This is a preprint version of the following article:
Brey, P. (2005). 'The Importance of Privacy in the Workplace,' *Privacy in the Workplace* (eds. S. O. Hansson and E. Palm), Fritz Lang, 97-118.

Chapter 5

The Importance of Workplace Privacy

1. Introduction

Existing discussions of privacy, including discussions of workplace privacy, too often rely on a vague and broad notion of privacy that cannot properly informed detailed analyses of specific privacy issues. As a result, such analyses often rely heavily on ad hoc considerations and intuitions, and analyses of different privacy issues do not add up to a coherent view on privacy. What is still lacking in the privacy literature is an adequate operationalized notion of privacy that affords a distinction between different types of private affairs, privacy rights, and privacy intrusions. In this paper, I attempt to develop such an operationalized notion of privacy and apply it to the analysis of workplace privacy issues. In section 2, I present this operationalized conception of privacy, which I then use in section 3 to identify the main privacy issues in today's workplace. In section 4, I identify the most important privacy rights in the workplace, and consider arguments for and against restrictions to these rights based on the employer's interest in good work performance. I summarize my main conclusions in section 5.

2. Towards an operationalized notion of privacy

Privacy as limited access to personal affairs

Systematic study of the notion of privacy began with Warren and Brandeis' famous essay titled "The Right to Privacy" (Warren and Brandeis, 1890), in which privacy is defined as "the right to be left alone". Since then, countless other definitions of privacy have been presented, many in the context of elaborate theories of privacy, that try to get at the core of this abstract and slippery notion. Theories of privacy generally allude to privacy as a

right of persons that is to provide protection against interference by third parties into their private affairs. In many theories, this right to noninterference is defined in terms of access and control: privacy rights are to restrict access to private affairs and give those persons whose private affairs are at issue the exclusive right to control such access.

Some authors have introduced the notions of "information" or "knowledge" as a defining feature of privacy (Westin, 1967; Fried, 1986; Parent, 1983). In such information-based conceptions of privacy, privacy is defined in terms of restrictions on access to, or control over, personal information, and intrusions on privacy are defined as situations in which personal information is collected or disseminated without consent of the individual who is the topic of this information. However, while it appears that many privacy issues revolve around the use of personal information, information-based conceptions of privacy are clearly flawed, as there is a number of privacy issues that cannot be fitted into an informational mold. That is, there are types of actions that can be recognized as intrusions on privacy but that do not seem to centrally revolve around the collection or dissemination of personal information.

Specifically, there are various sorts of intrusions into private affairs in which the violation of privacy seems to consist on the fact that these affairs are disturbed or disrupted, rather than that information is acquired about them. For instance, unlawful entry or trespassing, which is sometimes described as the violation of the privacy of someone's home, does not seem to revolve around information collection. Such an event may perhaps result in the collection of personal information by the intruder (if the intruder is not blind), but the violation of privacy does not seem to centrally reside in this collection but rather in the disturbance of private affairs. Likewise, not keeping a certain distance when talking to someone or sitting or standing next to them or touching their body may also be construed as violations of privacy even though they do not centrally involve the acquisition of personal information.

Therefore, if privacy is defined in terms of (control over) access, then clearly it is not just informational or cognitive access that is involved but also physical access, as when someone creates disturbances in private affairs. This corresponds well with Warren and Brandeis' description of the right to privacy as the right to be left alone: it is not just the right to be left alone from the gaze or opinions of others, but also the right to control

physical interference by others into one's private affairs. Adhering to the notions of access of control we may, with Ferdinand Schoeman, say that "A person has privacy to the extent that others have limited access to information about him, limited access to the intimacies of his life, or limited access to his thoughts or his body." (Schoeman, 1984, p. 3). The right to privacy is then the right of persons to control such access to their personal affairs.

Cognitive access, physical access and informed control

So far, I have distinguished two forms of access to private affairs: *cognitive access*, which is access to information about private affairs of a person, either through direct observation or through indirect means, and *physical access*, which involves direct interventions into private affairs that create a disturbance in them. In discussing cognitive access, I have stated that such access may result in the collection or dissemination of information. Privacy violations that involve the collection of information about private affairs may be called *snooping*, and those that involve the dissemination of such information may be called *exposure*. In snooping a third party makes personal information available to herself, whereas in exposure she makes it available to other parties. Cognitive access may moreover take various forms, depending on how information is collected. Cognitive access may involve live, unaided observation of private affairs, mediated observation (observation mediated through a camera or telephone line), or access to separate bearers of personal information (e.g., electronic databases, paper documents, photographs).

Physical intrusions, in which privacy is violated through physical interventions, may also be called *disturbances*. The term "physical intrusion" is meant in a broad sense here, to include physical interruptions of events, disturbances that take place by talking or making noise and disturbances that occur in virtual environments; when someone breaks into a private chatroom and starts insulting the participants, I would also call this a physical intrusion. Obviously, there are many privacy violations in which cognitive and physical intrusions occur jointly. This is only logical, because while disturbing the intruder usually also perceives things that are private (unless the person that creates the disturbance is blind and deaf).

There are also privacy violations that do not just center on cognitive access (snooping or exposure) or physical access (disturbance). Take, for example, a landlord who has installed cameras in the apartments of his tenants, and who does not just observe these tenants in their everyday affairs, but also makes systematic use of his observations to control the behavior of his tenants. If, for instance, he sees a tenant breaking house rules in their apartments, he may coerce her into obeying them in the future, or punish her by temporarily cutting of her electricity or by evicting her. This landlord is not necessarily creating a disturbance (because he may never enter any of the apartments) nor is he just snooping. Rather, he is making systematic use of his cognitive access to his tenant's apartments to control their behavior and living circumstances.

I would call this type of privacy intrusion "surveillance," were it not that this term is ambiguous; in a broad sense, systematic observation of subjects that does not result in direct attempts to control the thoughts and behavior of these subject is sometimes also called surveillance. So I opt instead for *informed control*. What is essential about informed control is the ability of a third party to exercise control over a person through his knowledge of private affairs of that person. This control may either be confined to the private affair about which the third party knows, or it may (also) affect other aspect of the person's life. For instance, if the snooping landlord observes that a tenant uses illegal substances, he may coerce her into stopping this behavior or doing it less frequently, but he may also use this information to blackmail the tenant, without necessarily interfering with the drug use itself. In the first instance, there is informed control over an observed private affair in that the conditions under which the private affair takes place are controlled. In the second instance, there is control over broader aspects of a person's life based on knowledge of a private affair. Notice, moreover, that informed control *may* include physical intrusions on privacy (when the landlord walks into an apartment every time he observes that rules are broken), but they are not *required*.

To summarize, privacy intrusions come in three kinds:

(1) unauthorized cognitive access (snooping and exposure)
(2) unauthorized physical access (disturbances)
(3) informed control (control over a private affair or broader aspects of a person's life).

Types of private affairs

So far, I have defined privacy in terms of limited access to private affairs, and I have described three modes of access to private affairs and corresponding ways in which privacy can be intruded on. I have not, however, said much about the objects of such access or intrusion: *private affairs*. What is a private affair, and what kinds are there? I will define private affairs as things connected to one's private life or work that one considers to be private. It turns out that there are many different kinds of private affairs. Private affairs may include behaviors, information bearers, aspects of the body, private rooms, personal objects and social events. Corresponding to these different types of private affairs are different types of intrusions on privacy. For example, violating the privacy of a social event like a dinner party (whether through cognitive access, physical access or informed control) is different from violating so-called informational privacy through access to personal information, which is again qualitatively different from violating privacy by going through the contents of someone's purse.

There have been few attempts in the privacy literature to systematically distinguish different kinds of private affairs and relate these to a theory of privacy. Westin (1967) has made a distinction between informational and relational privacy, where relational privacy is the right to determine one's own personal relationships and conduct without other people observing and interfering with them, and informational privacy is the right to selective disclosure of personal data. The private affairs corresponding to these two types of privacy are personal relationships and conduct, and personal data and their bearers. Nouwt and Vorselaars (in Bekkers et al., 1999) have further introduced the category of physical privacy, to supplement the notions of relational and informational privacy. Physical privacy is the right to control access to one's body; the private affairs it relates to are aspects of one's body. Allen (1999) also introduces a notion of physical privacy, but defines it more broadly to include both bodily integrity and restricted access to the home and one's personal belongings.

I believe that these attempts to define different types of privacy in relation to different types of private affairs should be further refined. Westin's and Nouwt and Vorselaars' notion of relational privacy lumps together personal relationships and

individual conduct, which are really distinct categories. I therefore propose to distinguish them: one type of private affair consists of individual conduc*t* (e.g., things one does when alone at home) and another consists of personal relationships, or social conduct involving instances of private communication and social interaction. Likewise, Allen correctly defines physical privacy to not only include bodily integrity but also integrity of the home and personal belongings. But then it also makes sense to distinguish the two: the human body is one type of private affair, and personal spaces and objects constitute another type, and different types of privacy rights apply to each of them.

Consequently, we may distinguish five basic kinds of private affairs, with corresponding rights to privacy: (i) the human body; (ii) personal spaces and objects; (iii) bearers of personal information; (iv) individual conduct and (v) social conduct. I will discuss these now in turn.

(i) The human body

By the human body, I mean the physical or biological body, with all its unique features as they apply to a specific person. Such unique features include physical and biochemical properties such as height, weight, facial characteristics, visual features of the nude body, fingerprints, medical conditions, the biochemical composition of blood, urine and feces and genetic makeup. Many such aspects of the body are privacy-sensitive, although there is often significant variation in the degree to which people hold certain aspects of their body to be private. This variation is strongly conditioned by culture, religion and gender. For example, in traditional Islamic cultures the female face is considered to be a private affair and is hidden in public areas, while in many nonwestern cultures, the nude body is not very privacy-sensitive, and public displays of nudity may be acceptable.

The human body is increasingly a contested site, as employers, law enforcers and others increasingly seek access to aspects of the body. Unwanted cognitive access may involve observation with the naked eye, mediated observation (e.g., through camera observation or body scans), medical tests, genetic tests, drug tests and biometric registration (recordings of fingerprints, iris prints and faceprints). Such cognitive access may be used for various types of informed

control, including an amount of control over the composition and appearance of the body and over biological functions. Unwanted physical access may include invasion of body space, unwanted touch, unwanted medical examinations and drug tests, unwanted registration of biometric properties like fingerprints, body searches, cavity searches, sexual assault and rape.

(ii) Personal spaces and objects

Personal spaces include the home, other personally owned and used spaces like the confines of one's car, and rented or appropriated personal spaces like a private chatroom on the internet or a claimed picnic spot. Personal objects are objects owned, hired or appropriated by a person for his or her personal use, such as jewelry, vacuum cleaners, refrigerators, teddy bears, etc. The privacy-sensitivity of personal objects or belongings may differ a great deal: mundane objects like pencils and vacuum cleaners will rarely be considered privacy-sensitive, whereas potentially revealing or embarrassing items like teddy bears, sexual apparel and antidepressants may be highly privacy-sensitive. Still, people sometimes want to keep mundane objects at their homes private as well, since these may still provide a lot of information about their personal lives.

Personal spaces and objects may be the subject of unauthorized cognitive and physical access in various ways: through house searches, break-ins, seizures, camera surveillance, remote sensing and ordinary peeking and snooping by curious third parties like house guests and fellow employees who cannot keep themselves from going through someone's personal belongings.

(iii) Bearers of personal information

Bearers of personal information are media that contain information about aspects of a person, for instance about her individual conduct, her thoughts and beliefs, her personal relations, aspects of her body or her personal belongings. Such bearers may include files, paper records, personal notes, pictures, diaries, electronic databases, video tapes, CD-Rs, personal digital assistants (PDIs), etc. They may encode information in various forms, including linguistic, numerical and pictorial,

and may include video and audio recordings. Bearers of personal information may be owned or used by the person in question. If so, they are a special type of personal object (as defined in the previous paragraph). However, many bearers of personal information are not owned and used by the subject of the information but by third parties, including doctors, insurance companies, banks, employers, government institutions, media agencies, internet providers, supermarkets and so on.

Bearers of personal information may be the subject of unauthorized physical access, resulting in disturbances if they are mishandled, but it is their cognitive function that is most important here: cognitive access to them may also provide cognitive access to aspects of someone's private life, and may offer concomitant possibilities for informed control.

(iv) Individual conduct

Individual conduct is defined in the context of this paper as nonsocial conduct, being individual behavior that does not (centrally) include interactions with others. A particularly important type of individual conduct from a privacy point of view is *solitary behavior*, being behavior that one performs when one is alone or "by oneself," without companions or observers that are believed to have access to one's behavior. Solitary behavior is often very privacy-sensitive. It may include behaviors that are quite similar to ones performed in more social or public settings (e.g., reading, watching TV, working) but also involves all kinds of intimate behaviors (e.g., taking care of bodily functions, autoeroticism), behaviors that do not adhere to normal public standards (e.g. laziness, sloppiness, gluttony, wearing outrageous combinations of clothing), exercising private personal hobbies, self-experimentation (e.g., making faces in front of a mirror), and generally, performing all kinds of actions that one would not normally perform in public, or even in a relatively intimate setting with family or friends.

Individual conduct, including solitary behavior, is increasingly subjected to monitoring (i.e., cognitive access), particularly through camera surveillance and

increased electronic registration of behavior (e.g., purchases, money withdrawals, vehicle use, computer use, internet use).

(v) Social conduct

Next to individual behavior there is social behavior: interactions with other human beings, whether they involve playing pool, making love, working together to plant a tree, having an e-mail exchange, or having a chat about the weather. From a privacy point of view, social behavior deserves to be treated separately from individual or nonsocial behavior, both because of special privacy considerations that apply to (solitary) individual behavior and because of special privacy considerations for social behavior, that result from the fact that it includes shared intimacy and trust. Indeed, many social interactions are private to some degree in that they are not meant to be (closely) observed or intruded on by third parties. One important form of social interaction that deserves special mention is *verbal communication*. Verbal communication, whether face-to-face, over the telephone, or via e-mail, SMS or internet chat, is often considered private, either because it contains privacy-sensitive information or because the conversationalists seek seclusion so as to create intimacy, trust or confidentiality between them.

Like individual conduct, social conduct is increasingly subjected to monitoring, particularly through camera surveillance and increased electronic monitoring of (technologically mediated) social interactions, for instance through telephone and e-mail monitoring.

In summary, I have argued that privacy can be defined in terms of the right of persons to control access to their personal affairs. I have argued that three types of access must be distinguished in the context of this definition: cognitive access (snooping and peeking), physical access (disturbances) and informed control (control, by means of cognitive access, over a private affair or broader aspects of a person's life). I have also argued that privacy rights must be specified in the context of five distinct types of (potentially) private affairs: aspects of the human body, personal spaces and objects, bearers of

personal information, individual conduct and social conduct (including, centrally, verbal communication).

3. Privacy issues in the workplace

As stated in the introduction, workplace privacy is increasingly a contested issue in organizations. Many new methods of monitoring workers have been developed in recent decades, building particularly on new developments in information technology and medical technology. In this section, I will outline the main privacy issues that play in today's workplace. I will do this in the context of my previous operational analysis of the concept of privacy. My typologies of private affairs and privacy intrusions are helpful in defining and categorizing challenges to workplace privacy, particularly challenges induced by new technologies. I will take as my point of departure the five types of potentially private affairs outlined in the previous section, and I will ask to what extent they appear in the workplace as contested objects. In doing so, I will take account of the fact that privacy intrusions in the workplace may take the form of unauthorized cognitive or physical access or informed control.

(i) The human body in the workplace

Worker's bodies are increasingly the subject of scrutiny by employers. From genetic dispositions to fingerprints, from the presence of scar tissue on the lower abdomen to to the presence of alcohol traces in worker's urine, employers increasingly know about, or are able to find out about, aspects of their worker's bodies. In some professions, moreover, such monitoring is accompanied by routine physical interventions, like periodical medical and drug tests and body scans. In an increasingly competitive business climate, employers are bent to know whether workers have medical conditions of genetic dispositions that may impact their work, or whether workers have a substance abuse problem. Also, organizations increasingly use biometric authentication and verification methods to provide security, which also touch on aspects of their worker's bodies. A wide variety of new and improved technologies has been instrumental in allowing employers access to aspects of their employee's bodies, and legislation has often not kept up with them.

Some of the main workplace privacy issues in relation to worker's bodies are the following:

- *Medical tests and medical background checks*

Employers increasingly make use of medical tests and access to existing medical records to assess the health of their employees. Psychological assessments are also increasingly sought. Such medical information increasingly plays a role in hiring and firing decisions, work benefits and career development, and its use is therefore controversial (Simms, 1994; Humber and Almeder, 2001; Rosenberg, 1999).

- *Drug testing*

Some employers routinely test their employees for substance abuse. Such tests are not normally defined as medical tests, and its use is more controversial that medical tests (Cranford, 1998; Gilliom, 1994; Rosenberg, 1999).

- *Genetic testing*

Genetic testing is usually performed for medical reasons, to determine whether a (prospective) employee is genetically predisposed to develop certain medical conditions, like cancer and hepatitis. Genetic tests are hence not ordinary medical tests, because the subject may not have any medical conditions, and the conditions for which he or she is tested positively may never actually develop. Their use is controversial, because they are not always reliable and the (prospective) employee may never actually develop a disease for which there is a genetic predisposition (Long, 1999; Chadwick et al., 1999).

- *"Pat down" searches and X-ray body scans*

In professions with high security risks, employees may be routinely subjected to "pat down" searches, some of which may also require (partial) undressing or even cavity searches, and to X-ray body scans. In an X-ray body scan, a technology used mainly at airports, low-dose X-rays are used to see beneath a person's clothing and undergarments. The result is an image of a nude body, with any devices or foreign objects that may be carried on the body. Major personal details of bodies, such as the

size and shape of breasts and genitals, masectomies, catheter tubes and penile implants, are revealed in such images (Murphy and Wilds, 2001). This technology is usually used with the consent of the person whose body is scanned but can also be used - and is being used - secretly.

- *Biometric screening*

Biometrics methods are increasingly used in the workplace as authentication and verification devices, for instance to monitor access to a building or area, to keep time on workers, or to monitor access to computer systems. Common biometric methods include iris scans, face scans and thumbprints. Biometric screening involves the electronic storage of privacy-sensitive biometric information, as well as the scanning process itself, which is experienced by some as privacy-intrusive (see Hes, Hooghiemstra and Borking, 1999; Alterman, 2003; Van der Ploeg, 2003).

- *Camera surveillance*

In most cases, camera surveillance in the workplace will not reveal private information about bodies or bodily conditions. Yet, it sometimes does so, for example if used in areas where employees (partially) undress or take care of their body. Camera surveillance in the workplace increasingly takes place in more (semi-) private environments, like offices, restrooms and leisure areas, and has been argued to invade privacy (McCahill and Norris, 1999; Dubbeld, 2003).

In most cases where bodily privacy is at issue in the workplace, it is cognitive access that is involved, which may in turn result in informed control (over the employee's drug use, health care, career development, etc.). Physical access to worker's bodies is not gained often, and is usually limited to medical or drug tests and body searches. (In stating this, I am not considering unwanted intimacies, which of course do occur often in workplaces. I am only considering physical intrusions on privacy that happen as a matter of company policy.)

(ii) Personal spaces and objects in the workplace

Workers frequently bring personal belongings with them to the workplace. These may include pens, wallets, handbags, personal digital assistants, laptops, plants, framed pictures of the family, and so on. Handbags and desk drawers may contain personal items like cosmetics, personal address books, medication and feminine hygiene products. Workers may also use the workplace as a temporary storage space, for example for groceries and other personal belongings. Workers also frequently have a workspace for their personal use (e.g. an office space) and personal equipment, furniture or tools (e.g., a desk, a personal compute, a closet) that they come to use as they own, and that they come to control. Workers often end up personalizing their workspace, not only by bringing in their own personal belongings, but also by modifying company property, for example by rearranging furniture or by choosing screensavers, backgrounds and settings on their PC. Workers tend to have privacy expectations concerning the access by others to personal belongings brought to work, and often also have an expectation of privacy regarding their workspace, e.g., the expectation that no one enters their office unannounced or goes through the contents of their filing cabinets or computer hard drive without their consent. Naturally, going through personal items like a handbag will be considered a greater violation of privacy than scrutinizing someone's tools or office furniture.

Privacy issues that may come up in relation to personal spaces and objects in the workplace may include unauthorized access by employers and fellow-workers to someone's personal workspace, camera surveillance of workplaces, workplace searches, and surveillance or searches of the contents of PCs. Workplace searches may include searches of employee offices, desks, lockers, personal items like purses and gym bags, files and mail. Surveillance and searches of the contents of PCs may involve inspecting the software and files on the employers' PC and taking random "snapshots" of the PC's desktop. In many professions, the working environment is increasingly a PC environment. The virtual work environment of a PC is much easier to inspect than a physical work environment, because it is usually possible for employers and system operators to have remote access to it, and because it is possible to perform quick searches for specific items.

(iii) Bearers of personal information in the workplace

A number of privacy issues in the workplace concern access to media that contain personal information about employees. Some such media may be in the possession of employees themselves, like personal belongings brought to work by workers that contain personal information (diaries, personal address books, photo albums) or items with personal information that were produced or received by the employee while at work (e.g., personal e-mail, paychecks, internet cookies). Searches of employee's belongings and surveillance of workplaces and electronic work environments may result in employers learning about such private information.

Other media may not be in possession of the employee herself but may be owned by (various departments in) the organization, or be found outside the organization but still be obtainable by its management. Regarding the body, medical records have already been mentioned as one type of medium of this sort. Many more personal records and media may be found in organizations, including financial records, personnel files, minutes of meetings, video surveillance tapes, and so on. Such files are usually meant to be accessible to a limited number of people, and it would be considered a breach of privacy if other persons in the organization were granted access as well.

Organizations also often perform *background checks* on prospective employees, which are increasingly easy to perform through the rise of the internet and electronic databases. Employees may, depending on legal limitations that may apply, check address history, criminal background, civil background, driving history, credit reports, and past employment. Obviously there are many employees who would consider at least some of these checks, when performed without their consent, a violation of their privacy.

(iv) Individual conduct in the workplace

Individual conduct in the workplace may either consist of working behavior (e.g., typing, drawing, soldering) or behavior for personal maintenance and leisure (e.g. snacking, reading internet newspapers, visiting the toilet, grooming, listening to music). Working behavior and personal maintenance and leisure of course sometimes mix, as when someone is working while listening to music or eating. The expectations of privacy for these three types of behavior will depend on the attitudes and beliefs of the worker, the

setting in which work takes place, and previous agreements that have been made. Obviously, surveillance cameras in a toilet will generally be considered unacceptable, whereas keystroke registration may be considered acceptable if it is part of an agreement between employer and employee.

Privacy issues that may play in relation to individual conduct in the workplace include unauthorized access by employers and fellow-workers to a private or temporarily privatized space in which someone is engaging in private behavior (e.g., a toilet or an office with a do-not-disturb sign), camera surveillance, computer keystroke monitoring, internet website monitoring, behavior monitoring using smart badges and motion detectors (e.g. to check if an employee washes hands after using the bathroom), location tracking using electronic employee badges, and satellite tracking (Givens, 2001). Camera surveillance and PC and internet monitoring are arguably the two most powerful techniques for monitoring individual conduct. Camera surveillance theoretically makes it possible to record and observe an employer's each and every movement. The monitoring of PC and internet use by their employees can give employers detailed, complete information on what workers type, read, access or download when working on their PC (see Ball, 2001; Wood, 1998; Alder, 1998; Brey, 1999; Rosenberg, 1999).

(v) Social conduct in the workplace

Social conduct in the workplace may, like individual conduct, be either work-related (e.g., teamwork, staff meetings) or directed at personal maintenance or leisure (e.g., joint lunches, social chats). Mixes occur as well, as when a conversation combines personal and work-related elements. Obviously, social conduct directed at personal maintenance or leisure will generally be more privacy-sensitive than social interactions that are work-related. However, work-related social interactions may also have a private character, involving confidentiality and trust, as when problems at work are a topic of discussion, or more generally when those who are interacting have an expectation of privacy.

As noted earlier, social interactions between persons may occur in unmediated form ("face to face" or in person) or be technologically mediated (e.g., telephone, e-mail,

internet chat, sms, voice mail, computer-supported collaborative work). Many privacy issues that apply to individual conduct in the workplace apply to social conduct as well. Other privacy issues are uniquely associated with social conduct. These include, amongst others, issues involving the monitoring of communications, as in telephone monitoring and e-mail monitoring. Another important privacy-related element in social interaction is, as previously mentioned, the potential importance of confidentiality, trust and intimacy between persons, for example between an employee and a fellow-worker or client, that may be violated by monitoring.

4. Workplace privacy and employer's interests

In most discussions of workplace privacy, it is recognized that employees have legitimate claims to privacy rights at work. In most discussion, however, it is held that such rights are to be balanced against the rights or interests of employers and other parties, which may require limitations on these privacy rights. In what follows, I will first make the case, based on the discussion of workplace privacy issues in the preceding section, that employees have legitimate expectations of privacy even while at work. I will argue that the privacy issues outlined in the previous section point to a set of *prima facie* privacy rights for employees that ought to be limited only if there are good reasons to do so. I will then consider some of the main arguments that have been made for restrictions on workplace privacy, which usually allude to the employer's interest in good work performance by his employees. I will then consider weaknesses in these arguments for restrictions on workplace privacy, and argue that they do not succeed in justifying strong curtailments of privacy rights at work in most circumstances.

***Prima facie* privacy rights in the workplace**

In discussing privacy in the workplace, it may be useful to distinguish between privacy rights that hold in principle and privacy rights that hold in practice, i.e. after calibration with circumstantial factors which may include other rights or interests. In general, rights of any kind may have to be weighed against other rights or they may be voluntarily forfeited, so that rights that are held in principle may not turn out to hold in practice. For instance, people may have a right to smoke, but it can be justifiably argued that this right

may not be exercised in confined public areas because it collides with other people's rights to clean air, or in cleanrooms because it could damage private property. I therefore want to arrive at a conception of the principled or *prima facie* privacy rights of employees, that may be argued to hold in advance of any balancing of such rights against other rights or interests, and preceding any possible voluntary forfeitures of such rights. On the basis of such principled privacy rights in the workplace, we may then go on to ask under what circumstances curtailments of such rights can be justified.

A determination of *prima facie* privacy rights in the workplace should ideally be sought through a method of reflexive equilibrium (Van den Hoven, 1997) in which existing privacy theory is balanced against privacy intuitions, existing social norms and practices, empirical research on the psychological and social dimensions of privacy, and other relevant data. I will not perform a full analysis of this kind here, but take a bit of a shortcut, relying mainly on existing privacy norms, laws and intuitions to arrive at a set of *prima facie* privacy rights in the workplace. I propose that *prima facie* privacy rights apply to a thing or activity in the workplace (e.g., the use of a toilet, an e-mail message, the contents of a purse) when such things or activities are generally considered to be private outside the workplace. More precisely:

> *Prima facie* privacy rights apply to an entity (thing or activity) in the workplace if and only if entities of that type outside the workplace are generally considered to be private affairs.

In the discussion of privacy issues in the workplace in the previous section, I have already identified many issues involving affairs that at least some people claim to be private. In some cases, this may involves entities that may also be contested outside the workplace as to whether they should be considered private. This may happen either because there are no shared social norms on whether or to what extent an entity should be considered private and therefore subject to privacy rights (e.g., some cultures or traditions consider the female face to be private, whereas most others do not), or because the private nature of a type of entity is heavily dependent on situational factors and subjective

intentions (e.g., whether a conversation is private depends in part on the intentions of the talkers and on the setting in which they choose to have their conversation).

For most of the privacy issues identified in the previous section, however, I believe that general agreement exists that the entities in question are private in ordinary circumstances. The disagreement about them concerns the extent to which the special circumstances of a workplace setting can void these ordinary privacy rights. At least the following matters considered in the previous section would be considered private to some degree in ordinary circumstances:

- aspects of the human body that are not visible in everyday life
- the contents of purses, shopping bags, desk drawers and lockers,
- rooms that function as a working or living environment for a person or group of persons
- solitary forms of behavior like toilet visits and solitary work breaks
- conversations about personal or leisure subjects
- person-to-person postal, voice mail or e-mail messages
- files or records with personal information

Prima facie privacy rights apply less obviously to activities that are strongly work-related and that involve few personal elements, such as many individual working activities and work-related interactions and conversations. This is because these activities often do not include many privacy-sensitive aspects like personal information, intimacy or confidentiality. However, a case can be made that such activities are still subject to some privacy rights. Helen Nissenbaum has argued in an important paper that even though there is a diminished expectation of privacy in public places, people still have justifiable privacy expectations even when they are in public (Nissenbaum, 1998). Her argument is that surveillance in public places that involves the electronic collection, storage and analysis of information on a large scale, without the consent of the public, violates privacy because this practice does not conform to normal information-governing norms in public places. Such norms require that observers or information collectors make themselves known and do their work visibly (e.g., surveilling police officers) and maintain contextual integrity, meaning that information deemed appropriate in one context is not used in contexts for which it was not intended and for which it was not

voluntarily made available. Such contextual integrity is often not maintained in electronic surveillance, because the information may easily be used in different contexts.

Nissenbaum's argument seems to apply to the workplace as well as it does to public areas. Here, solitary working activity and work-related interactions and conversations are not usually privacy-sensitive to the extent that accidental or intentional intrusions on them by third parties necessarily constitute serious violations of privacy, but sustained intense surveillance of such activities, possibly even done in secret and possibly performed without accountability for the use of the information thus collected, appears to run contrary to normal information-governing norms and normal expectations of contextual integrity, and can therefore be identified as *prima facie* violations of privacy. These violations of privacy clearly do not just rest on cognitive access of the surveillor to working activity of employees, but also on the informed control that such cognitive access affords, which may result, next to diminished workplace privacy, in diminished worker autonomy, the erosion of trust between employee and employer, lower morale, and stress and health problems (Persson and Hansson, 2003; Brown, 2000; Brey, 1999).

I conclude, then, that *prima facie* workplace privacy rights apply, to a lesser or greater degree, to nearly all the contested items that were discussed in the previous section.

Arguments for restrictions on workplace privacy

The main argument that has been put forth in favor of a limited right to privacy in the workplace is that employers have a strong, legitimate interest in monitoring the performance of their employees, and that this strong interest cannot be reconciled with strong privacy rights for employees. Good performance here relates to more than the question of whether employees work hard enough, create enough work output or create output that has enough quality. Good performance also means not harming the organization (for example though carelessness, wastefulness, theft and embezzlement, or through baseless lawsuits against an employer) and adequate fulfillment of role responsibilities. Therefore, both to ensure productivity and quality of work and to protect himself against harm, the employer must be able to monitor aspects of the employer's work (Miller and Weckert, 2000).

Persson and Hansson (2003), in a discussion of arguments pro and con workplace privacy, point out that adequate performance by employees is not just a strong interest of employers, it is also something for which employers get paid wages and salaries and it is part of the contract that workers sign with their employees. As they emphasize, workers are accountable to their employers for their work. This entails a right to oversee that workers do their work, and do it properly. Many contracts even specifically sign over rights from workers to employees, often giving employers the explicit right to test or supervise the work performance of the employee. Persson and Hansson quite rightly separate this contractual obligation from a desire to make profits which is present in many organizations: clearly, non-profit organizations also have an interest in adequate work performance.

It can be concluded that the interests of employers and the obligations of employees present a strong case in favor of at least some monitoring of employees' work, arguably not only of work results, but also of the workplace itself (workplace surveillance). Persson and Hansson also identify two other arguments in favor of workplace surveillance. First, third parties, such as clients, sometimes also have interests or rights that may warrant workplace surveillance. For example, the management of a public transport corporation has a duty to reduce passenger risk as far as possible. This may require monitoring of drivers, including, for example, drug testing. Second, it can be argued that surveillance is sometimes in the interest of employees themselves. For example, medical tests and genetic screening can be used to protect the health of workers, and drug tests can help decrease drug use and thereby reduce the risk of workplace accidents. In conclusion, several good arguments can be made to restrict workplace privacy, based on rights and interests of employers, third parties such as clients, and employees themselves.

Arguments against limitations on workplace privacy

The strongest and most straightforward argument for limitations on workplace privacy is undoubtedly the argument that employers have a strong interest, or even a right, to ensure good performance by their employees. I take this to be a matter of fact. The relevant question to be asked, however, is whether this right or interest of employers requires

strong limitations on workplace privacy. If such limitations are not necessary to ensure good performance, then it is hard to see how such limitations on privacy could be justified. I have stated earlier that good performance involves quality and quantity of work output, doing no harm to the organization, and adequate fulfillment of role responsibilities. It may be asked, then, whether the employer's interest in any of these three aspects of work performance requires strong workplace surveillance.

As for quality and quantity of work output, it would seem that close surveillance of workers often is not necessary to ensure such output. Clearly, there is no necessity to install surveillance cameras or monitor PC use and e-mail traffic if employers could also be asked to hand over their work output for inspection at the end of each day, week or month. The adequate fulfillment of role responsibilities by workers is sometimes more difficult to evaluate *post hoc*. But in most organizations managers have enough normal interaction with the employee, his or her fellow-workers and possibly clients to be able to know when an employer is not fulfilling role responsibilities. In most cases, therefore, close surveillance of the fulfillment of role responsibilities therefore seems unnecessary.

The prevention of harm to the organization, which might result amongst others from carelessness, wastefulness, theft and embezzlement, clearly sometimes warrants workplace surveillance, as when there are clear indications that an employee is engaging in fraud or theft. In such cases, invasions of the employee's privacy, including searches and e-mail and telephone monitoring, may be justified. At issue, however, is whether the prevention of harm to the organization justifies routine searches, routine e-mail and telephone monitoring, extensive camera surveillance, and so on. This would, indeed, be hard to justify as it would run counter to the way security is balanced against privacy and civil liberties in other sectors of society. For instance, police does not search your home or read your mail or tap your telephone conversations unless they have probable cause that you are engaging in illegal activity. The probable cause principle seems equally reasonable for workplace surveillance. If there is no probable cause that an employee is causing harm to the organization, then there may be less privacy-intrusive means to protect the organization against harm, like clear rules and procedures, company trainings aimed at improving safety, security and waste reduction, regular accounting checks and audits, tagging company property, and anonymized screenings of web and e-mail traffic.

An exception may apply to heavily-regulated industries (e.g., aviation, military and nuclear energy industries) and in organizations where employees have access to highly confidential records. In such organizations, a closer monitoring of employees may be required.

Background checks and tests that are performed as part of the hiring process seem to present a special type of workplace privacy issue. Here, it is not performance that is monitored, but the promise of good performance. The relevant question is: what types of personal information may an employer require in order to assess the prospects of good workplace performance? To answer this question, one must not just assess the privacy-sensitivity of certain types of information, but also their predictive value in assessments of employees. Moreover, issues of social justice and equality are also involved: is it reasonable for an employer to exclude employees because they have a genetic disposition to develop a certain medical condition or because they have a criminal record, and should employers therefore have access to such information? It would seem that privacy rights and considerations of equality and social justice impose serious limitations on the use of personal information in the hiring process.

I conclude that, so far, the burden of proof is on proponents of strong limitations on workplace privacy to demonstrate that such limitations are necessary to ensure good performance by employees and that alternative, less privacy-intrusive means to ensure good performance are not available. And it seems, so far, that such alternative means are often available. It may still be argued by proponents that contractual obligations or later agreements, voluntarily entered into by the employee, may void privacy rights. These contracts or agreements may for example specify that the employee is subject to certain types of surveillance, tests or searches. With such a contract, the employee obviously does not have a strong claim to resist such measures. But as Persson and Hansson rightly point out, such a contract does not void the moral obligation of the employer, which may sometimes also be a legal obligation, to choose those means for monitoring performance that are least privacy-intrusive. After all, as they point out, “The employee does not sell him/herself (that would be slavery) but his or her work” (p. 63-64).

5. Conclusion: privacy rights in the workplace

In my discussion of workplace privacy, I first presented an operationalized notion of privacy in section 2. Privacy was defined in terms of limited access to private affairs, after which three modes of access to private affairs were described (cognitive access, involving snooping or exposure, physical access, involving disturbances of private affairs, and informed control, involving the regulation of private affairs or wider aspects of someone's life). Next, five types of private affairs were distinguished, the human body, personal spaces and objects, bearers of personal information, individual conduct and social conduct, and it was claimed that these types correspond with different sets of privacy rights. In section 3, this operationalized notion of privacy was used to identify the main privacy issues in today's workplace. These are issues that range from genetic testing to video surveillance to e-mail monitoring.

In section 4, I then presented arguments for privacy rights in the workplace, followed by arguments pro and con restrictions on such rights. I concluded at the end of section 4 that while employers may have a strong interest in good work performance, it does not follow that strong limitations on workplace privacy are justified. Most arguments I presented for this position are not principled but practical ones: the fact is that strong limitations on workplace privacy are often not necessary to ensure good work performance. And if such limitations are not necessary, then it is hard to see how they could be justified. I have criticized one such justification that has been presented: that the limitations may be company policy and part of a contract that the employee has voluntarily entered into. I have argued that organizations have a moral obligation, regardless of such contractual agreements, to ensure that privacy intrusions are not greater than necessary.

References

Alder, G. (1998). 'Ethical issues in electronic performance monitoring: a consideration of deontological and teleological perspectives,' *Journal of Business Ethics,* 17, 729-744.

Allen, A. (1999). 'Coercing Privacy,' *William and Mary Law Review*, 723-724.

Alterman, A. (2003). '"A Piece of yourself": Ethical Issues in Biometric Identification,' *Ethics and Information Technology* 5(3): 139-150.

Ball, K. (2001). 'Situating Workplace Surveillance: Ethics and computer Based Performance Monitoring,' *Ethics and Information Technology* 3(3), 209-221.

Bekkers, V., Koops, B. and Nouwts, S. (eds.) (1996). *Emerging Electronic Highways: New Challenges for Politics and Law*. The Hague: Kluwer Law International.

Brey, P. (1999). 'Worker Autonomy and the Drama of Digital Networks in Organizations,' *Journal of Business Ethics*, 22: 15-25.

Brown, W. (2000). 'Ontological Security, Existential Anxiety and Workplace Privacy,' *Journal of Business Ethics*, 23(1), 61-65.

Chadwick, R. Shickle, D., Ten Have, H. and Wiesing, U. (eds) (1999). *The Ethics of Genetic Screening*. Dordrecht: Kluwer.

Cranford, M. (1998). 'Drug testing and the right to privacy: arguing the ethics of workplace drug testing, *Journal of Business Ethics* 17: 1805-1815.

Dubbeld, L. (2003). 'Observing Bodies. Camera Surveillance and the Significance of the Body,' *Ethics and information Technology*, 5(3), 151-162.

Fried, C. (1986). 'Privacy,' *The Yale Law Journal*, 77: 3, 475-493.

Gilliom, J.(1994). *Surveillance, Privacy and the Law: Employee Drug Testing and the Politics of Social Control.* University of Michigan Press.

Givens, B. (2001). 'A Review of Current Privacy Issues,' *Privacy Rights Clearinghouse*, March 2001.

Hes, R., Hooghiemstra, T. and Borking, J. (1999). *At Face Value: On Biometric Identification and Privacy*. The Hague: Registratiekamer.

Hoven, J. van den (1997). 'Computer Ethics and Moral Methodology.' *Metaphilosophy* 28: 3, 234-248.

Humber. J. and Almeder, R. (2001). *Privacy and Health Care*. Totowa, NJ: Humana Press.

Long, C. (ed.) (1999). *Genetic Testing and the Use of Information*. AEI Press.

McCahill, M. and Norris, C. (1999). 'Watching the Workers. Crime, CCTV and the Workplace,' in P. Davis, V. Jupp and P. Francis (eds.), *Invisible Crimes. Their victims and their regulation*. London: MacMillan.

Miller, S. and Weckert, J. (2000). 'Privacy, the Workplace and the Internet,' *Journal of Business Ethics* 28: 255-265.

Murphy, M. and Wilds, M. (2001). 'X-Rated X-Ray Invades Privacy Rights,' *Criminal Justice Policy Review*, 12(4), 333.

Nissenbaum, H. (1998). 'Protecting Privacy in an information age: The problem of privacy in public,' *Law and Philosophy* 17: 559-596.

Parent, W. (1983). 'Privacy, Morality and the Law,' *Philosophy and Public Affairs*, 12: 269-88.

Persson, A. and Hansson, S. (2003). 'Privacy at Work - Ethical Criteria,' *Journal of Business Ethics* 42: 59-70.

Rosenberg, R. (1999). 'The Workplace on the Verge of the 21st Century,' *Journal of Business Ethics* 22: 3-14.

Schoeman, F. (ed.) (1984). *Philosophical Dimensions of Privacy. An Anthology*. Cambridge University Press.

Simms, M. (1994). 'Defining Privacy in Employee Health Screening Cases: Ethical Ramifications Concerning the Employee/ Employer Relationship,' *Journal of Business Ethics*, 13(5), 315-325.

Van der Ploeg, I. (2003). 'Biometrics and Privacy. A note on the Politics of Theorizing Technology,' *Information, Communication, Society,* 6(1), 85-104.

Warren, S. and Brandeis, L. (1890). 'The Right to Privacy,' *Harvard Law Review*, 4: 193-220.

Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.

Wood, A. (1998). 'Omniscient organizations and bodily observations: electronic surveillance in the workplace,' *International Journal of Sociology and Social Policy*, 18(5), 136-174.