; Type, Purpose, Excess, Storage, Access, Awareness and Influence. This dimensional analysis is suggested as an instrument for assessing actual or potential surveillance devices and practices and the severity of privacy intrusions. It is proposed that by systematically trying to reduce the privacy intrusiveness of work-related surveillance in all these seven aspects, minimally intrusive means and ways of surveillance can be reached. In cases where surveillance capable technology cannot be avoided, its negative implications may at least be reduced. In most practical cases, the negative effects may be reduced along one or more of these dimensions and every reduction along one of the dimensions is to be considered an improvement.
4. A descriptive analysis of privacy

Having outlined the content of my dissertation briefly, I will next provide a broader framework for the discussion. In this section, I first sketch ways in which surveillance has been theorized. Then, I present some of the research on work-related surveillance practice and workers’ experiences thereof. Lastly, laws and codes relevant to the protection of employee privacy are outlined.

4.1. Surveillance at work

The social impacts of surveillance technology have been approached from several disciplines. Scholars within the fields of criminology, law, philosophy, social science, sociology and Science and Technology Studies (STS) have all been concerned with the social, legal and ethical implications of surveillance. In fact, as a reaction to the proliferation of surveillance, an entirely new discipline has emerged that is called “Surveillance studies”.\(^5\) Although work-related surveillance has attracted less attention than public surveillance,

\(^5\) For an illuminating discussion on the development and the focus of Surveillance studies, see David Lyon’s “Surveillance Studies – an overview” (2007).
important empirical research on work-related surveillance has been carried out within sociology.

In “Punishment and Discipline” (1964) Michel Foucault developed his highly influential theory on surveillance, that draws on Jeremy Bentham’s ideal prison the “Panopticon” in which inmates could be observed by a prison-guard without themselves noticing it – a condition that was taken to generate self-discipline. Panopticon would be arranged so to allow prison-guards to monitor all cells from a control tower without themselves being seen, shielded behind Venetian blinds (Bentham, 1787). In the same vein, covert modern surveillance technology was assumed to discipline individuals. Foucault himself used the panoptic metaphor to describe the disciplinary and normalizing power at work within factories and other institutions involving intensive assessments and observations of individuals. The influence of Foucault is reflected in how surveillance often is described as privacy invasive since those subjected to surveillance change their behaviour in order to conform to what they believe those monitoring their movements/actions will find acceptable or normal (cf. Goffman, 1966, Westin, 1967, Brannigan and Beier, 1985). In contrast to Foucault’s view of surveillance as a top-down type of control, the past decades have witnessed an increasing emphasis on assemblage aspects in the surveillance debate. Whereas Foucault used the panoptic logic to characterize a one-way type of surveillance, the rhizome
serves as a metaphor for the “surveillance assemblage” indicating the growth of a loosely integrated network of databases (Stalder and Lyon, in Lyon: 2003:91). In the work context, the assemblage would denote the multi-layered surveillance typical for a modern firm and an employer’s possibility to collect and collate work-related data and information about an employee’s private life. The panoptic model was abandoned for the reason that it does not account for interaction with and resistance to the technology.\(^6\) Approaching work-related surveillance, recent sociological research reveals how workers empower themselves through various social techniques, expressing a refusal to conform to imposed norms in cases where they disagree with the reasons for or modes of surveillance.

Several qualitative assessments have been undertaken on workers’ reactions to surveillance. Most of the studies have been carried out in call-centers i.e. confined work sites where employees typically work individually on well-defined tasks and are often subjected to rather extensive surveillance. Call-center work is described as stressful and repetitive (Wilson and Ball, 2000, Ball, 2001, 2003). In addition to the heavy workload employees conduct emotional labour. That is, call-center workers are typically expected to display certain emotions and to act in a cheerful manner regardless of the customer

---

\(^6\) It has been noted though, that the centralized “Big Brother” surveillance should not be viewed as entirely a thing of the past, supplanted by the assemblage (Stadler and Lyon in: Lyon, 2003:91).
response – something that itself may be psychologically straining (Merz Smith, 2004:59pp). The performance of call-centre workers is controlled by monitoring technologies that track and record their calls, measure the number of calls and the amount of time spent on each providing statistics on employee performance (Ball, 2003). Behavior intended to subvert or neutralize surveillance is typically identified where workers disapprove of surveillance (Marx, 1984). Among the reactions voiced in these surveys, call-center workers describe resisting the invasive nature of surveillance by making the work setting more relaxed and evading surveillance technology to create more breaks (Merz Smith, 2003:71).

Although these studies typically conclude that the work conditions cause burn out and high turnover rates, it is also contended that the technology must not by necessity be perceived as a threat and a way to subjugate employees. In cases where the employer’s goal is the social control of workers, one typically finds anxiety, stress and worker antipathy (Aiello and Kolb, 1995, Thompson and Ackroyd, 1995, Fairweather, 1999, Lankshear et al., 2001, Margulis, 2003). Studies of workers’ reactions to surveillance have also reported decreased social interaction among co-workers (Irving, Higgins and Safayeni, 1986) and adverse health effects (Lund, 1992). In some cases overly close surveillance have lead to aggression among workers e.g. when the U.S. Postal Service monitored workers’ bathroom visits (Day and Hamblin, 1964). That being
said, work-related surveillance can be considered acceptable by employees, when perceived of as a neutral means of assessing their productivity (OTA report, 1987) and in particular when aligned with goals that they accept (cf. Lankshear et al., 2001, Margulis, 2003). Depending on implementation and use, surveillance can allow for involvement and thus enhance employee participation in task design and assessment (cf. Thompson and Ackroyd, 1995). Several analyses of the technology and the labour process reveal that empowerment and disempowerment, skilling and deskilling, control and autonomy can coexist, depending on the context of the technology, the methods of its deployment, the gender of employees and the structure of the organization (Zureik, 2003:52).

4.2. The legal framework

The increased sophistication and accessibility of work-related surveillance have given rise to legal assessment. A rich plethora of international and national privacy protection codes and laws mirror this development, aiming at establishing that current and prospective employees’ privacy interests are adequately protected in employment negotiations. To the extent that the following essays refer to the existing legal framework, it is to European rather than North American jurisdiction. When suggesting ways of improvement, again these recommendations primarily address European legislation. In order
to canvass the differences in how privacy is framed and protected however, European privacy protection legislation will be contrasted with North American jurisdiction.

In Europe, workers enjoy protection both regarding contractual content and the form of employment contracting. Several European countries adopted data protection acts in the late 60s - early 70s in response to an increased computerization of archives of personal data. Furthermore, data protection regimes such as those laid down in the European Directive on Data Protection are typically morally and legally underpinned by reference to individual privacy rights. Information about an employee’s health status, sexual orientation, political opinion and religious affiliation are generally considered privacy sensitive and enjoy a rather strong protection (UN Declaration on Human Rights, article 8, 1948, International Labour Organization, ILO, 1993). The Fair Information Practice principles (FIPs) regulate the ways in which data may, legitimately, be collected, stored and transferred. The European Union’s constitutional values are those of “respect for human dignity, freedom, democracy, equality and the rule of law and respect for human rights of

---

persons belonging to minorities” and, it is stated that “every worker has the
group of "persons belonging to minorities” and, it is stated that “every worker has the
right to working conditions which respect his or her health, safety and
dignity”.

The International Labour Organization’s (ILO) sector-specific code
protects personal data in the context of work (The ILO code on Protection of
Workers’ Data, 1996). Although not legally binding, the ILO code is
internationally recognized and central for the protection of workers’ privacy
rights. And, in response to potentially privacy intrusive novel technology,
partial investigations have been undertaken as in the case of genetic
screening and at present, the assessment of Radio Frequency IDs.

In addition to restrictions regarding the content of contractual negotiations,
there are laws and codes directing the contractual procedure. Job applicants
are protected by employee representatives and by certain general principles.
For instance, countries like Austria, Belgium, Germany, The Netherlands,
Norway, Spain and Sweden have legislation that establishes worker councils to
protect workers’ privacy (Delbar et al., 2003:28). Furthermore, the ILO code
explicitly invalidates agreements in which individuals waive or trade off their
privacy rights. While collective agreements on the implementation and use of
surveillance technology are occasionally concluded at a national level, they
occur more often at the company level between local union representatives

---

10 See: [ww.rfideconsultation.eu](http://www.rfideconsultation.eu)
and management (either via agreements or through works councils or other employee representatives’ exercise of co-determination) (Delbar et al., 2003:23). Employees may also enjoy local support from company codes that recognize privacy claims. Furthermore, in contract law, good faith obligations prohibit the contracting parties from deliberately misleading or deceiving each other.

Whereas in Europe, and in particular in countries like Austria, Germany, Norway and Sweden, employers are obliged to comply with rather comprehensive data protection laws, workers in the US (and in many Third World countries) enjoy few legal privacy protections. In the absence of a general data protection legislation, workers’ privacy rights rely on an intricate network of statutory, common law, constitutional and voluntary provisions in the U.S. (Bennett in:. Hansson and Palm eds., 2005:84, Gellman in:. Nouwt (Eds), 2005).11 In accordance with the North American Employment at Will (EAW) tradition, the terms of employment, including privacy provisions, are typically negotiated between employer and employee. The contracting parties are considered perfectly symmetrical since both are equally at liberty to accept

11 Following legal scholar Anita Allen, North American common law protects privacy rights against four classes of injury; intrusion into seclusion or private affairs, public disclosure of embarrassing private facts, publication placing another in false light and the appropriation of name likeness and identity (Allen in:. Rössler, 2004:23). The term “privacy” means: limited access to information, confidentiality, secrecy, anonymity, and data protection (informational privacy), limited access to persons, possessions, and personal property (physical privacy), decision-making about sex, families, religion and health care (decisional privacy) and control over the attributes of personal identity (proprietary privacy) (Fourth Amendment Law and Fourteenth Amendment law) (Allen in:. Rössler, 2004:26).
and discard offers on the labour market and free to enter and quit contracts at their will (as long as the contract entered does not stipulate something else). In a cross-jurisdictional report on “Reasonable Expectations of Privacy” (covering the US, Canada and nine European countries), it is stated that the regulatory framework in the US often focuses on artefacts or techniques rather than the actual relation between employer and employee, an as a result, workplace privacy regulations are rendered too “technologically dependable” (Nouwt et al. 2005:341). In the North American legal system, the criterion “reasonable expectations of privacy” is used to assess the right to privacy.\footnote{The concept was first introduced in American case law in the light of the Fourth Amendment’s prohibition of “unreasonable searches and seizures”. In 1968, the Supreme Court, in \textit{Katz v. United States} held unconstitutional the federal authorities’ unwarranted placement of an interception device outside a public phone booth to record a phone conversation (Koops and Leenes, 2005:127-128).} A two-fold standard serves to establish whether a person has a reasonable expectation or not (Nouwt et al. 2005: 3). It is required that (1) she has an actual expectation of privacy in a certain situation and that (2) society recognizes this expectation as objectively reasonable. In brief, this means that in a situation where surveillance is already in place, privacy expectations are unreasonable. And, in virtue of being the owners of the work site and its resources, employers are free to dictate conditions that concern their property. Clearly, this system leaves little space for privacy at work since employers are free to decide how the resources that employees often use for private purposes such as computers and telephones should be used (Levin, 2005). In contrast,
Article 8 of the ECHR 1950 specifies that where privacy intrusive measures are necessary to protect public interests, the criteria of legitimacy, subsidiarity and proportionality should apply. I will leave the question of reasonableness for now however, returning to this issue in the normative discussion.
5. A normative analysis of privacy

We have now considered how surveillance may influence individuals in the context of work as well as factors that may affect their acceptance of or resistance to such conduct. In the following, I will suggest a concept of privacy suitable for the context of work. In brief, the value, range and scope of privacy will be investigated in connection to work. As a basis, three influential discussions on different aspects of privacy will be used. These are (1) Beate Rössler’s investigation of the value of privacy (2005), (2) Helen Nissenbaum’s discussion on contextual integrity and (3) Priscilla Regan’s pragmatic argument that privacy should be legally coded as a social rather than individual good.

5.1. The value of privacy

Undoubtedly, privacy is one of the moral issues most frequently analyzed in relation to surveillance. Still, in spite of a longstanding discussion on how to understand privacy, on a theoretical level, little unity is to be found. The lack of unity can be traced to the complexity of the term “private”. It can be attributed to actions, situations, states of affairs and states of mind (Rössler,
The notion of privacy can be described in terms of limited access to persons, relations, personal property, spaces, information and communication. It can regard decision-making about sex, families, religion and health-care and control over attributes of personal identity.

Rather than trying to identify one category of personal information that is inherently private, it seems more promising to focus on why privacy is important and on ways of protecting this value. The way in which I frame the value of workers’ privacy draws, to a large extent, on Beate Rössler’s conceptualization of privacy in “The Value of Privacy” (2005). Apart from Ferdinand Schoemann’s anthology “Philosophical Dimensions of Privacy” (1984), Rössler’s contribution is the most thoroughgoing philosophical analysis of the meaning and value of privacy. She argues that privacy, in liberal societies, is valued for the sake of individual liberty and autonomy. Unless privacy is secured, individuals are unable to develop themselves in accordance with their own chosen life-plans (however rough and imprecise these might be) towards a life that is personally rewarding (Rössler, 2005:44). A most significant feature of privacy, it is argued, is that of the individual’s chances to control certain aspects about herself. Individuals should be able to control both “direct physical admission to spaces” and “a metaphorical access to their personhood”. Moreover, that which should be protected as private is separated in three different aspects: (1) local privacy, (2) decisional privacy and...
(3) informational privacy. More precisely, privacy is the spatial and intellectual sphere that enables individuals to decide over matters that concern them, to control who has access over information about themselves (both direct sensory access and stored data) and to establish and develop different types of relations. Privacy intrusions are defined as unwarranted intrusion in to: the private realm, personal decisions and personal data respectively (Rössler, 2005:44).

On this basis, I argue that privacy at work consists of (at least) two different aspects; “informational privacy” and “local privacy” and that both these aspects should be protected in order to sufficiently accommodate an employee’s need for privacy, and thus, autonomy. By informational privacy I understand an employee’s chance of controlling and restricting certain aspects about herself, both socially stigmatizing data and information that the individual herself consider privacy sensitive. The type of information concerned may range from information about the content of the worker’s computer screen to genetic data. Importantly, the worker needs to control her self-representation and to be able to compartmentalize certain aspects of herself. Control over personal aspects is necessary for workers to govern their persona and the various roles they hold in relation to customers, colleagues and managers.
Local privacy concerns a worker’s ability to withdraw from public gaze, to be to herself and to, at times, carry out certain work tasks in private. Moreover, it refers to the employee’s ability to influence her physical workspace in terms of choosing and/or personalizing her work-station, and to control personal belongings kept in the workspace and work tools (cf. Brey in: Hansson and Palm, 2005). It may concern freedom from revealing one’s position at all times as can be done by means of RFID or GPS.

Importantly, privacy is not everything that is private or secret but that which is related to autonomy. Informational and local privacy are important for the reason that they allow employees to form and enact their own goals and express their identity and values. Arguably, workers’ privacy should be protected for the sake of personal autonomy i.e. the various ways in which an individual can play a governing role in her own actions. The acts of deciding what to reveal of oneself to others, compartmentalizing information, creating personal space, influencing relationships and surroundings – are all expressions of self-government.

The argument that privacy should be protected for the reason of autonomy may seem somewhat puzzling in a context where individuals typically surrender parts of their discretionary power to the employer when entering a position. The absence of individual control is typically a prerequisite for an employment relationship to come into existence. This is my reason for not
stressing Rössler’s third dimension, decisional privacy, in the context of work. But even if workers cannot be granted full freedom to decide in all matters that concern them, there is still room for them to influence and control their person and situation. If we cannot influence how others perceive us by limiting the disclosure and dissemination of data concerning ourselves, we have lost a great measure of our ability to make meaningful decisions. The case has been made that such control is particularly important in a relationship between an individual and an organization since workers could unwittingly experience a loss of autonomy that might result from decisions made about them on the basis of e.g. collected data. Even if not directly harmed, an individual could be wronged in the process (Alpert, 2003:303).

In order to further strengthen the case for privacy as grounded in autonomy, we will consider two frequently met alternative positions. Apart from the proposed understanding, the value of privacy has foremost been identified as intimacy (cf. Gerstein, 1978, Inness, 1994, Cohen, 2002) and dignity (cf. Bloustein, 1964, Levin, 2005). Julie C Inness has suggested that the core of privacy should be understood in terms of “intimacy” (Inness, 1994). Following her, what we perceive of as privacy sensitive is typically motivated by an intimate concern or somehow tied to intimate relations, love or care. But although intimacy may be an important part of what we define as private and privacy sensitive, it does not necessarily cover all of it. A person may wish to
keep her political views to herself - an interest that typically is viewed as a matter of privacy - but it does not have much to do with privacy. Employees may find drafts of work documents a private matter but not because these are motivated by intimacy, love or care (at least not if care is understood in a stronger sense than as the opposite of indifference). Certainly, the employee might experience a greater privacy intrusion if her love letters were openly distributed among her colleagues than if her drafts of work documents would be so. Nevertheless, the latter may be a private matter to her. Inness’ way of anchoring privacy would only be capable of explaining why traditionally recognized privacy sensitive data should be protected, leaving aside several aspects of informational privacy and, in particular, local privacy. This approach does not accommodate privacy expectations in professional contexts and relations.

The second suggestion is that privacy should be framed as founded on dignity rather than on liberty (Bloustein, 1964, Koops and Leenes, 2005, Levin, 2005). As pointed out by Levin, dignity is first and foremost seen as a social value, conceptually distinct from other values that privacy may protect, such as an individual’s liberty. A common reason for advocating dignity as a fundamental value seems to be that privacy, in the North American context, has become intimately connected with property rights and negative liberty. A shift of focus would mean the possibility of starting anew.
True, in North America, privacy has been associated with individual interests like liberty and property rights. In terms of conceptual clarity however, nothing is gained from replacing autonomy with dignity (Bloustein himself admits that the concept is somewhat vague). Dignity seems to concern how individuals behave and respond to certain circumstances. An employee may adjust to excessive surveillance or other forms of exploitation with dignity i.e. in a certain manner. Whereas an employee can maintain her dignity during continuous aggressive surveillance, her autonomy would be seriously impaired. In my view, anchoring privacy in autonomy is preferable for reasons of explanatory force. Moreover, the understanding I propose, detaches privacy from places and property and stresses that privacy is a collective interest as well (see below).

An advantage with the proposed autonomy-based privacy concept is that it combines elements from the two most frequently met approaches in the privacy discourse. Broadly speaking, and although a difference of emphasis rather than of kind, two significant approaches can be extracted; privacy can either be understood in terms of separation or in terms of control. Whereas, “separatists” tend to describe privacy in terms of a right to be left alone and in terms of seclusion (e.g. Westin, 1967:7), “control advocates” emphasize the importance of the individual’s ability to control information about herself as well as others peoples’ access to certain aspects of her (e.g. Fried, 1984:209).
Both these views stress important aspects of privacy. Instead of choosing side, I emphasize both as important components of privacy. Importantly, the autonomy-based theory can handle that we, in many cases, do not want to be left alone or secluded, but still we want to be able to claim privacy.¹

What then is the scope of privacy? I suggest that “private” can apply to actions and decisions irrespective of where these take place. Just like the act of voting is considered a highly private matter even if it takes place in the public realm, a worker could for instance expect privacy regarding certain e-mail and telephone communications while at work although such acts are not conventionally held to be private. Importantly, which things we consider private and rightfully private are based on social constructions and the conventional view of privacy as belonging only to the traditionally private sphere and not to the semi-public area of work needs to be challenged. With Rössler I argue that, rather than understanding particular realms or spaces as private, dimensions of an individual’s actions and interests can be private (Rössler in: Rössler (Ed), 2004:7).

¹ For a promising way of combining these aspects see the Restricted Access/Limited Control – RALC-theory recently proposed by Moor and Tavani (Moor 2004, Tavani, 2007).
5.2 Privacy in public

That claims of privacy and autonomy are typically viewed as practically impossible or unreasonable in the context of work can be explained by reference to a public - private split. A distinction between a public and a private sphere has influenced much of our thinking and reasoning about human behaviour and institutions. The ancient Greek distinction between a public sphere synonymous with the political realm and a private sphere equivalent to the domestic area still influences how we frame the concept of privacy (cf. Regan, 1995, Nissenbaum, 1998). The distinction also informs the differences between state and non-state actors and between public good and private property. However, such a split between the public and the private has been unfortunate for the understanding of privacy. It is a common misconception that privacy is a reasonable claim only or at least primarily in obviously private domains such as an individual’s home. Outside this indisputably private domain, privacy expectations are held reasonable in certain relations either of an intimate (cf. Gerstein, 1978, Inness, 1994) or institutionalized kind as between doctor and patient. Both Priscilla Regan (1996:32) and Helen Nissenbaum (1998:568) have discussed the unfortunate

---

2 The significance of the public - private divide in Ancient Greece is reflected in the word “idiotes” – the origin of “idiot. Being a free man would require active participation in public matters such as voting on issues before the assembly. Those working on their own household rather than for the common good would be considered irrational and labelled “idiotes”. See: Liddell-Scott-Jones A Greek-English Lexicon.
consequences of framing privacy as something that primarily belongs to privately owned domains. For example, such a narrow understanding leads to the result that privacy is typically considered more reasonable in (and related to) the domestic sphere than in the public sphere. "For the majority of theorists, it follows seamlessly that the concept and the value of privacy corresponds with, or applies to, the sphere of the private alone" (Nissenbaum, 1998:568). In effect, an employee’s claims on privacy in the semi-public domain of work are not likely to be properly recognized. This sharp dichotomy obscures how people operate in a range of contexts where they are more or less private (Regan, 1996:32). Arguably, the semi-public realm of work is one such example and a brief description of the computerized work site will serve to highlight the problems of such a construct. Surveillance technology like video surveillance, computer monitoring, location positioning and biometric measures may blur the distinction between individuals work role and aspects of their private life. Work tasks can be carried out both in public and private settings as conventionally conceived. Whereas taxi drivers typically operate in the public space, health care workers may assist patients in their homes and, equipped with company laptops, professionals such as clerks may, temporarily, conduct work in locations other than the office - even in the obviously private realms of their own homes. An increased usage of wireless communication enables workers to undertake work assignments while
traveling by air or train, and while transporting themselves to and from work. The possibility of carrying out computer and Internet-based work virtually anywhere and anytime serves to dissolving the borders between public and private and between work and leisure time as traditionally understood.\(^3\)

Moreover, drawing a clear border between public and private becomes extraordinarily difficult with regard to relations between colleagues and business contacts. Even if these contacts may be established in a professional setting, the actual relationships may be of a private nature. The domain of work also contains private elements in that employees keep personal belongings in drawers and lockers, and they may personalize their work-station with pots, plants and images (Brey in: Hansson and Palm, 2005). For these reasons, a conceptualization of the worksite as a public area in contrast to the private domestic sphere is untenable and should be avoided. Hence, the term “workspace” seems more appropriate than the commonly used term “workplace”. The former includes work executed in a fixed location, labour carried out by a mobile workforce and work temporarily conducted in areas other than the main worksite. At times, the traditionally private context - the domestic sphere - may be the worksite.

Even though privacy in public is generally insufficiently accommodated, to some extent, privacy at work has been recognized in European case law. In the

\(^3\) See: http://www.ict-barometer.nl/rapporten.php.
case *Niemitz vs Germany* (ECHR, 1992) it was acknowledged that all relations established in the premises of work may not be strictly professional and hence, that interpersonal relations should be free from inspection. In 1997 the European Court of Human Rights ruled that workers have a reasonable expectation of privacy in making and receiving phone calls at work, which can be applied to electronic communication as well (ECHR, 1997). Although not a work-related case, *von Hannover vs Germany* (ECHR, 2004) states that a public person has a reasonable expectation of privacy in public and not only regarding obviously socially stigmatizing data. These cases may indicate an erosion of the sharp public private split.

It was first suggested that the private is applicable to actions and decisions irrespective of where these take place. Then it was shown that the public – private divide is practically untenable and that it should not serve to distinguish legitimate privacy claims. Individuals need privacy in order to act on the public stage i.e. in situations where they are exposed to others. An understanding of privacy that accommodates individuals’ need for privacy in public (exposure) is found in Helen Nissenbaum’s discussion on privacy as

---


5 Some have interpreted these cases as the beginning of a third generation of data protection law. Whereas the first generation of data protection acts (1960s) has a clear technology focus i.e. the computerized data procession, the second generation that came as a reaction to the proliferation of personal computers, stressed individual self-determination rather than regulating the technology. Now, the passing of the 1997 German *Telekommunikationsdatenschutzgesetz* has been seen as a new era within privacy protection law www.dataprotection.eu.
contextual integrity (1998, 2003). In the following, Nissenbaum’s contextualized understanding of privacy is presented and applied to the context of work.  

In “Protecting Privacy in an Information Age” (1998) she questions the two frequently made assumptions that (1) “there is a realm of public information in which no privacy norms apply” and (2) that “an aggregate of information does not violate privacy if its parts, taken individually, do not” (Nissenbaum 1998:455,458). Whereas traditional approaches to privacy yield unsatisfactory conclusions regarding public surveillance and fail to address how information and communication technology (ICT) has blurred borders between public and private, contextual integrity is suggested as a means to better capture such challenges. Most importantly, computerized data-collection enables combinations of data stated in various contexts. Although an individual may have stated personal information in an informed manner in each single case she may not approve of the combined effects of such data in compilation. Following Nissenbaum, the context in which information is stated, the capacities in which the individuals sending and receiving the information are acting, the types of data involved and the “principle of transmission” should

---

6 Although the moral implications of the public – private divide have been recognized by several scholars, Helen Nissenbaum was one of the first philosophers to pin-point the problem and her theory on contextual integrity has proven to be most influential - not least since it has lent itself to practical application i.e. her “principle of transmission” has been translated in computer programs. See: http://www.economist.com/science/displaystory.cfm?story_id=8486072.
be considered. That is, information may be transferred in the course of a commercial exchange, as an expression of intimacy, or in response to a formal legal request - these are all examples of transmission principles (Nissenbaum, 2003). At the base of this approach lies a view of society as consisting of several spheres, each governed by its internal norms and principles. An adequate privacy protection requires that the norms of specific contexts are respected and that information gathering and dissemination is appropriate to that particular context.

Applied to work, the contextualized approach would require a greater sensitivity to the broad variety of work settings and types of work and the concomitant flora of needs and claims. That employees, at times, act in another capacity than the professional while at work must also be recognized. Although two types of privacy have been identified as in need of protection - informational privacy and local privacy - exactly what these include cannot be stated. Rather, the particular work context will influence what workers consider privacy sensitive and not. Work can be creative or uninspiring, rewarding or straining, alienating or empowering, conducted within a large- or small scale firm, in a team or solitary. These features, as well as, for instance an employee’s position within the firm, gender or ethnicity may influence her
perception of surveillance and expectations of privacy. Furthermore, privacy expectations are likely to vary with the context in which work is carried out, between on-line and off-line activities and when conducting one’s work assignments at home and at work etc. Although we may be able to identify certain general features of privacy sensitivity and privacy invasiveness, an exhaustive list could not be accomplished (at least not without substantial effort). Certain aspects become privacy sensitive due to the physical work site and to particular relations at work.

The kind of privacy that I have advocated is not tied to private domains or ownership but to persons and relations, and in that way, it avoids some of the problems that privacy normally is associated with. However, it remains to develop norms and principles that can govern privacy at work.

5.3 Privacy as a social good

Moving on to the third component, “privacy as a social good”, the issue at hand concerns how a worker’s privacy is best protected. The case will be made that even if an employee’s privacy is valuable for the reason that it secures and enhances personal autonomy, this does not exclude the possibility that privacy is also a social good. Nor does it exclude the fact that it is best protected when

---

7A similar perspective has been suggested by Moor and Tavani, arguing that the setting always decides whether personal information is perceived of as privacy sensitive, not the information per se. (Tavani, 2007:15).
legally coded as a communal interest. Inspired by Priscilla Regan’s (1995) pragmatic argument in favour of a legal coding of privacy as a social good, I suggest that a worker's privacy should be recognized as a collective interest as well. Regan exemplifies how the traditional framing of privacy as an individual interest has been inefficient. The alternative is to emphasize that people have a shared interest in privacy and in a right to privacy, and that privacy is socially valuable because it supports and is supported by a democratic political system (Regan, 1995:213). So far (to the best of my knowledge), privacy is legally coded as a communal value only in German legislation. The German legislation stipulates that;

“The right to informational self-determination is incompatible with a social and legal order in which citizens cannot know anymore who knows what, when, and under which circumstances about them. Anyone who is unsure whether deviant behaviour will be permanently stored, used, or circulated, will shy away from such behaviour. If a person has to reckon that his participation in an assemblage or citizens' action committee will be recorded by public authorities, he/she may abstain from using his respective fundamental rights (Art. 8, 9 of the Basic Act). This would not only negatively affect the individual developing opportunities of single individuals, but also the common welfare, because informational self-determination is a basic functional requirement of a free and democratic social order based on the ability of its citizens to take action and participate” (Translated from Bundesverfassungsgericht, Amtliche Sammlung, Vol 65, 1).
Importantly, this perspective serves to strengthen privacy in that privacy rights should be respected regardless of whether that claim is made or not. As will be seen in the following section on “reasonable expectations”, workers’ privacy is also strengthened in relation to the main rivals; ownership, safety and efficiency.

From a human resource perspective, employers may also be interested in securing a certain amount of privacy at work for their employees. It has been argued that employers should grant employees privacy in order to prevent long-term negative effects on individual wellbeing, social cohesion and trust (Fairweather, 1999, Brey, 2003, Introna, 2003). If allowed more control over the pace of work and more breaks to manage stress; workers may be more productive and less likely to burn out (Buchanan and Koch-Schulte, 2000). Moreover, the usage of methods of surveillance in personal selection procedures may also be of interest to employers. If specific procedures are perceived of as invasive, individuals who are sensitive to privacy issues may not apply for openings in organizations that use such procedures. As a result, organizations may find themselves facing decreasing numbers of suitable job-applicants, resulting in unfavourable selection ratios (Stone-Romero, Stone and Hyatt, 2003:347). Furthermore, Gary T. Marx argues that there are good reasons to expect unrestrained monitoring to be counter-productive. A 1993 World Labor Report claims that "...stress costs American employers $200
billion a year through increased absenteeism, diminished productivity, higher compensation claims, rising health insurance fees and additional medical expenses”. Marx contends that whatever the actual figures are, we must ask ourselves what the causal structure looks like. It is far too easy to assume that monitoring always is a response, rather than also a cause, of some of these problems (Marx, 1999).

5.4. Reasonable expectations of privacy from a moral perspective

Having seen why privacy is important in the context of work and why it should be protected, we will now discuss (1) how privacy should be balanced against competing claims like those of efficiency and safety and (2) employees’ chances of securing privacy claims in employment negotiations.

An employee’s privacy expectations in relation to an employer are typically complicated by the fact that employers and managers, for several reasons, must require data from the employee and exercise a certain amount of control over her doings. As we have seen, the employers are responsible for the health and safety of their workers and often also of third parties. This may motivate a certain amount of data collection about current or prospective employees. The information requested may at times be potentially privacy sensitive. An additional incentive for employers to conduct surveillance is of course their
interest in running their businesses efficiently. As previously explained, in North American jurisdiction, what qualifies as a reasonable expectation of privacy depends on the actual conditions for privacy. It is dependent on (1) whether the employee has actual expectations i.e. if the actual circumstances admit of privacy or not and (2) if her expectations are socially recognized as objectively reasonable. These criteria are clad with (at least) two problems. The first criterion accepts privacy expectations as reasonable if practically feasible and is therefore sensitive to the increasing use of automated surveillance. In the face of technical developments reasonable expectations of privacy erode (Nouwt et al., 2005: 352-353, Tunick 2000, MacArthur, 2001).8 Second, it is assumed that those engaged in criminal activity can anticipate the police’s attention and hence, have lower privacy expectations, without stating what the law-abiding majority can expect. Applied to the context of work, this understanding would mean that workers have reasonable expectations of privacy to the extent that the employer’s policy allows (Nouwt et al., 2005: 352-353). As a consequence, privacy is subject to easy change. Arguably, reasonableness should not be conditioned on either actual surveillance practice or property. If de facto surveillance practice would be the norm, we might have to accept the zero privacy scenarios depicted in dystopias like 1984 (Orwell,

---

8 In practice, privacy is primarily used to protect decisional and proprietary interests. Privacy of communication like e-mail, business transactions and medical records are some of the aspects that Allen identify as insufficiently protected by American legislation (Allen in.: Rössler, 2004:27).
1949) and Kallocain (Boye, 1949). Privacy regulation should have social relations as its focus rather than special places, objects or technologies. In contrast to the juridical understanding above drawing on actual conditions, in the following an attempt will be made to identify privacy expectations that are reasonable irrespective of actual policies regarding surveillance or surveillance practice. That is, “reasonableness” will be used in a normative sense.⁹

In European privacy legislation, the criteria of legality, legitimacy, subsidiarity and proportionality (EHCR) are of central importance to balance conflicting but reasonable claims such as safety and privacy. In the following however, I will suggest a way of assessing the moral status of the claims, drawing on a Neo-Kantian understanding of “reasonableness”. More precisely, I will suggest an understanding of reasonableness based on John Rawls' and Thomas Scanlon’s contractualism.

The Kantian heritage is manifest in both theories according to which the moral agent is both reasonable and rational (Rawls, 1993:50, 2001:6-7, Scanlon, 1998:32-33,191-197). Both theories safeguard personal autonomy and the emphasis on individuals as rational and reasonable has a parallel in Kant’s categorical and hypothetical imperative where reasonableness has priority over the rational. That is, individuals are not only capable of identifying the best

---

⁹ These criteria are also embedded in the fair information processing standards set by EC Directives and implemented in national data-protection legislation in the EU member states (Koops and Leenes, 2005).
ways of obtaining their goals, they are also reasonable in the sense that they recognize that under certain circumstances, morality requires that they impose restrictions on themselves and on their personal advancement. Hence, they are morally required to take the effects of their actions on other persons and their interests into account. Following Scanlon, due to their reasonableness, moral agents are concerned with identifying principles that no reasonable and rational individual could have reason to object to. In order to reach a contractual agreement justifiable to all, the contractors realize that morality may require of them not to act on the alternatives that would best promote their personal interests. One would be unreasonable by not giving weight to other peoples’ moral claims. Most importantly, one is required to take the interest of others into account irrespective of whether these are explicated or not (Scanlon, 1998).

That is, individuals have the capacity to identify the needs and interests of others and hence, the responsibility of doing so. Given the significance of privacy for self-government, workers are justified in expecting privacy at work, just like in other areas of society. In cases where their interests in privacy collide with employers’ interests in efficiency and safety, both sides are obliged to provide each other with generally acceptable reasons, i.e. arguments that rational and reasonable others could not have reason to object to. Most significantly, the Neo-Kantian understanding of reasonableness prevents
efficiency- and safety claims from trumping workers’ privacy interests as traditionally has been the case.

5.5 Securing privacy - the contractual procedure and content

Moving on, we will now consider employees chances of securing their privacy interests at work. As a result of the increase in work-related surveillance, job-applicants (and employees re-negotiating work conditions) are forced to try to secure their privacy interests in employment negotiations to a much larger extent than was previously the case. Since the ways in which surveillance will be conducted are typically stipulated in the employment contract, the conditions under which contractual agreements can be considered morally acceptable deserve attention. Arguably, the previously mentioned dependency asymmetry between the contractors is morally significant. The employee or applicant is typically disadvantaged when it comes to advocating her interests. Although some workers may be in a strong position *vis à vis* the employer at times, this is not the case for workers in general (cf. Bagchi, 2003:1885). Due to this dependency asymmetry, prospective employees are likely to trade away more of their privacy claims than what is in their reasonable interest (cf. Miller and Weckert, 2000, Hoeren and Eustergerling, in: Nouwt *et al.*, 2005:226-227 Phillips in: Nouwt *et al.*, 2005:60). That is, job-applicants may accept worse
work conditions than they would have had the circumstances under which they negotiate been more favourable to them.

In addition to the legal support enjoyed by the contracting parties in employment negotiations (see p. 25-27), stronger restrictions are needed regarding both the contractual procedure and contractual content in order to balance the previously discussed dependency asymmetry.

Most often, consent is used, implicitly or explicitly, as a criterion of the moral acceptability of contractual agreements. Although it is seldom disputed that consent, in order to be meaningful, should be given without coercion, the definition and boundaries of coercion are often subject to disagreement. While some types of coercion are obvious, there are less recognizable forms which we need to be aware of. Some would take consent to secure moral acceptability as long as it has not been stated under direct force, fraud or manipulation and that the rights of others have not been adversely affected thereby. Others would require that consent should not only be stated in the absence of force but also in the absence of undue influence. In many practical cases, as long as the individuals concerned have consented to a certain conduct, they are assumed to have chosen this particular alternative out of their own free will. A common mistake is to assume that an individual’s *de facto* choice is an expression of consent (Peter, 2004:3) thus securing voluntariness. Ian Maitland for instance, argues that prevailing employment contracts should
be considered voluntary since the contracting parties are not only “[f]ree to take or leave the rules provided by the law, but also nothing prevents them from choosing not to contract with a corporation, at all, or from limiting their business to other types of business organization” (Maitland 2001:132). On this view, prevailing contracts are those that the contracting parties have preferred over others. Although, in most cases less explicitly stated, the relation between contractual consent and legitimacy is often present in economic reasoning (Peter, 2004:5). My point here is not that, in order for an individual’s consent to be meaningful, they must have a certain number of alternatives available, but rather that the situation in which they give their consent should be fair.

The context in which individuals consent is of importance for the moral standard of the resulting agreement, and Jon Elster’s discussion on preference adaptation will be used to illustrate the significance of the contracting context (Elster, 1985). Following Elster, an individual’s preferences and the choices that she makes are likely to be conditioned on the degree to which she considers her alternatives attainable. Elster takes his starting point in the fable of the fox who, when facing grapes beyond his reach, convinces himself that the grapes would be sour anyhow. The fable serves to illustrate that the set of alternatives that we believe to be open to us shapes our preferences. The fox does not want the grapes because he cannot reach them. Elster does not say that individuals have other and more authentic preferences than those
expressed by their consent. The point is rather that we ought to consider, not only what preferences individuals have with regard to privacy but why they have them. An individual is not free to act just because there are a great many alternatives open to her – she must also value and (autonomously) want these options in order to be free in a meaningful sense. In a situation where job-applicants face few attractive alternative position and where the competition is hard, they may be tempted to downgrade their privacy claims in order to secure a position. The lower degree of education and work experience the job-applicant has, the more likely such trade-offs are. That being said, there are reasons to consider workers’ privacy a potential sour grape i.e. as given up because seemingly unattainable.

The tendency to confuse choice and consent facilitates a legitimization of almost any contractual agreements. For instance, legitimacy may be given to employment contracts where job applicants have agreed to work under severely privacy-intrusive conditions. The situation framing the contractual process and the context in which individuals consent is given significantly affects the moral standard of the resulting agreement. However, in order for consent to make up an adequate criterion on the moral status of contractual agreements, more is required. The contract may be voluntarily entered (in the absence of explicit or implicit force) and in that sense the contracting process may be morally acceptable. Still, the content thereof may be demeaning and
exploitative. For this reason I suggest that both the contractual procedure and the content should be considered. The International Labour Organization (ILO) discards contracts in which employees waive their privacy rights. However, from a moral perspective, it should be further emphasized that individuals should not be at liberty to enter employment contracts in which their privacy is seriously impaired. That is, they should not be allowed to waive their control over personal aspects that, now or in the future, may hinder them from managing their public persona and from influencing important relations like that to the employer.

In the following section, the contractualist perspective will also be used to suggest fair conditions for employment negotiations, including both contractual form and content. A probe for fair terms of contracting will be suggested.
6. A theoretical framework for fair contracting

Let us now return to the contractualist approach. When searching for a theoretical framework within which the concepts of privacy and consent may be further developed, contractualism seems to be a suitable normative starting point. In a Kantian vein, contractualists emphasize the importance of consent. To the extent that individuals’ consent in matters that concern them has not been sought, they are not sufficiently respected as autonomous agents and their rights are not treated as ends in themselves. Following Rawls, in order for consent to be meaningful, the individual should not only consent to a particular course of conduct, but also approve of the structural framework within which she is making her choice, since that has an impact on the alternatives from which she is choosing. Even if individuals make a choice between given alternatives they may not necessarily have consented to the set of alternatives. In Rawlsian terms, a certain background justice is required for individuals’ consent to be meaningful (Rawls, 1971:83-90). The moral agent must recognize the framework in which she expresses consent and she must
accept the constraints that have shaped the set of alternatives that she faces (Rawls, 1971). In brief, this approach shows why de facto consent is insufficient, raising demands on the contracting situation. It requires acceptable background conditions - equal and fair terms. The suggested criterion on reasonableness serves both to “correct” preference formation in a long-term perspective and to secure the individual contract.

Although fair procedure is necessary for the moral acceptability of an individual’s consent, it is insufficient for an employment contract to be morally justifiable. Hence, the requirement of an acceptable basic structure will be accompanied with an obligation specified by Thomas Scanlon in “What We Owe to Each Other” (1998). Once acceptable background conditions are in place, Scanlon argues, it is necessary that individuals take each other’s reasonable interests into consideration and justify acts that affect the other with reasons that no rational and reasonable person could object to. Scanlon focuses on an interpersonal form of contracting where the aim is that of spelling out the principles that should regulate individuals’ conduct (Scanlon, 1998:228). Although, Rawls and Scanlon both derive certain standards from the starting point of the moral agent understood as both rational and reasonable, these theories operate on different levels. Scanlon’s contract does not, like Rawls’, only occur in a pre-society but rather reoccurs perpetually in society.
Taken together, against the background of fair basic conditions, Scanlon’s theory provides a good tool for identifying responsibilities between employer and employee and gives weight to moral claims such as that on privacy in the context of work. It challenges the “economic man perspective” which both implicitly and explicitly comes out in most reasoning on contractual consent. Whereas the employment contracting process is often considered a self-interested bargaining process, Scanlon emphasizes a moral obligation to take others’ interests into account – a shared responsibility. Although the individual’s consent to a certain condition or conduct is of importance, it is not sufficient in the sense that it would free others from responsibilities. Principles that individuals reasonably could not object to should be respected whether explicitly claimed or not. In this light, privacy is taken to be an interest that should be respected whether claimed or not since a general respect for privacy is essential for individuals to establish relations and to enhance their self-understanding. In this sense, privacy is a precondition for autonomous acts. Without an assurance that we are entitled to keep certain aspects of ourselves private, our self-understanding would be fundamentally altered. By respecting other individuals’ needs for privacy we respect their value as persons. According to Scanlon, if we pursue ends that affect people who disapprove of those ends, those persons would simply be treated as means to ends (Scanlon, 1988:154).
The above is not a suggestion for a normative framework for ethical technology assessment (eTA) in general but for the confined task of further explicating the central issues generated by this assessment of work-related surveillance. In Essay I, I stated that an ethical technology assessment should not initially be conducted on the basis of one particular normative theory but rather that tools should be borrowed from several such theories. A lot remains to be done in order to fully spell out the conditions under which workspace surveillance can be morally acceptable. In taking on that task, contractualism seems to offer a suitable framework.
7. Issues for further research

This thesis is in no way seeking, nor claiming, to give an exhaustive account of the ethical issues attached to privacy in the area of work. For reasons of space and focal clarity, several aspects relevant to this discussion have been left to the side. In the final sections I will briefly point to some of the issues that merit discussion within this discourse but which could not be encompassed fully in this thesis.

Throughout my thesis, privacy has been understood as a positive value – a necessary condition for the fundamental value of personal autonomy. Furthermore, privacy has been framed as a social good. It should be noticed however, that privacy also may further anti-social ends. The case has been made that by assuring individuals privacy in the form of freedom from observation they may engage in subversive conduct. From a feminist perspective, it has been argued that the special status ascribed to privacy can be detrimental for women and children because it can serve to control and silence them and to cover up abuse (cf. MacKinnon, 1989). This critique
however, relies on the traditional divide between a private and a public sphere and expresses a property based approach. That is, individuals are considered at liberty to do more or less whatever they want within the domestic realm. The type of privacy I defend, however, does not connect privacy to a certain sphere where unrestricted freedom is allowed. Rather, I emphasize the responsibility for individuals to take the interest of others into consideration.

Another question that requires analysis is that of equality and the importance of fair allocation of surveillance. Equality is an ethical issue closely linked to privacy that merits attention. Convincing arguments have been made to the effect that individuals value privacy and fair treatment in work organizations. Methods of observation or measurement that violate expectations of privacy are considered unfair by workers and beliefs about privacy and fairness are strongly correlated with one another (Stone-Romero, Stone and Hyatt, 2003). When individuals believe that they are being treated unfairly by a work organization (e.g. that their privacy has been invaded by an organization), they will be less prone to accept job offers from the organization, more likely to quit jobs in such an organization, and less likely to exhibit a number of organizational citizenship behaviours (cf. Folger and Cropanziano, 1998). Social class is another aspect of equality worth mentioning. Although the case has been made that computerized surveillance can have a democratizing effect (Rogerson and Prior in Hansson and Palm,
2005), surveillance seems more likely at the conveyor belt than in the offices of directors. As already mentioned, the level of education and work experience typically influence an individual’s chances of obtaining a surveillance-free position.
8. Conclusions

This analysis was motivated by the potentially negative social and ethical implications of surveillance at work. Although the ethical implications of workspace surveillance are more problematic than those of public surveillance, work-related surveillance has not received sufficient attention in moral and legal discussions. A well-informed analysis of employees’ experiences of work under surveillance and a well-reflected view of the values at stake regarding surveillance practice are necessary for an adequate privacy legislation. This is not to say that legislation is the sole means of privacy protection but that laws should, as far as possible, be anchored in well-reflected norms and values. By explicating the meaning and value of privacy at work and aspects relevant for perceived privacy intrusions I intend to contribute to a basis for better privacy legislation and also to the recently initiated “workplace assessments” i.e. processes whereby trade unions and employers together assess work performance according to checklists of environmental, resource, occupational,

---

10 Agenda 21 and the World Summit on Sustainable Development (WSSD) have created a framework for the development of partnerships for employee-employer assessments in workplaces.
health or social criteria. Such assessments are intended to identify and resolve problems ranging from the simple e.g. energy & resources wastes to the complex e.g. improving workplace conditions, employment issues or matters related to social security, public health or technology matters.

Finally, I will highlight some of the findings and contributions of the analysis.

Contrary to common understanding, the case has been made that the “private” can apply in various contexts and that it should be applied to the realm of work. Workers’ privacy is valuable and should be protected for the reason that we thereby protect its fundament – personal autonomy. However, privacy is not only an individual interest but a collective such and we are mutually responsible for protecting this interest whether requested or not. In consequence, the frequently met view of privacy as a \textit{prima facie} value is proven untenable. In cases where privacy comes in conflict with competing claims privacy is not at forehand the weaker value. A privacy intrusion or neglect of privacy would require a generally acceptable reason.

By and large, existing privacy protection laws and codes are based on too narrow a definition of privacy. A brief survey of prevailing legislation shows that only one of the normative aspects of privacy is sufficiently protected, i.e. that of obviously privacy sensitive and potentially stigmatizing information such as information about an employee’s sexual, political or religious
orientation (ECHR, 1950, ILO 1997). Although the ILO privacy code and privacy regulation in countries such as Austria, Germany, Norway and Sweden stipulate minimum standards regarding what should remain within an individual’s control, these acts primarily regulate the usage of personal data, leaving workers in a weak position to secure privacy interests that exceed the legally protected types of personal information. While existing privacy protection legislation and codes primarily focus on the collection, storage, dissemination and use of personal data, local privacy is overlooked. Both these dimensions are preconditions for autonomy and should be recognized in order to adequately protect workers’ privacy. Failure to acknowledge particular conditions and relations regarding work and the workspace contribute to an insufficient protection of workers’ privacy. Although the duty of good faith may be used to address the relational asymmetry between employer and employee, this is a rather general principle and more is needed to rectify the imbalance between employer and employee when negotiating work conditions or advancement. Contractual consent is in particular need of better recognition and the employment contracting process would benefit from the incorporation of the good faith obligation (bona fide) with a clear delineation of the conditions under which the agreement of contracting parties can be considered voluntary.
References


ECHR 23 Nov 1992 Series A No 251/B PN 2004-200


EU, Directive 95/46/EC of the European Parliament and Council, on the protection of individuals with regard to processing of personal data and on the free movement of such data (24 October 1995).


Gerstein, R. S., “Intimacy and Privacy“, *Ethics*, 1978


Merz Smith, E., “Everything is monitored, everything is watched – Employee Resistance to Surveillance in Ontario Call Centers“, MA Thesis. Department of Sociology, Queen’s University, Canada, 2004.


Rachels, J.,“Why Privacy is Important”, *Philosophy and Public Affairs* No. 4, 1975.


**Links:**


“The Logic of Privacy - A New Way of Thinking about personal information”,