Scandinavian Journal of Information Systems

Volume 18 | Issue 2 Article 3

2006

The Embedded Panopticon: Visibility Issues of Remote Diagnostics Surveillance

Katrin Jonsson
Umeå University, katrin.jonsson@umu.se

The Embedded Panopticon: Visibility Issues of Remote Diagnostics Surveillance

Katrin Jonsson

Department of Informatics, Umeå University, Sweden
katrin.jonsson@informatik.umu.se

Abstract. Remote diagnostics technology is embedded into physical products in order to prevent breakdowns by monitoring the products' condition via sensors. However, this technology also hides indirect possibilities to monitor the users. The aim of this paper is to explore how remote diagnostics technology changes surveillance and its ethical consequences by studying which surveillance dilemmas users and suppliers identify in remote diagnostics technology and the rationale behind their perspectives. The results show how visibility and non-visibility are of decisive importance concerning whether or not users can examine ethical dilemmas in computer use as visibility seems to be what triggers employees' feelings of being monitored or not. Despite their monitoring possibilities, remote diagnostics systems do not seem to evoke such feelings. By embedding technology and thereby also the monitoring into physical things, both the technology and the cues of surveillance become concealed, both literally and virtually for the user. To the user the direct reminders of surveillance are thus embedded together with the technology, creating an embedded panopticon. As the users cannot examine possible ethical dilemmas the responsibility remains with the suppliers and challenges them to pick a strategy for how to handle ethical questions.

Keywords: remote diagnostics technology, surveillance, panopticon, ubiquitous computing, visibility

1 Introduction

In 2001 an employee at a company in England was found to be misusing the company's equipment. The employee had discovered a way to overload a motor with rubber, which gave him longer coffee breaks but also significantly shortened the lifetime of the motor. This was detected by the motor manufacturer in Sweden who had a remote diagnostics system installed in the motor to monitor its performance. The manufacturer made the company attentive to the problem and they took action. The remote system monitored different parameters and data was collected and analyzed in order to prevent breakdowns. However, besides showing the motor's condition the system also gave indirect information about how the operator used the product.

The use of information technology (IT) generates new ethical situations (Conger and Loch 1995). Some are rather obvious ethical dilemmas such as unauthorized access to information, distribution of illegal material on the Internet, monitoring of email or misuse of data. Other situations might not be as clear cut, for example policies incorporated into an expert system or incorrect information upon which decisions are taken. In the latter cases the users might never be aware of the hidden reasoning in the systems.

Through the omnipresent penetration into people's everyday life information technologies, especially those based on pervasive and ubiquitous computing, have the potential to overcome many deficiencies of current IT applications, but at the same time they entail tremendous threats to people's privacy (Cas 2005; Cuff 2002; Langheinrich 2005). According to Cas (2005) ubiquitous technology contradicts the fundamentals of privacy protection as the extent and the purpose of the data collection are difficult to define and people can hardly be informed of what is being collected, both due to practical reasons and incompatibility with the very goal of pervasive penetration into the everyday environment. Ubiquitous computing applications are nowadays designed to support use in both private spheres and in public spheres such as in the workplace. For example, a car can be equipped with a system to support the driver with instructions and information while driving, or products in the workplace can incorporate identifiers to allow for automatic stock management. Remote diagnostics is a ubiquitous technology designed to monitor equipment at a distance in order to prevent breakdowns. It can be used both for private equipment in people's homes as well as for products at work. This paper focuses on work-related use of the technology in industries. Even though monitoring the user is not the primary function of the systems, they are capable of surveillance as user-related parameters can be monitored, for example how the equipment is used.

Many previous studies on ubiquitous computing and surveillance are either conceptual papers theoretically discussing the emerging impact on privacy (Banavar and Bernstein 2004; Bohn et al. 2004; Cas 2005; Cuff 2002; Lahlou et al. 2005; Langheinrich 2002) or design oriented developing privacy protecting functions (Hong and Landay 2004; Jendricke et al. 2002; Langheinrich 2005). However, there are few empirical studies on surveillance and ubiquitous technologies. This paper aims to explore how remote diagnostics technology changes surveillance and its ethical consequences by answering the following questions:

1. Which surveillance dilemmas do users and suppliers identify in remote diagnostics technology?
2. What is the rationale behind the users' and suppliers' perspectives?

The issues of surveillance will be investigated from a user perspective—those who might be exposed to the surveillance—and a supplier perspective—those who develop or are responsible for the implementation of the technology—as ethical dilemmas of technology use are important to be aware of and responsive to, both for employers, employees and those with whom they interact, for example suppliers, consultants or customers (Sipior and Ward 1995). A qualitative research approach based on interview data is used to seek an understanding of the different actors' views on remote diagnostics.

The remainder of this paper is organized into five sections. Section two provides the background for the study and examines previous research on surveillance in relation to IT and ubiquitous computing. The panopticon as a concept and framework to understand the surveillance in society is also introduced here. Section three contains a description of the research design and the case organizations. Section four presents the findings, which are discussed in section five. The paper finishes with some implications and brief-conclusions.

2 IT and Surveillance

The use and development of information technology create new ethical issues and unforeseen possibilities for potential controversial actions and events (DeGeorge 2003; Johnson 1989). For business organizations it becomes a part of their business ethics (Gattiker and Kelley 1999) to consider such issues, as IT use raises questions concerning privacy of personal data, surveillance, ownership of data and access to name a few examples (Mason 1986). Organizations and individuals cannot afford to be uncommitted to how these issues should be dealt with as they, by their judgements and actions, "shape the world we live in" (Mason 1986). However, according to Conger and Loch (1995) people may not understand ethical issues of computer use as they are unable to compare computing experiences to offline circumstances. Therefore, computer users might make judgements related to online situations, which they would not have made in other situations. On the other hand, in a later study Gattiker and Kelly (1999) found that computer users were able to recognize ethical dilemmas in computer use as they were able to compare them with offline situations.

One computer related ethical dilemma is the possibility of monitoring employees. Such surveillance raises questions of privacy invasion and privacy protection, for example regarding monitoring employees' email messages (Sipior and Ward 1995). In the USA estimates suggests that as many as two thirds of companies monitor their employees (Weckert 2001). The moral aspects of employee monitoring are made even more explicit when there are examples of employees' losing their jobs after being detected misusing the company's equipment. Today, many different kinds of software exist which enable monitoring. Computer based performance monitoring is used in among other places call centers to monitor the employees' work rate (Bain and Taylor 2000).

2.1 Surveillance and Ubiquitous Computing

In 1991 Weiser (1991) envisioned ubiquitous computing as the information technology for the 21st century. In contrast to other types of IT that are designed to bring the computer to the foreground, ubiquitous computing is designed to make technology vanish into the background. Processors and sensors are integrated into everyday objects, which make the technological devices disappear. Besides being embedded, ubiquitous technology also supports mobility (Lyytinen and Yoo 2002). From a surveillance point of view ubiquitous computing is a step towards technology that gives continuous and everlasting access to information and that transforms, among others, tools, books and people into monitored objects (Araya 1995). The vision of living in an environment filled with embedded interacting technologies offers many new possibilities. The concept of a 'smart home' is often used to describe how the technology pushes towards a pervasive penetration of everyone's everyday life. The refrigerator helps to keep track of the food items' expiry dates and to produce a shopping list, the smart bed remembers the user's preferred sound, smell, light and temperature settings at wake up time and the smart mat recognizes who steps in by sensing body weight and foot prints (Park et al. 2003).

Although they seem to have been produced largely unnoticed by the general public (Bohn et al. 2004), there are, however, also apprehensions about the long-term and sometimes unanticipated consequences which these applications will have for people's everyday life and ethical values. With the technology's monitoring possibilities we could end up in a surveillance society that will invade people's privacy to an extent we cannot even imagine if such questions are not dealt with (Cas 2005; Cuff 2002; Langheinrich 2002).

From a surveillance point of view there are five basic properties that distinguish ubiquitous computing from traditional data systems (Langheinrich 2005): (1) collection scale—it becomes possible to monitor more and more areas, e.g. homes, offices and things, (2) collection manner—we can no longer know when we are monitored by the technology, (3) new types of data—it allows for a higher quality of data coming from sensors smaller than buttons, as even emotional status can be monitored, (4) collection motivation—almost every information can be valuable in a digital environment and finally, (5) data accessibility—the systems are able and need to collect large amounts of data in order to provide valuable services in different contexts.

There have been attempts to design ubiquitous computing applications which respect privacy (Hong and Landay 2004; Jendricke et al. 2002; Langheinrich 2005). These applications include identity management technologies and personal assistants, which administer privacy preferences set by the user. The idea of these applications is to allow the user to set the preferences themselves instead of leaving this role to the designer. However, Cas (2005) contends that there is a conflict between the principles of protecting privacy and the characteristics of ubiquitous computing. To protect privacy, data collection should be limited, its purpose should be clear, and people whose data are collected should be informed. Ubiquitous computing is, however, designed to support people in a variety of situations and its purpose is not always predefined. People's basic awareness that data about them might be collected can be supported by, for example, visible tags, but detailed knowledge about which data is collected is difficult to provide and contradicts the technology's goal of unobtrusiveness (Cas 2005).

Cas (2005) also argues that living in a society where monitoring can take place anytime and anywhere creates a situation where "the only realistic attitude of human beings living in such environments is to assume that any activity or inactivity is being monitored, analyzed, transferred, stored and maybe used in any context in the future" (Cae 2005, p. 5). Such monitoring societies are sometimes described as, and compared to, a panoptic society. Thus the panopticon can be viewed as a metaphor for surveillance (Bain and Taylor 2000; Cas 2005; Cuff 2002; Koskela 2003; Zuboff 1988).

2.2 A Panoptic Society

The panopticon was originally designed by Bentham (cited in Foucault 1979) as a special surveillance tower for factories and was later adopted in prisons. The tower was constructed to allow guards to watch the convicts without their knowledge. A backlight ensured that the guards could see into the area where the convicts were housed, while the inmates could not see if the guards were present or not. With this design, surveillance became depersonalized as the identity of the observer remains hidden and is not important (Albrechtslund 2005). The convicts were aware that they could be watched, which should make them act as if they were constantly monitored. The panopticon thus automated the surveillance system and reduced the need for actual guards (Shell 2002). Knowledge about the possibility of being watched and about others having the power to intervene can make people act as if they were watched (Sayer and Harvey 1997). Accordingly, the panopticon was designed to increase self-control among convicts, and made them act as if they were constantly controlled.

Visibility is vital in the panopticon. It creates the feeling of constant monitoring. It is also important to communicate the aim of the surveillance to the individuals, to make them understand why they are being monitored and to evoke their self-discipline (Sayer and Harvey 1997). The tower is visible and reminds the prisoners of the possibility of being watched. Moreover, how they are monitored is visible and, finally, it is the prisoners' visual behavior that is controlled.

Zuboff (1988), among others, has related IT-based surveillance to the concept of the panopticon. When she found that people in a plant did not like being observed by an IT-system all the time, she compared environments where people feel constantly observed with panopticons (Banavar and Bernstein 2004). According to Zuboff (1988) IT liberates data from time and space constraints and makes it independent of a specific institution or person. Such liberation enables new types of data analysis surveillance through linking different databases and searching for associations. Computerized monitoring of employees' work rate has been studied in call centers where the systems serve as tools of control for management and to undermine possible worker protests and resistance. In this context, the panopticon concept has been used to describe a vision of the future for call centers (Fernie and Metcalf 1998). However, in the studied call centers the individuals were aware of the monitoring possibilities in the IT-systems.

Even though the panopticon is a strong metaphor and has been widely adopted as a framework to understand computer-based monitoring it also has limitations with regard to contemporary surveillance possibilities. In the panopticon, surveillance is restricted in time and space and people cannot know for sure whether or not they are being monitored. They are, however, lured to assume that. This in effect creates a permanent panopticon although it is discontinuous in its action (Bain and Taylor 2000). However, a ubiquitous computing environment allows for a form of surveillance which persists across time and space and people have to assume that they are being monitored the whole time (Cas 2005). With embedded sensors, surveillance can potentially be everywhere, performed by any actor, for unknown purposes. These systems thus depart from the geographic centeredness which is included in the original concept of the panopticon (Cuff 2002).

According to Bain and Taylor (2000) adopters of the panopticon give no or little account of resistance which is in line with the assumption that the self-discipline evoked by the panopticon makes people's resistance disappear (Koskela 2003). However, studies of computer based monitoring have shown that resistance exists and workplace surveillance is more complex than the panopticon suggests. Employees are sometimes able to circumvent surveillance capabilities in the systems (Timmons 2003), find out when they are being monitored and organize collective resistance (Bain and Taylor 2000). It is thus a mistake to believe that monitoring IT systems result in complete managerial control (Bain and Taylor 2000).

Different concepts have been introduced to go beyond the limitations of the concept of the panopticon and to better describe the emerging surveillance society. As the panopticon does not reflect all aspects of computerized surveillance the term super-panopticon is used by Poster (1995) to better explain technological surveillance. He discusses the resemblance between databases and the panopticon, but he also demonstrates how databases allow for a more enhanced and effective monitoring as they can be moved in space and persist over time. Moreover, private information such as economic transactions becomes public through databases by acts of individuals. When a credit card is used, databases are provided with and store information. The concept of the super-panopticon is thus used to illustrate technologically enhanced surveillance which is enabled by databases (Poster 1995).

The postmodern-panopticon is another concept presented by Albrechtslund (2005) to stress the new dimension introduced by ubiquitous computing. It is intended to incorporate the thinking of the panopticon while also signaling that there is a new conceptual and technologically constituted environment, which needs a new framework for ethical discussions (Albrechtslund 2005). Koskela (2003) also stresses the weaknesses of the concept panopticon as power and control are more dispersed and flexible in modern society. Post-panopticon and electronic super-panopticons are concepts used to incorporate the thinking of the panopticon but also stress the differences with today's computerized monitoring possibilities (Boyne 2000; Lyon 2001).

However, although the panopticon concept has limitations, there are strong reasons for keeping it. Koskela (2003) argues that it helps to understand some of the most vigorous kinds of visual control and surveillance. This is important since we cannot escape the monitoring, only try to understand it (Koskela 2003).

There are few studies which empirically investigate questions of surveillance (Langheinrich 2002). This paper attempts to contribute to the understanding of the phenomenon by utilizing such an approach and by specifically exploring surveillance in remote diagnostics environments in workplaces.

3 Research Approach and Case Organizations

This study seeks to explore surveillance issues of remote diagnostics technology in an empirical setting, thus organizations with experience of this type of technology were selected. The research data were collected in five different organizations. The companies are MacGregor Cranes, Monitoring Control Center (MCC), PowerDrive, Alpha and Beta (the last three of which are fictitious names), all located in Sweden. The selection of the sites was based on theoretical rather than statistical reasons (Yin 1989), as the primary aim of this study is to understand more than it is to generalize. The results might thus not be generalizable, but that does not exclude that they can contribute to the collective body of knowledge of a discipline (Kautz and McMaster 1994). The selection of the sites was based on their willingness to cooperate, the availability of multiple sources and the possibility of purposeful sampling (Peppard 2001; Yin 1989). Two of the organizations, both suppliers of remote diagnostics technologies, MacGregor Cranes and PowerDrive, were part of a larger research project and contact had thus already been established with them. Together with PowerDrive, two customers were selected who had experience of using remote diagnostics technology. Finally, MCC has experience with providing remote diagnostics services and agreed to participate in the study.

The study employed the qualitative data collection technique of semi-structured interviews. In all, the study included 31 interviews, conducted by the author and a co-researcher. Ten interviews were held at MacGregor Cranes, three at PowerDrive, seven at MCC, five at Alpha and six at Beta. The interviews lasted between 45 minutes and 3 hours, with an average of about 60 minutes. Each interview was recorded, which allowed the researchers to focus upon the respondent and formulate follow-up questions. The interviews were then transcribed to enhance the analysis. All interviews were conducted on site at the respondents' workplace, which enabled the researchers to gain some insight into the work. When choosing participants we wished to include individuals with different relationships to the technology. No restrictions on participation were imposed from management so respondents were chosen in consultation with a contact person at each company. At the two organizations representing users of remote diagnostics technology participants were chosen to cover both individuals in a managerial position and people working with products equipped with the remote diagnostics system. At the three supplier organizations we were also allowed to meet respondents in managerial positions and technicians developing the technology.

This study is part of a wider research project focusing on the use of remote diagnostics technology in the manufacturing and process industry, therefore the data collection covered more issues than just surveillance related ones. The interviews have thus included issues of value, benefits and challenges of using this technology. Concerning surveillance possibilities the respondents were asked questions regarding whether they saw and experienced surveillance possibilities in the technology, their view on this type of surveillance and if they had experienced other types of surveillance at the workplace. Depending on the respondents' experiences follow-up questions were asked during the interview.

The results of this study were developed in a three-stage analysis. During stage 1 the transcription from each interview was read through. While reading, notes were taken to summarize the material. After reading each data source, stage 2 began, which involved a cross analysis of the interviews to find similarities and differences. Each interview gave an explanation of the phenomenon from a certain perspective, for example a technician's view could be compared with a manager's view on the technology. This crosschecking of different perspectives secures a certain validity as the interpretation is built up from multiple sources. The analysis was not guided by any formal hypothesis; it sought to retain a large degree of theoretical flexibility to ensure that the emergent constructs were built on the empirical data (Eisenhardt 1989). However, the analysis did include some foresight with regard to the primary purpose of the investigation and the posed questions, which were gleaned from the aim of the study and from prior research presented in section 2. This second stage resulted in a description including both general themes among the respondents as well as more individual views. The third stage of the analysis included a cross-case analysis, searching for similarities and differences between the cases. The case organizations were classified as developers/suppliers or users of remote diagnostics technology and the comparison took place within these two groups.

Of the five organizations included in the study three are classified as developer/suppliers of remote diagnostics while two are classified as users of the technology. This classification is shown in Table 1.

Organization	*Activity*	*Relation to remote diagnostics technology*
MacGregor Cranes	Manufacturer of cranes	Developer/Supplier of services
PowerDrive	Manufacturer of motors	Developer/Supplier of services
MCC	Specialized in condition-based monitoring of products	Takes part in developing projects/ supplier of services
Alpha	A process-industry company. Customer to PowerDrive and MCC.	Has systems installed in its plants.
Beta	A process-industry company. Customer to PowerDrive.	Has systems installed in its plants.

Table 1: The case organizations

MacGregor Cranes is a manufacturer of cranes and has recently developed a first prototype of a remote diagnostics system to enhance the maintenance of cranes. Sensors are installed into the crane to collect data about its condition and the time of use. These data are sent to a server at MacGregor every time the crane is turned off and then analyzed to find out when maintenance is needed. Since the cranes travel all around the world they are also equipped with a Global Positioning System that shows where they are at any given moment. This position is sent to MacGregor every six hours and is valuable when scheduling the maintenance. A remote diagnostic service is offered to the customers where MacGregor takes responsibility for monitoring the cranes and for signalling when maintenance is needed. By the time of this study the system and the service were rather new so they did not have any existing customers.

PowerDrive is a manufacturer of motors and has developed a remote diagnostics system to enhance the maintenance of the motors. Their system is based on sensors embedded in the motors, which collect data about their condition. Data are collected every 30 seconds and are temporarily stored in the remote system before they are transferred once a day to a server at PowerDrive for analysis. If something is detected an alarm is automatically sent out to technicians via SMS or e-mail with information about the problem. A report, which summarizes the motors' condition and detected problems, is put together every month and sent to the customer. The company offers their customers a similar service as MacGregor Cranes, where PowerDrive takes responsibility for monitoring the motors and signals when maintenance is needed.

MCC is a provider which offers remote diagnostics services. In contrast to MacGregor and PowerDrive they are not manufacturers and they do not develop remote systems on their own but they participate in such projects with other companies. MCC takes responsibility for implementing the remote systems into the customers' products and they also take responsibility for analyzing the collected data and informing the customers when maintenance is needed.

The last two companies, Alpha and Beta, have remote diagnostics systems installed in their plants. Further information about these organizations is withheld due to confidentiality agreements.

All five companies in this study are developing or using remote diagnostics with the primary aim of enhancing the maintenance process of machinery by enabling condition-based maintenance. IT is used to monitor products and maintenance decisions are based on both scheduled activities and identified maintenance needs shown by the systems.

4 Findings

4.1 Employees Are Attentative to Activities Which Have the Potential of Surveillance

A few years ago the technicians at Alpha were asked to begin filling in work reports after every completed job. When the management launched these new reports there were a lot of discussions among the employees about the surveillance aspects of this new working procedure.

> Surveillance has gone too far. When the time reports were introduced there were a lot of discussions, we experienced it as if we were being monitored since they [the employer] could see how long it had taken to complete a specific task. (Technician, Alpha)

The maintenance manager confirmed the discussions about the time reports and the surveillance possibility they create.

> If there's a problem with a machine they [the technicians] should report how long it takes to fix it. However, they don't want to do that since they think we are monitoring them and checking the time reported… They have an old perspective, believing the employer wants to punish them, but that's not the case. We want to improve the work, we want to make a profit, survive as a company and that requires becoming more effective. (Maintenance manager, Alpha)

Monitoring and surveillance are sensitive issues to some of the employees who were interviewed in this study. Time reporting is perceived as a rather obvious instrument that can enable monitoring. Writing down how long it had taken to perform a certain activity directly evoked the employees' feeling of being monitored and the risk of being punished by the employer. With these reports the employer has the possibility of comparing different employees and controlling what each employee is doing. However, as the maintenance manager expressed, this was not the objective. The purpose of the reports was to serve as a basis for organizing the work and making sure that nothing was missed. According to the manager the organization did not use the reports to compare different technicians; instead the organization wanted to use them as a tool to improve the plant. For example, if these reports showed that a certain machine required a lot of maintenance, the data could be used to find the reasons for any problems so they could be removed through new installations or reconstructions. Management thought the time reports could help them to find the most time-consuming machines in the plants, but the employees perceived them as a way of monitoring their work.

Another situation where workers showed resistance due to indirect monitoring possibilities arose when Alpha equipped all employees in a certain division with tags to improve safety. The tags made it possible to see where people were located. When the employees received these tags there were serious discussions about the surveillance possibility as their location could be tracked with the system. The employees' union was involved, but after a while, when no negative consequences were experienced, resistance faded.

At Beta the maintenance organization was reorganized a couple of years ago. Earlier the organization had one production team and one maintenance team responsible for urgent problems. When the maintenance team decided to start walking around the plant and to explicitly search for problems in order to prevent breakdowns, the production team perceived the maintenance team as "acting like police," searching for errors caused by the production team. The daily rounds were viewed as a monitoring mechanism controlling their performance.

The examples described above show how employees are attentive to activities that they think are performed in order to monitor their performance. In this study, however, the respondents reported that these activities have now been accepted as no negative effects were experienced and their purpose has been properly recognized and approved.

4.2 Suppliers Are Aware of the Surveillance Potential of Remote Diagnostics

According to the respondents in this study the primary aim of the remote diagnostics systems is, in all cases, to improve production by preventing unplanned breakdowns due to product errors. However, these systems also enable the monitoring of how the product is used by the operator and maintained by the technicians, thus providing a surveillance possibility that was also mentioned by all suppliers in this study.

The example of the tyre company in the introduction of this paper is an actual case reported by the respondents at PowerDrive. They started receiving regular indications of overloads via the remote system and the cause of the overloads was found in an operator misusing the equipment.

MCC is aware of the possibility of monitoring activities of the customers' employees.

> This is to a large extent a surveillance system. We have taken temperature measurements on drills and with that data you can see exactly how the machine is operated, how long the breaks have been and how long it takes between every shift until the machine is turned on again. (Employee, MCC)

The respondents at MacGregor also recognize the potential for employee surveillance, which is enabled by the monitoring of the crane's performance and time of use. Like MCC, MacGregor can also see how the operator uses the equipment, the time between start-ups and so on. All suppliers in this study are aware of the surveillance possibility with remote diagnostics systems.

4.3 The Suppliers Do not Emphasize the Surveillance Potential When Communicating With Customers

In the design of the business offer and in relation to the customers the suppliers choose not to foreground the surveillance potential of the product. A respondent at MacGregor says that:

> I don't know if the customers are aware of what can be monitored. I don't think the sellers talk much about this system. They don't have much knowledge of the system either. Of course they can talk about the system and show its advantages, but what we monitor they don't know much about… I don't think they [the seller and the customer] discuss it. (Developer, MacGregor Cranes)

Surveillance issues and possibilities of monitoring seem to be pushed into the background. Another respondent from MacGregor confirms this and says that they are aware of the possibilities, but as long as the customers do not react, neither will they:

> We have thought about the surveillance possibility but we aren't concerned about it. We would be if the customers have any opinions, but so far they haven't. So we will deal with it if it arises some day. Gradually they may start to think, what if we give the data to an insurance company or someone else? We have been thinking about the surveillance issue but the customers haven't, so far. (Project leader, MacGregor Cranes)

MCC chooses to handle the surveillance issue in a similar way; as long as the customers and their employees do not object the issue is not discussed.

> The operators don't object since they aren't aware of the monitoring. If they were aware of it they might object. If the management punished them and used the data as evidence they would object, definitely. (Employee, MCC)

4.4 In Remote Diagnostics Visibility Is Lost And Information Collection Can Be Easily Concealed

As these cases have shown, surveillance is possible with remote diagnostics systems and the strategy from a supplier perspective is to keep the issue in the background, which is easy since what is monitored is not visible to the customers! When the technology is embedded into a product the visibility of the monitoring instance is lost. This is not only true for remote diagnostics systems, but for embedded systems in general. In embedded technology the last signs of monitoring are vanishing. For example, the system embedded into MacGregor's cranes is invisible to the operator.

> The crane operator will not get any warnings or alarms. He has to open a special hatch to see the system. To the operator the system says nothing. (Manager, MacGregor Cranes)

Although the operator might know that a system is installed and why, the embedded technology makes it difficult to know what is being monitored.

> PowerDrive had their remote diagnostics system installed in one of our motors, but we don't know what information they got from it. (Technician, Beta)

This technician knew that a system was installed and he knew the purpose of the installation but he did not know what data the system collected as the sensors are hidden in the machine. Furthermore, in this organization the monthly report that is put together is sent to the maintenance manager and not spread in the company so the technician is not automatically informed about the condition of the equipment he or she is working with. The product looks the same regardless of whether the system is installed or not, so the visibility of the surveillance instance is lost with remote diagnostics systems.

4.5 Visible Monitoring Possibilities Evoke Employees' Feelings of Being Monitored While Remote Diagnostics Do Not

One thing common to this study among the respondents was a lack of discussion and objections regarding the surveillance possibilities in remote diagnostics systems. Some respondents were not aware of the possibilities and those who were aware of the possibilities often did not know what data were collected. One explanation from an engineer at Alpha for why there had been no objections towards the surveillance possibilities in remote diagnostics systems was that "everything [in the production process] is computerized today". Employees are thus exposed to these kinds of possibilities all the time. However, if increased surveillance capabilities due to computerization is the only explanation for why users do not perceive remote diagnostics systems as capable of surveillance they would not have reacted to the other situations. As was shown earlier, employees do react to surveillance possibilities, but their reaction occurred in situations when surveillance was visible to them. Regardless of the aim, employees seem to object or at least discuss visible surveillance and its potential consequences. When it comes to remote diagnostics technology and its embedded possibilities, however, there has scarcely been any discussion or objection. Visible functions with indirect monitoring possibilities in contrast evoke employees' feelings of being monitored and of possibly being punished, even though they are informed that this will not happen. Despite their monitoring possibilities remote diagnostics systems do not seem to evoke these feelings, at least not in the studied organizations.

5 Discussion

The aim of this research is to explore how remote diagnostics technology changes surveillance and to consider its ethical consequences by identifying which surveillance dilemmas users and suppliers see in remote diagnostics technology and by analyzing the rationale behind their perspectives.

The primary aim of remote diagnostics technology is to prevent unplanned breakdowns by condition-based monitoring of products. However, as has been shown here these systems are capable of surveillance. It is for example possible to see how an operator has used a product, how long breaks lasted and thereby if the operator has fulfilled the required work assignment. Despite these monitoring possibilities the users in this study have not identified them as a surveillance dilemma or contemplated the surveillance possibilities and their consequences. On the other hand, there were examples when concerns were expressed with regard to monitoring through new routines in the workplace. In none of these cases was the primary aim to monitor the employees, but in the cases of new work routines—tags and new forms to fill in—they were reacting upon the indirect monitoring possibility. The case of remote diagnostics monitoring, however, appears to be different.

By embedding technology into machines at the workplace it becomes invisible for the employees. The literal embeddedness of the technology distinguishes ubiquitous computing from traditional desktop computing. From a user perspective this development brings with it a lack of choices; it is no longer possible to turn the computing device on and off. Moreover the users may not even be aware of the computer hiding in their everyday artefact, and even if the users are aware of it they may not know why it is there or what data it collects.

The embeddedness characterizing ubiquitous technology makes it difficult for users to be aware of the monitoring possibility. The embedded technology does not just hide the possibility of surveillance, it also hides the signs of what is being monitored. With remote diagnostics technology the users do not always know what is controlled, even if they are aware of the installed technology. Apart from hiding the sign of the surveillance possibility, the embedded technology thus also makes it difficult to know what is being monitored.

The suppliers and developers of the remote diagnostics technology who are aware of its indirect surveillance choose to keep this issue in the background, both during the development process and in discussions with customers. Along with the lack of awareness of individuals concerning the surveillance possibility, the whole issue remains hidden. As the surveillance aspects of remote diagnostics technology are pushed or left in the background, and in combination with the embedded technology that hides the cues of the monitoring, the concept of an *embedded panopticon* arises. The embedded panopticon makes the surveillance possibility invisible for the user; he or she cannot see it and be aware of it.

The embedded panopticon is a metaphor to highlight the indirect possibility of a supervised workplace brought about by ubiquitous technology, as the original panopticon cannot shed light on all characteristics of the technology and its effects. The issue of visibility is the main difference between the original panopticon and the contemporary surveillance capabilities in ubiquitous computing. As has been shown in this study visibility is also a crucial concern for whether surveillance dilemmas are identified and discussed.

The issue of informing individuals that they are being subjected to monitoring is vanishing as a result of ubiquitous computing. As the technology becomes embedded the individuals will not even know that they are users of an IT artefact, if they are not explicitly informed somehow. Another visibility issue concerns clarity of what is being monitored. The embedded technology does not only hide the signs of possible surveillance, it also hides the signs of what can be monitored. When the users receive no sign of the monitoring instance or information about it they are consequently unable to understand what is being monitored. A third visibility issue is to make the aim of the surveillance visible to the individuals. As both the sign of the monitoring and information about what is being monitored are hidden, the aim of the monitoring will also be obscure. As a result, these visibility issues create an embedded panopticon: a possibility of a pervasive supervised workplace hiding in the environment.

The embedded panopticon raises a number of ethical issues. Should the suppliers inform the customers about the indirect employee monitoring possibilities, or is this not necessary? As long as nothing happens and the data are not abused, for example for punishment, will this information just lead to unnecessary discussions and objections? Or is it everybody's right to be informed and to decide how he or she wants to behave during monitoring? The embedded panopticon gives the actors with knowledge of the technology the possibility of answering these questions, while others will not even know that the questions could be asked.

This study shows how visibility and non-visibility are of decisive importance in determining how employees will react to monitoring possibilities in the workplace. In contrast to an earlier study by Gattiker and Kelly (1999) which showed that users were able to understand ethical dilemmas in computer use, this study shows that there is a lack of problem recognition and understanding of ethical dilemmas from a user perspective. The results of this study thus confirm Conger and Loch (1995), who claim that people are not able to draw analogies from computing situations to offline circumstances. In the case of remote diagnostics, people often do not even know that they are users of technology, which makes them unable to see potential dilemmas of the embedded work routines.

As long as no one objects it seems that the case companies will continue to develop without considerations of how surveillance should best be dealt with. All three suppliers in this study, MacGregor, PowerDrive, and MCC, are aware of the surveillance power of the data, but as long as the customers do not react they will not bring the question of surveillance to the fore. Since the technology is embedded the customers' employees cannot easily know about the surveillance possibility. Consequently, they will probably not object as long as the systems are not used in a way that negatively influences them or for other forms of interference or punishment. The embedded technology thus even embeds the questions of surveillance.

6 Implications and Conclusions

The aim of the research presented has been to explore how remote diagnostics technology changes surveillance and to consider its ethical consequences by studying which surveillance dilemmas users and suppliers see in the technology and by analyzing the rationale behind their perspectives.

Ubiquitous computing transfers technology from the office into everyday private and professional environments, and in the case of remote diagnostics technology to the plants and factories and the daily work of operators and technicians. This paper shows how visibility and non-visibility are of decisive importance in determining whether or not users can examine ethical dilemmas in computer use as visibility seems to be what triggers employees' feelings of being monitored or not. Despite their monitoring possibilities remote diagnostics systems do not seem to evoke such feelings. By embedding technology and thereby also monitoring into physical objects, the technology and the cues of surveillance are vanishing, both literally and virtually for the user. For the user, the direct reminders of surveillance are embedded in technology, thus creating an embedded panopticon.

With respect to practice this paper informs both suppliers of embedded technologies and customers who adopt the technology in their organizations. For both types of companies the embedded monitoring possibilities challenge their business ethics and should trigger them to pick a strategy of how to handle ethical questions.

Ubiquitous technology shows promising potential in enabling new types of usage, for example in preventing costly breakdowns of motors, but as has been shown in previous information systems research, the effects of IT are emergent and organizational consequences of IT indicate contradictory evidence with many examples of unintended consequences (Orlikowski 1992; Robey and Boudreau 1999).

With respect to research, this paper presents one way of how to study embedded technologies and their consequences. As the technology may be as invisible for the researcher as it is for many users, a user's perspective may not be enough. A broader perspective, as adopted in the work presented here, which also includes other actors for example—providers and developers—is thus required. These actors can help researchers to understand both the technology itself as well as its consequences.

Acknowledgement

The European Union's regional development fund, the Kempe foundation and ProcessIT funded this study. Thanks are due to the reviewers and associate editor for useful comments on an earlier draft of this paper. Thanks are also due to Ulrika H Westergren for the important role she played in collecting the data.

References

Albrechtslund, A., "The postmodern panopticon: Surveillance and privacy in the age of ubiquitous computing," in Proceedings of CEPE 2005, Sixth international conference of computer ethics: Philosophical enquiry, Enschede, Netherlands, July 17-19, 2005.

Araya, A., "Questioning ubiquitous computing," in Proceedings of the 1995 ACM 23rd annual conference on Computer science. Available at: doi.acm.org/10.1145/259526.259560, Nashville, TN, USA, Feb 28- March 2, 1995.

Bain, P., and Taylor, P., "Entrapped by the 'electronic panopticon? Worker resistance in the call centre," *New Technology, Work and Employment*, (15:1), 2000, pp. 2-18.

Banavar, G., and Bernstein, A., "Challenges in design and software infrastructure for ubiquitous computing applications," *Advances in computers*, (62), 2004.

Bohn, J., Coroama, V., Langheinrich, M., Mattern, F., and Rohs, M., "Living in a world of smart everyday objects: Social, economic, and ethical implications," *Human and Ecological Risk Assessment*, (10:5), 2004, pp. 763-785.

Boyne, R., "Post-Panopticism," *Economy and Society*, (29:2), 2000, pp. 285-307.

Cas, J., "Privacy in pervasive computing environments: A contradiction in terms," *IEEE Technology and Society Magazine*, (Spring), 2005, pp. 24-33.

Conger, S., and Loch, K. D., "Ethics and computer use," *Communication of the ACM*, (38:12), 1995, pp. 30-32.

Cuff, D., "Immanent domain: Pervasive computing and the public realm," *Journal of Architectural Education*, (57), 2002, pp. 43-49.

DeGeorge, R. T., *The ethics of information technology and business*, Blackwell publishing, Malden, MA, 2003.

Eisenhardt, K. M., "Building Theories from Case Study Research" *Academy of Management Review*, (14:4), 1989, pp. 532-550.

Fernie, S., and Metcalf, D., 22 "(Not) hanging on the telephone: Payment systems in the new sweatshops," Centre for Economic Performance, London School of Economics.

Foucault, M., *Discipline and punish: The birth of the prison*, Peregrine Books, London, 1979.

Gattiker, U. E., and Kelley, H., "Morality and computers: Attitudes and differences in moral judgments," *Information Systems Research*, (10:3), 1999, pp. 233-254.

Hong, J. I., and Landay, J. A., "An architecture for privacy-sensitive ubiquitous computing," in Proceedings of the 2nd international conference on mobile systems, applications and services (MobiSys 2004), Boston, MA, USA, June 6-9, 2004, pp. 177-189.

Jendricke, U., Kreutzer, M., and Zugenmeier, A., "Mobile identity management," Workshop on Security in Ubiquitous Computing (Ubicomp), Göteborg, Sweden, Sept 29, 2002.

Johnson, D. G., "The public-private status of transactions in computer networks," in: *The information web: Ethical and social implications of computer networking,* G. C.C. (ed.), Westview Press, Boulder, CO, 1989, pp. 37-55.

Kautz, K., and McMaster, T., "Introducing structured methods: An undelivered promise? A case study," *Scandinavian Journal of Information Systems*, (6:2), 1994, pp. 59-78.

Koskela, H., "'Cam Era': The contemporary urban Panopticon," *Surveillance and Society*, (1:3), 2003, pp. 292-313.

Lahlou, S., Langheinrich, M., and Röcker, C., "Privacy and trust issues with invisible computers," *Communication of the ACM*, (48:3), 2005, pp. 59-60.

Langheinrich, M., "Privacy invasions in ubiquitous computing," Workshop on Socially-informed Design of Privacy-enhancing Solutions (Ubicomp 2002), Göteborg, Sweden Sept 29, 2002.

Langheinrich, M., "Personal privacy in ubiquitous computing. Tools and system support," Publisher, Place Published, 2005.

Lyon, D., *Surveillance society: monitoring everyday life*, Open University Press, Buckingham, 2001.

Lyytinen, K., and Yoo, Y., "Issues and challenges in ubiquitous computing," *Communications of the ACM*, (45:12), 2002, pp. 63-65.

Mason, R. O., “Four ethical issues of the information age,” *MIS Quarterly*, (10:1), 1986, pp. 5-12.

Orlikowski, W. J., “The duality of technology,” *Organizational Science*, (3:3), 1992, pp. 398-427.

Park, S. H., Won, S. H., Lee, J. B., and Kim, S. W., “Smart home - digitally engineered domestic life,” *Personal and Ubiquitous Computing*, (7:3-4), 2003, pp. 189-196.

Peppard, J., “Bridging the gap between the IS organization and the rest of the business: plotting a route,” *Information Systems Journal*, (11:3), 2001, pp. 249-270.

Poster, M., *The second media age*, Polity, Cambridge, 1995.

Robey, D., and Boudreau, M.-C., “Accounting for the Contradictory Organizational Consequences of Information Technology: Theoretical Directions and Methodological Implications,” *Information Systems Research*, (10:2), 1999, pp. 167-185.

Sayer, K., and Harvey, L., “Empowerment in business process reengineering: an ethnographic study of implementation discourses,” in Proceedings of the 18th International Conference on Information Systems, Atlanta, GA, 1997, pp. 427-440.

Shell, J. S., “Taking control of the panopticon: Privacy considerations in the design of attentive user interfaces” CSCW 2002 workshop on privacy in digital environments: Empowering users, New Orleans, LA, USA, Nov 16, 2002.

Sipior, J. C., and Ward, B. T., “The ethical and legal quandary of email privacy,” *Communication of the ACM*, (38:12), 1995, pp. 48-54.

Timmons, S., “A failed panopticon: surveillance of nursing practice via new technology,” *New Technology, Work and Employment*, (18:2), 2003.

Weckert, J., “Computer ethics: Future directions,” *Ethics and Information Technology*, (3), 2001, pp. 93-96.

Weiser, M., “The computer for the 21st century,” *Scientific American*, (Sept), 1991, pp. 66-75.

Yin, R. K., *Case study research: Design and methods*, Sage, Newbury Park, 1989.

Zuboff, S., *In the age of the smart machine: The future of work and power*, Basic Books, New York, 1988.