Poiesis Prax (2008) 5:265–290
DOI 10.1007/s10202-007-0041-z

ORIGINAL PAPER

Ubiquitous technologies, cultural logics and paternalism in industrial workplaces

Katharina E. Kinder · Linden J. Ball · Jerry S. Busby

Published online: 11 December 2007

Abstract Ubiquitous computing is a new kind of computing where devices enhance everyday artefacts and open up previously inaccessible situations for data capture. 'Technology paternalism' has been suggested by Spiekermann and Pallas (Poiesis & Praxis: Int J Technol Assess Ethics Sci 4(1):6–18, 2006) as a concept to gauge the social and ethical impact of these new technologies. In this article we explore this concept in the specific setting of UK road maintenance and construction. Drawing on examples from our qualitative fieldwork we suggest that cultural logics such as those reflected in paternalistic health and safety discourse are central in legitimising the introduction of ubiquitous computing technologies. As such, there is little doubt that paternalism plays an essential role in people's reasoning about ubiquitous computing in this setting. We argue, however, that since discourses such as health and safety are used by *everyone* (including both managers and workers) in the organisation to further their own aims, technologies transcend purely paternalistic conceptualisations and instead become a focal point for ongoing struggles for control between those deploying and using them. This means that the benefits and costs of such new technologies become harder to define from an ethical and social perspective.

Resumé L'ubiquité informatique ou 'Ubiquitous computing' en anglais est un nouveau concept qui décrit la manière avec laquelle l'embellissement des objets

K. E. Kinder (✉) · J. S. Busby
Department of Management Science, Lancaster University Management School, Lancaster LA1 4YX, UK
e-mail: k.kinder@lancaster.ac.uk

J. S. Busby
e-mail: j.s.busby@lancaster.ac.uk

L. J. Ball
Department of Psychology, Lancaster University, Lancaster LA1 4YF, UK
e-mail: l.ball@lancaster.ac.uk

du quotidien se fait de manière électronique et conséquemment nous permet de découvrir de nouvelles situations, qui étaient auparavant inaccessibles, d'obtenir des donnés. Spiekermann et Pallas (Poiesis & Praxis: Int J Technol Assess Ethics Sci 4(1):6–18, 2006) propose le concept de 'paternalisme de technologie' pour explorer et examiner les conséquences sociales et éthiques de cette nouvelle forme de technologie. Dans nos travaux, nous examinons cette proposition en utilisant une étude sur l'industrie de construction des routes en Grande-Bretagne. Nous utilisons des exemples qui sont basés sur nos donnés qualitatives et suggérons que la construction des logiques culturelles, qui s'expriment dans le cadre du discours paternaliste autour du thème de 'la santé et la sécurité' (au travail), soit très important pour rendre légitime l'introduction des technologies de l'ubiquité informatique. La proposition du system de paternalisme de technologie joue un rôle important et influent dans le raisonnement du rôle de la technologie d'ubiquité dans ce contexte. Cependant, puisque le discours sur le thème de la santé et la sécurité est utilisé par tous les employés de chaque organisation, indépendamment de sa position hiérarchique, y sont inclus la direction tout aussi bien que les travailleurs, nous soutenons que, l'avancement d'un débat unique qui soutiendrait davantage une certaines forme de pensés et ses différentes formes de technologies, encouragent une tension continuelle entre ceux qui les contrôlent et ceux qui les utilisent. Dans ce contexte il devient plus difficile de définir les avantages et désavantages de ces nouvelles formes de technologie d'un point de vue sociale et éthique.

Zusammenfassung Ubiquitous Computing ist eine neue Art von Informationsverarbeitungstechnologie, bei der Gegenstände des Alltags elektronisch erweitert und vormals nicht erreichbare Gebiete der Datenerfassung zugänglich gemacht werden. „Technologiepaternalismus" ist ein von Spiekermann und Pallas (Poiesis & Praxis: Int J Technol Assess Ethics Sci 4(1):6–18, 2006) vorgeschlagenens Konzept zur Einschätzung der sozialen und ethischen Auswirkungen solcher neuen Technologien. Im vorliegenden Text untersuchen wir dieses Konzept am Beispiel der Straßenbauindustrie in Großbritannien. Unter Bezug auf Beispiele aus unserer qualitativen Feldfoschung schlagen wir vor, dass kulturelle Logiken, wie sie im paternalistischen Diskurs um 'Health and Safety' zum Ausdruck kommen, bei der Legitimation der Einführung von Ubiquitous-Computing-Technologien entscheidend sind. Technologiepaternalismus spielt damit zweifellos eine entscheidende Rolle in der Argumentation der Betroffenen im untersuchten Zusammenhang. Wir vertreten jedoch die Auffassung, dass, da Diskurse wie „Health and Safety" von allen in der Organisation (d.h. sowohl vom Management als auch von den Arbeitern) verwendet werden, um die eigenen Ziele zu verfolgen, die Technologien über eine paternalistische Konzeptualisierung hinausgehen und zum Schwerpunkt andauernder Auseinandersetzungen um die Kontrolle zwischen den an Einführung und Nutzung Beteiligten werden. Damit wird es aus einer sozialen und ethischen Perspektive schwieriger, die Vor- und Nachteile solcher Technologien zu bestimmen.

1 Introduction

Ubiquitous computing, where devices are seamlessly embedded within everyday artefacts in order to enhance familiar situations, is a very tempting vision of a new kind of computing. Marc Weiser suggested the term 'ubiquitous computing' in 1988 to describe a future in which invisible computers make personal desktop computers obsolete: "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it" (Weiser 1991).

The main characteristics of ubiquitous computing systems are invisibility and a focus on communication, mobility' smart tools and new forms of interaction (Weiser 1993). Hardware is said to 'disappear' in everyday situations (Want et al. 2002). Since Weiser's definition, computer scientists have been working on a variety of application scenarios aiming to make this vision come true. Ubiquitous technologies have been introduced into hospitals and nursing homes (Hansen et al. 2006; Drugge et al. 2006; Stanford 2002), vineyards (Burrell et al. 2004), police cars (Kun et al. 2004) and other non-office environments such as road construction sites (Davies et al. 2005). Although more complex systems usually have not yet gone further than the trial stage, new technologies such as RFID tags, wearable computing devices and other location and sensing systems have been developed. Closed Circuit TV (CCTV) cameras and GPS navigation systems in cars have become part of our daily lives. This development is beginning to change our world by taking computer technologies out of the office so as to create a whole 'internet of things' (Fleisch and Mattern 2005).

Although many people see a great potential for ubiquitous technologies to change our world for the better (e.g. in terms of health monitoring, crime prevention and asset management; see Greenfield 2006) there are also many critics who address potential problems such as the fact that ubiquitous computing may threaten people's privacy and security (e.g. through the acquisition of previously inaccessible data about actions and behaviours; for a discussion of the issues connected with privacy see Roussos and Moussouri 2004). A concept that has been developed to focus the discussion concerning potentially negative consequences of ubiquitous computing is that of 'technology paternalism' (Spiekermann and Pallas 2006). This concept aims to capture the fact that whilst many of the new technologies are supposed to be 'for our own good' they can end up embodying such extreme levels of automated rule-based control that it may become difficult for people to override systems and retain the 'right for the last word'.

In this article we explore the issue of technology paternalism in the setting of road construction and maintenance. Our research was motivated by three key questions. First, what do the settings look like into which technologies are being introduced? Second, what do the technologies that are being developed and deployed look like? Third, who are the stakeholders and users in these settings and what are their various roles? We will unpack these three questions in more detail below and explain why they were influential in driving our research. Suffice it to say for now that one of our key concerns was that the concept of technology paternalism

may need to be extended in order to capture the nuanced realities associated with the deployment of ubiquitous computing in real-world work contexts.

To begin the analysis of issues relating to paternalism and ubiquitous technologies we start off by examining the difficulties associated with defining ubiquitous computing as a bounded domain of technological development. This leads us to propose an encompassing view of ubiquitous technologies for the purposes of analysing the contemporary social and cultural contexts of their emergence. We then move on to review current critiques of ubiquitous computing in the social science literature, focussing particularly on Spiekermann and Pallas' concept of technology paternalism. We propose that whilst paternalism can play an influential role in instigating the introduction of ubiquitous technologies it may well be the case that not all ubiquitous systems are designed to be controlling, and, even if they are so designed, they may not end up achieving the intended effect. Indeed, a considerable body of research has shown that unforeseen modes of use emerge around new technologies and that it is the users who create and communicate the meaning these technologies have (Dourish 2001). Likewise, it is not always clear who gains from the introduction of ubiquitous technologies or where the balance of power lies in a specific scenario, since 'subjects' (e.g. supervised operatives) may gain levels of control that, in fact, give them power over the 'patrons' who sanction the introduction of the technologies in the first place. After outlining possible limits of technology paternalism, we then overview some of our own fieldwork relating to the design, deployment and use of ubiquitous technologies in an industrial environment. Our findings confirm that there are complexities and subtleties relating to the control and power relations connected with the introduction of ubiquitous computing in real-world contexts. We propose that these complexities and subtleties can only be addressed effectively by placing an emphasis on the specific application contexts associated with technology introduction. Such contexts are, we argue, usefully characterised in terms of broader contemporary discourses or so-called 'cultural logics' (Ong 1999). Only by examining the particular cultural conditions at the time of their emergence can we understand technologies (Escobar 1994) and why they appear.

2 Defining the nature and scope of ubiquitous computing

Although some of the features of ubiquitous computing are apparent in many new technologies (for example one could argue that CCTV cameras are more or less seamlessly embedded into public space), they are usually not wholly 'ubiquitous' (CCTV cameras are neither necessarily 'smart' or mobile, nor do they focus on communication) and it is hard to distinguish between 'ubiquitous' technologies and those that are not; indeed the question is whether truly 'ubiquitous' systems actually exist. Even the ubiquitous computing research community is divided upon the importance of topics such as embeddedness, interaction, seamlessness, calmness and their impact. Often developers prefer to describe their work as taking place in areas such as 'mobile sensor networks' or 'pervasive computing'. In many cases neither the ubiquitous computing community nor the critics of ubiquitous

computing have anything but Weiser's vision to go on from, and most researchers agree that fully 'ubiquitous' systems very rarely exist. Rather, ubiquitous computing needs to be seen more as something of a 'trend' within new technology development.

In order to assess the implications of ubiquitous computing we have to look at technologies that possess features of the envisioned technologies such as mobility, pervasiveness and surveillance. From these we may be able to identify which cultural logics are important and shape design and use of new ubiquitous technologies. The line between existing technologies that have some 'ubiquitous' features and 'ubiquitous computing' as such is not always easy to draw. For example, surveillance in general is not necessarily always a ubiquitous computing issue, but surveillance with tracking systems in places where there used to be no possibility of data capture may be 'ubiquitous computing'. However, in order to research people's attitude towards surveillance and how this changes people's behaviour or has an impact on existing power relations it may be necessary to look at both. In the following we will nevertheless be using the term 'ubiquitous computing' or 'ubiquitous technologies' in order to focus discussion and to make it clear that we are talking about the realm of *new, networked and embedded mobile computing technologies*, as opposed to more traditional desktop computers.

3 Contemporary critiques of ubiquitous computing

Despite the difficulties in definition and the unpredictability of where development may be going, ubiquitous computing has recently become a focus of the social science literature. Attempts have been made to assess the impact of ubiquitous computing systems as they are envisioned and deployed. Many of these texts are very critical of these new technologies seeing them as "an attempt at a violent technological penetration of everyday life" (Araya 1995) or as a vision that threatens with 'totality' and therefore totalitarianism (Adamowsky 2000). Most critics concentrate on the topics of privacy, surveillance and data security (Brey 2005), although other categories of criticism include 'marginal perceived value', 'false promise' and 'loss of control' (Rohs 2002). The technologies are assumed to have unforeseen impacts as they "will transfigure our notions of space and time, self and other, citizen and society in ways that we haven't begun to contemplate" (Greenfield 2006). Most authors therefore demand that ubiquitous computing and its development will have to be monitored closely, in order "to steer this development in a direction that has more in common with Weiser's optimistic vision of the 21st century than with the depressing mix of consumer terror and police state conjured up by Steven Spielberg in his movie 'Minority Report'" (Bohn et al. 2004).

Social scientists seem to agree that ubiquitous computing needs to be studied and focussed on by social and cultural studies (Galloway 2004). They call for a wide public discussion about ubiquitous computing with a deeper involvement of the people affected (Spiekermann and Pallas 2006) in order to develop policies that allow us to build "a pervasive computing world that is empowering and liberating, rather than irritating and oppressive" (Stajano 2002). A concept that has been

proposed in order to provoke and focus such a discussion is that of 'technology paternalism'.

4 Technology paternalism

Generally, the concept of 'paternalism' originates in the idea of a father looking out for his children, but usually it means an authority that undertakes to supply the needs of, or to regulate the conduct of, those under its command. Such paternalism is often seen as repressive since whilst it claims to be in people's own best interests (protecting them and satisfying their needs) it actually removes their freedom and responsibility. The term 'technology paternalism' was proposed by Spiekermann and Pallas (2006) to describe the way in which ubiquitous technologies can control people in intelligent environments. They define 'technology paternalism' as the "uncontrolled autonomous action of machines that cannot be overruled by object owners" (Spiekermann and Pallas 2006). They further propose that since technologies will often have the capacity to sense what is rightful and what is not they will limit people's actions, thereby becoming paternalistic. Indeed such technologies may not only require obedience but command total compliance. The authors fear that people may be subdued to machines' autonomous actions and may lose control in environments that are "supposed to be totally automated". Thus, with ubiquitous computing, a new type of "potentially paternalistic interface would come into being: the objects people use or are surrounded with" (Spiekermann and Pallas 2006).

These notions capture very well the arguments that are in currency both among designers, stakeholders and critics of ubiquitous technologies. Designers are tempted by the idea of systems that have the potential to improve everyday life by making it impossible for people to behave in a 'risky' way. Stakeholders such as companies introducing ubiquitous technologies may prefer a proactive approach in a system in order to extend control. And the loss of control and the feelings of exclusion and infantilisation that critics voice, for example, when they talk about 'nanny culture', are very well captured by the term 'technology paternalism'.

4.1 Are the situations into which the technologies are being introduced paternalistic to begin with?

In our opinion, the definition of technology paternalism provokes an immediate question, which is whether the situations into which the technologies are being introduced are paternalistic to begin with. If this is the case then the new technologies merely reproduce a paternalistic system that was already in place by enforcing existing regulations. This question itself raises further issues concerning what it is exactly that is *new* about ubiquitous computing, and whether the technological paternalism is of a different quality to what pre-existed.

In order to answer these questions we need to look at the conditions under which the technology introduction happens and the reasons for it, which, we propose,

requires a focus on contemporary cultural logics. Technology clearly emerges under specific cultural conditions, which means that it is inevitably culturally constructed. Technologies then again have an influence on these social and cultural conditions, in a repeating co-constitutive cycle (Introna 2007). Escobar (1994) has likewise explained how new technologies are based on cultural constructions and reconstructions which they, in turn, help to shape. Every technology represents a cultural invention and emerges out of particular cultural conditions and then, in turn, helps to create new cultural conditions (Escobar 1994). Several recent anthropological and ethnographic works have validated such theorising by demonstrating that economic, scientific and technological aspects need to be seen in their cultural contexts and cannot be understood without them (e.g. Downey 1998; Escobar 1994; Ilyes 2003; Rabinow 1999).

Instead of defining culture as distinct from more 'rational' institutions such as economies, legal systems or even states, it is necessary to investigate the 'cultural logics' that shape these institutions. Ong (1999) explains how everyday human actions, motivations and struggles are influenced by specific cultural logics. Individuals then respond fluidly and opportunistically to changing conditions by adopting strategies within the specific contexts of power in which they find themselves. In our research area an example of such a cultural logic would be the general debates and discourses surrounding 'health and safety' that can influence the everyday structure and organisation of workplaces. Looking at the various discourses and practices that emerge around and through new technologies as 'cultural logics' allows the researcher to examine the local impact of global processes on specific workplaces by grounding research in relevant contemporary changes. Such changes, for example, globalisation, modern information and communication media and deregulated work practices, not only question traditional frontiers between nations but also challenge the distinction between online and offline, between virtual and real and between private life and work life. Due to these challenges, concepts and definitions of culture have been developed that stress the complexity of cultures: Cultures are no longer autonomous and only bounded to a certain degree (Hannerz 1992). In fact, only a fluid concept of culture makes it possible to study technology in contemporary work situations and to identify various cultural logics that influence such situations. As will be explained later, it has become very difficult to disentangle the various logics and influences that have an impact on an organisation such as a company as traditional distinctions become less important.

To describe the impact that cultural logics have on technology design, deployment and use, we are proposing to view the process as one of 'theming'. This refers to the logic of assemblage, of recombination, extraction and reduction on easily recognisable signifiers—in short, the method of theme park building. Theming means the application of a narration to an object. Typically the source of the theme is different from the object regarding space, time, topic (or all of these) and therefore generates a "veneer of meaning and symbolism to the objects to which it is applied" (Bryman 2004). There are comprehensive sources for theming: History, movies, geography, social organisation, art and literature provide rich sources for possible combinations and scenarios. Theming is not only applied in

theme parks but has spread over all areas of society. Mostly this phenomenon is referred to in terms such as "Disneyization" (Bryman 2004) or "McDonaldization" (Ritzer 2004) to point out its US-American roots and the strong commercialisation of certain sectors such as tourism. When interacting with technology—and also when introducing it into the organisation—people theme the technology referring to specific cultural logics; for example, the management might see a new GPS system as a way of improving 'health and safety' in the workplace and the drivers in whose vans the system is installed might potentially see it as a 'control instrument', as a 'toy' or as a 'status symbol'. Indeed, we saw examples of all of these various kinds of theming during our fieldwork, but the most striking and prevalent theme applied by all of the people we observed related to health and safety. We believe that a particularly valuable aspect of the concept of 'theming' is the way in which it captures the dependence of technology perception on specific situations and contexts, without losing the perspective of globally applicable logics and structures.

4.2 What do systems look like in terms of levels of automation and control?

A second key question that arises during a consideration of the concept of technology paternalism concerns the issue of what a ubiquitous computing system looks like. Spiekermann and Pallas' (2006) approach implies a clear definition of ubiquitous computing—but as mentioned before, this is unclear even in the ubiquitous computing community. The vision of full automation seems to have little in common with actual scenarios and the designs of various ubiquitous computing systems are, in fact, very diverse and not necessarily only proactive or 'totally automated'. An example of such a scenario is the trial of a highly interactive system which Roduner et al. (2007) conducted. Mobile phones were used in order to operate a variety of appliances in different task settings and although this included the collection of data about individuals' actions the actions themselves needed to be triggered by the users who could then operate devices such as dishwashers and printers using their mobile phones as 'remote control'.

Spiekermann and Pallas' hypothesis assumes a system that in this way does not yet exist and therefore is difficult to assess. Our assumption is that the actual systems that emerge out of the complex design processes in ubiquitous computing may indeed have autonomously acting components. However, the specific application scenarios may be quite complex and interactive so that it becomes important to research key issues such as: where decision-making processes reside, who benefits from the system and in what way, and how the system integrates into existing structures of power and control. When Spiekermann and Pallas claim that "people may be subdued to machines' autonomous actions", it needs to become clearer who these people are. Is there more control for some than before and less for others? Or is there more or less the same amount of control for all but of a different quality? Deleuze (1992) describes such a change of control in his concept of the 'societies of control'. In these, forms of free-floating control have replaced the old disciplines, which were typical of classic disciplinary institutions such as hospitals, the military or factories. Control societies promise more flexible systems of power

relations. However, these may as well turn out to be just as harsh as the former confinements. The rise of observation systems is just one example of this process. In these new and different spaces of internment individuals pass through various independent spaces governed by different variables and paradigms. These different control mechanisms are nevertheless inseparable variations or 'modulations' of control that will change from one moment to another (Deleuze 1992).

4.3 Who are the stakeholders and users of the technologies and what are their roles?

A third question that arises when considering technology paternalism in a ubiquitous computing context concerns the roles of the various stakeholders and users associated with such technologies. For example, there are often specific economic and governmental interests that dictate the introduction of ubiquitous computing, so it becomes questionable who the patrons of technology paternalism actually are in the first place. Spiekermann and Pallas (2006) discuss three groups of potential patrons: the engineers who design ubiquitous technologies, the marketers who promote them and the regulators who influence application design. Certainly, corporate financial benefits could be a key driver of technology paternalism. Often the patrons' motivation to implement a paternalistic design is that they want to reduce their own insurance liabilities arising from potential indemnifications to victims of accidents. But, according to Spiekermann and Pallas, technology that is controlling should only be used to limit an action when that action causes costs to stakeholders other than the person or institution making it (e.g. the decision to pollute the atmosphere has impacts beyond the individual or organisation causing the pollution). Any other use of such technology should, they argue, be considered paternalistic and be avoided.[1] As such, they propose that "if people take the risk and harm themselves through drilling without glasses, then that is their choice and they have to bear the consequences" (Spiekermann and Pallas 2006).

We would suggest, however, that the situation is often more complicated than Spiekermann and Pallas propose. For example, due to contracting or subcontracting obligations an employer may be forced to ensure the adherence to specific health and safety regulations in order to fulfil their contract with a client. Also, employers have to be very careful to ensure that they have done everything to make the workplace safe; apart from the fact that accidents are tragic and also costly, employees can sue for compensation in case of an accident, which means that employers have the choice of either adopting a paternalistic stance or being sued by employees who have become used to being able to sue the state or companies for compensation in the case of accidents. It almost seems as if paternalism 'strikes back': We can still discuss whether we should have more or less paternalism but we also need to deal with the consequences of the possibilities that arise by this trend.

[1] This seems to merely translate the question into another one: Who gets to decide what is good for the general public? The problem of whether machines should assist or prevent specific behaviour remains. In order to solve this dilemma we need to find out who is responsible for making these decisions and how it happens that they need to be made at all.

Stakeholders might still be able to reflect upon ubiquitous computing using technology paternalism as a conceptual basis for discussion but they also have to deal with paternalism 'in effect'. They have to make sure that they do not lose out by not following the rules of a society where paternalistic behaviour is not only expected but also legally enforced. We therefore need to look at what motivates patrons: What kind of changes or social and cultural logics cause employers to become patrons of ubiquitous computing?

Also, apart from obvious stakeholders such as designers or companies, a fourth group of potential patrons of ubiquitous computing are the users of the technologies. Their impact on design, deployment and modes of use needs to be researched in order not to neglect potential backflow and 'backtalking' by assuming 'total control' where this may in fact not be achieved. Technologies are not just paternalistic and controlling but, indeed, everyone faced with them will aim to define situations of use with the available discourses to their own advantage—for example when workers subvert a specific system because it is too awkward or cumbersome.[2] Individuals faced with a new technology can make use of it in unexpected ways. There may also be cases where people are clearly using ubiquitous technologies intended to monitor them to their own advantage and it may not always be easy to say who benefits from such technologies.

5 Exploring technologies and paternalism

We established above that there are three questions that are of interest in connection with the concept of technology paternalism:

- What do the situations look like into which the technologies are being introduced (in particular, are they paternalistic to begin with)?
- What do systems look like in terms of levels of automation and control?
- Who are the stakeholders and users of the technologies and what are their roles?

In order to explore these questions we decided to adopt a qualitative approach to gain an in-depth understanding of stakeholders' and users' motivations and the specific application scenarios of ubiquitous technologies. We therefore pursued a two-year study of such a specific scenario, namely the workplaces at a major UK maintenance and construction company (henceforth referred to as company X). In recent years this company has been introducing various location and monitoring systems and has also been cooperating with the independent research and development project NEMO[3] at Lancaster university in testing and developing a ubiquitous vibration exposure monitoring technology.

[2] For example, this happened in our project when workers rejected wrist-mounted units in favour of mobile phone-style ones.

[3] http://www.comp.lancs.ac.uk/nemo.

6 Methods

For our research we used ethnographic methods such as participant observation and interviews. Data were collected over 2 years. The interviews were conducted by two researchers and interview partners were drawn from a variety of managerial levels and functions within the organisation. We also interviewed administrators and other office personnel at depots, foremen and working crew members who were involved in design, deployment or use of the researched technologies. The daily happenings at depots and the work practices on sites, in offices and mess halls were observed. Additional material such as posters, circulars, health and safety bulletins, memos and strategy plans were used to complement the observation and interviews; this material was then compared with material by other parties, e.g. Highways Agency publications or legal texts. Also, we observed decision-making processes about technologies to be introduced in meetings between the management and designers.

Generally our approach was as open as possible in order to allow interview and observation partners to introduce topics themselves and also to accommodate the unexpectedness in a very unpredictable field. For example, construction sites on motorways proved to be a very labile environment, characterised by sudden changes in plans and the need to react quickly to incidents and unforeseen problems. Interview and observation partners and their work practices had to be accommodated and often conversations would take place while driving in vans or having tea in mess halls. The collected data were then transcribed and analysed in an iterative way, repeatedly going back to initial transcripts in order to ensure data were as grounded as possible.

In the following we will outline four examples from our fieldwork at company X in order to explore the concept of paternalism and technologies in this setting. We will present these data in the form of four cases, staying very close to the actual happenings at company X as we experienced them.

7 Background to the cases

Company X is a major road construction and maintenance company in the UK. It has area contracts with the English Highways Agency to maintain high-speed roads, and also with local county councils to maintain and construct local road networks. The Highways Agency encourages several companies to bid for area contracts, and this results in a variety of contracts and subcontracts for each area. Likewise, not all councils have outsourced all maintenance and construction work and also when such outsourcing does arise, it may involve multiple companies. In addition, company X also uses sub-contractors for specific types of work. This situation becomes even more complicated not only because contracts and therefore responsibilities and alliances change over time, but also because of other schemes. Government initiatives like the Public Private Partnerships[4] and resulting DBFO

[4] http://www.hm-treasury.gov.uk/documents/public_private_partnerships/ppp_index.cfm.

(Design, Build, Finance, Operate) schemes since 1996[5] create exceptions and special circumstances for specific types of work. This whole structure leads to a heightened need to prove which work has been done by whom. Company X's management is therefore very interested in gathering as much data as possible about what is going on in the workplaces.

7.1 Health and safety at company X

The workplaces at company X were mostly in high-risk environments since construction and maintenance sites are typically located on public roads. Especially on high-speed roads heavy machinery and tools posed hazards and there was also the risk of road accidents. In addition, there were long-term health risks for the workers, for example, caused by the exposure to noise and vibration (when operating vibrating tools such as jackhammers). Due to these risks health and safety was very important for company X.

Apart from the concern for workers' wellbeing, there were three other reasons why health and safety were very important topics for company X and its employees. First, company X had to conform with the health and safety law, especially with the Health and Safety at Work Act from 1974 and numerous regulations such as the Control of Substances Hazardous to Health (COSSH) Regulations from 2002. Second, there was pressure from clients such as local county council authorities or the Highways Agency to improve health and safety. Therefore health and safety was a 'seller' in the bid for new contracts, and company X aimed to be seen as adopting cutting edge procedures and technologies in this important area. Third, there were liability issues to be considered: If company X did not provide safe workplaces it could be sued for compensation by injured employees or members of the public, for example, when traffic management was insufficient and therefore dangerous to drivers, or when workers suffered long-term damage such as loss of hearing (Stranks 2005).

The importance of health and safety resulted in a heightened awareness of the topic on all levels of company X's organisation. Training was provided and material was continuously being circulated amongst employees. Health and safety was the most frequent topic of posters and leaflets in mess rooms and hallways. Also, health and safety adherence amongst workers was enforced by taking disciplinary action against workers who did not comply with health and safety rules. For example, a worker could be reprimanded for not wearing personal protective equipment such as a high visibility jacket. Company X was constantly trying to improve health and safety standards in the workplace.

Therefore company X was interested in introducing new (ubiquitous) technologies that would enforce adherence to health and safety rules. Also, new systems could assist with cost and asset capture in order to avoid liability issues and to fulfil client requirements. Cutting the time workers had to spend on administrative tasks also meant reducing the time they had to spend on sites, which again reduced the

[5] http://www.highways.gov.uk/roads/3008.aspx.

risk of accidents. Some new systems such as a GPS tracking system had been introduced recently, others, such as a vibration monitoring device (Davies et al. 2005) were being tested or were in the planning stages.

All of these factors meant that in our research we were looking at work practices at company X at a point in time where several systems were just coming into being that were either ubiquitous or had features that are typical for ubiquitous computing technologies (such as embeddedness, surveillance and mobility). This was fortuitous in that we were able to look at the interlinking of health and safety and ubiquitous computing and how associated discourses justified and shaped the introduction of the technology and ensuing work practices.

8 Four examples from the fieldwork

In the following examples we will look at what health and safety meant in everyday work situations and how it played out in practice: for the first example we will take a look at the work practices of a two-man maintenance crew on a county council contract. Although this case is not actually about ubiquitous technologies, it nevertheless provided necessary insights into what health and safety meant in the researched context, which thereby enabled us to understand the context for the introduction of ubiquitous technologies.

8.1 Case 1: securing road maintenance sites and finding a place where it is safe to work

Here we will describe the decisions that the crew had to make at one work site. As these observations were made by only the first author of this article the first person singular will be used. The observed work site was on a road with several potholes of various sizes. The crew's work order stated that several of these holes should be fixed by the crew on that day. The crew, consisting of L. and D., had driven on site with their van, which contained equipment to break open and remove the damaged tarmac (e.g. a jackhammer) and new tarmac to fill in the holes. However, L. and D. had difficulties determining which 'patches' to fix on the rather badly damaged road. They told me that they "cannot find them" and apparently the paint markings around damage on the road and footpaths were no help. Also, another crew with a 'Rhino' apparently had received a work order for fixing damage in the same road. A Rhino is a plant that can be used to fix broken tarmac by heating and reapplying it without the need to break the patch open manually. Due to having a Rhino, L. and D. judged the other crew to be more suited to fixing the bigger patches. Both L. and D. had Rhino training (a 1 week course) and knew that most of the patches were suitable for being fixed using a Rhino. As no hand-held vibrating equipment needed to be used, a Rhino would not only be faster but also safer.

There also was the difficulty of traffic management. Some patches were in the middle of the road and L. and D. explained, that they could not "do those" at all, as they would need two more men to divert the traffic. In order to have safe traffic

management, a stop-and-go system on only one lane would need to be put in place and traffic would have to be diverted around the traffic island in the middle of the road. Taking the road layout and traffic management situation and the size of the patches into account, L. and D. decided that they would prefer to only fix those damages that could be worked on safely without a Rhino or proper traffic management. L. and D. called the management at the local depot on their mobile phone to find out which patches they were supposed to fix. They were told to "do the ones that need patching". D. said to me after the phone call: "There is no writing on them saying 'These need to be patched [as opposed to needing to be done with a Rhino]', is there?" It became clear that the management at this point wanted them to 'get on' with the work. However, an inspector was sent out to drive by the site to point out which patches were the ones detailed on the work order.

L. and D. eventually decided not to fix the biggest patch but to start with a medium sized one and to see how far they got that day. They started breaking up the tarmac around a pothole with a jackhammer and taking the old tarmac away. New tarmac was poured into the hole, raked, watered and then compressed. They used hand-held equipment such as a shovel, a wheelbarrow, a rake, a watering can and a Wacker plate (to compress the newly applied tarmac). Next, L. and D. decided, to 'quick-fix' the holes in the middle of the road which they had previously judged to need extensive traffic management. They poured some tarmac into the holes without first drilling up the old tarmac or putting up traffic management such as cones. Their compromise was to have one of them quickly filling the holes while the other one looked out for cars. When cars approached, they briefly interrupted their work and waved to drivers to indicate that they could pass. Having difficulties finding a defect that was safe to work on was a common problem for D. and L. Often defects would be obstructed by parking cars or the specific location would require more complicated traffic management than they could put up as a two-men crew. D. told me that sometimes they spent hours driving around to find damages that were in locations where it was safe to fix them. Often, supervisors and managers would not take this problem seriously and D. complained that "they think we make it up", when they call to say that work cannot be carried out safely. He argued that if they really did not want to work they could just take longer breaks or take their time and that they did not enjoy having to drive around looking for patches.

8.2 Discussion of case 1: workers demanding adherence to health and safety rules

Health and safety is a cultural logic that has become more and more important in the UK, and at company X we could see how it was adopted to fit the requirements of the specific workplaces and their organisation. Although there always had been interest in the company in preventing accidents and looking after people's health, it was only in recent years that health and safety had become such an important factor that it was now considered in every part of the organisation and the workplace. However, health and safety rules could be vague or difficult to adhere to and therefore had to be re-evaluated in each situation. Also, workers were expected to

'get the work done' and this could put them under conflicting pressures. They sometimes felt that they were not able to adhere to health and safety rules, for example because they lacked the proper equipment. Therefore, workers in turn demanded that the management took more notice of the health and safety rules. They would use the health and safety argument to legitimise the way they carried out their work or even to explain why they refrained from carrying out specific work.

Health and safety as a discourse or logic was seen to have paternalistic aspects. Health and safety rules were enforced by the management but supposed to be for the workers' own good. At the same time workers felt that they should not override such rules and that they were cutting down on their freedom, for example, when they were not allowed to work without cumbersome personal protective gear. This meant that there was a paternalistic system already in place at company X, and everyone situated their actions within it. Operatives and management had adopted health and safety as an important logic and something that was part of their everyday work experience. Although they would sometimes complain about what they called 'nanny culture', all arguments took place 'within' the discourse about health and safety.

However, as we could see above, health and safety not only cut down on workers' freedom but it also empowered them to take actions that they otherwise may have had difficulties legitimising. In effect, the heightened awareness of health and safety initially resulted in a striving for more rules and clearer rules about how work should be carried out. But it then caused an increase in the possible actions employees could take and legitimise. For example, a road maintenance crew could decide about whether to fix a patch due to their assessment of traffic conditions as safe or too unsafe for work to be carried out. A 'correct' course of action became harder to define. Although at first glance there were more restrictions there were also more loopholes as things became more complex. It seemed that with more structures being introduced, everything became more complicated and not necessarily clearer as was actually intended. Health and safety was not just 'paternalistic' and controlling but workers actually themed situations with this discourse to their own advantage as well.

As mentioned above, company X was interested in introducing ubiquitous computing technologies in order to increase health and safety in the workplace and also to intensify the control over assets, personnel and work practices in the face of increasingly complex outsourcing and subcontracting situations. With their ability to collect more data than before and in places that previously were not accessible for data collection, ubiquitous computing technologies promised to meet this need for control. They could provide information and proof for liability cases. However, with our observation in mind that health and safety rules increased complexity and provided arguments for different actions being taken by the workers, we assumed that ubiquitous computing technologies may not, in fact, provide the promised control and reduction of complexities either. They may even invite unexpected modes of use and again provide arguments for the legitimisation of contradictory actions. Our next step, therefore, was to look at how individuals in the workplaces interacted with technologies and whether they made use of them in order to advance

their own aims. The following two examples relate to our focus on specific ubiquitous systems[6] at company X.

8.3 Case 2: a GPS system on road inspectors' PDAs

We researched the use of hand-held devices by district inspectors working for company X. We specifically looked at one depot with about ten district inspectors who covered the whole of the area network. Inspectors were given a different route every month which they then inspected for various defects that fell under the obligation of company X's road maintenance contract with the local county council. Usually the inspectors would arrive at the depot in the morning to pick up their vans and then spend all day inspecting roads. They returned to the depot in the evening to download the collected data to the backend system. The inspectors used hand-held devices (PDAs) with a special software programme that listed roads and defect types and generally supported the collection of data about defects.

The inspectors decided by themselves in which order to inspect the roads on their route and they had individual ways of organising their work. For example, many inspectors drew their own maps of their routes and based decisions—e.g. about which parts to inspect first—on factors such as weather conditions or changing amounts of traffic. Generally their way of working was rather individual and they were free to arrange their own schedules.

One typical task for the inspectors was to determine ownership of roads to find out whether damages found were actually within the responsibility of the contract or whether the damaged road was privately owned. The question of ownership was further complicated by the fact that there were different budgets depending on the type of road or other public property. For example, some private roads which were not actually repairable under public expense had a special fund due to having a lot of public use. When I followed one inspector, K., on a typical workday, he had several boxes of maps and statutory plans in the back of his van which he used to determine ownership of roads and other surfaces. Generally, inspectors not only needed a lot of local knowledge in order to decide about the most effective order in which to inspect roads but they also depended on specific knowledge about ownership and budgets that could be rather complex. Often decisions needed to be based on previous experiences. K. had developed different ways of using the PDA in his work which depended on the specific nature and requirements of the job he needed to do. For example, for the first job on that day he did not take the PDA with him but used pen and paper and also took some paper stat plans to determine ownership of the parts of road with the defects. As he did not have to move away from the car more than a couple of metres, he left the PDA in the car so it could be recharged by the cigarette lighter. Back in the van K. put the data into the PDA, using a time-saving system where he re-used the input for one defect and just altered

[6] As mentioned in the introduction, the definition of ubiquitous computing is not always clear. We defined the PDA system used by the inspectors and the GPS built into gritting vehicles as ubiquitous since they were mobile, integrated into the environment (as in-car systems), and provided data about previously inaccessible places.

differing details for another one. The second road K. inspected on that day was a longer one and as this was not just a follow-up inspection, K. took the PDA with him. Walking down the road, K. was observed to input defects on the PDA whenever he found them. Even though it was cloudy it was very hard to see anything on the PDA display which was already switched to the brightest setting. Back in the car he finished the data input by ticking off the different aspects that needed to be inspected and he also added condition ratings. For example, the carriageway was in a below average condition and the road markings in a good condition. A third way of inspecting a road was called a 'driven inspection'. K. told me that he would use this method when stopping the car was too awkward or dangerous (e.g. on a three-lane roundabout). If this was the case, he would spot the defect, memorise as many details as possible and write them down as soon as he found a place to park the car safely.

In order to improve the data collection process for defects, the management was planning to introduce a so-called 'GPS button'. At the time of my visit K. was first told about this new system that was going to be installed on the inspectors' PDAs. Instead of manually typing the description of a defect location the inspectors would simply press a button while standing next to the defect (e.g. a pothole) and a longitude and latitude reading would automatically be recorded. K. immediately said that he did not like the idea of the new system at all. There were several aspects to his critique. First, driven inspections would not be possible anymore. K. argued that having to click a button at the exact location of a defect would be awkward in certain situations and may even be contradictory to company X's quest for more safety. Second, information on the PDA display was often hard to see. So in bad weather conditions he did not like taking the PDA outside but would finish the inspection as quickly as possible and input the data later in a café where the light would be better. A third reason for his critique was that the button was in his opinion an unnecessary feature that he did not need because he already had a lot of experience and local knowledge. The feature would not give him any additional information. K. said:

"I do not see why I should need a GPS map to show me where I am".

There were two other aspects to K. and the other inspectors' critique of the planned GPS button that also had to do with them feeling that their work was not valued enough and that their competences and knowledge were being questioned. First, inspectors were complaining about the size and facilities in the shared office and the fact that there were not enough desks and PCs. Only since they had been transferred to the current depot in a recent centralisation had it been necessary for all inspectors to share one small office with a single PC and PDA cradle. This set of affairs contributed to what seemed to be the most important reason why K. did not like the proposed GPS system: for him it was just another example of the management trying to control his work. He and the other inspectors had, after many years of experience, developed best practices and individual ways of 'getting the work done' as efficiently as possible. In his opinion the management were trying to control this by introducing potentially sub-optimal rules, regulations, practices and technologies which the inspectors were expected to adhere to.

The management, however, wanted the system to be introduced. They believed, for example, that it would make it easier for patching crews to find defects—and the less time that crews spent on the road then the safer the workplaces were. Patching crews, which were sent out to fix defects, often had difficulties finding the exact location of potholes. I was able to verify this myself when going out with crews: Often a road would have several holes and defects and the crew would have to make an educated guess as to which pothole was the one to be fixed. Owing to the council's annual budget already being exceeded, only holes of a certain depth would get fixed, which meant that crews had to choose the correct ones. At such sites, however, it was often difficult for inspectors to make accurate descriptions of defect locations. Another reason that the management were keen on the introduction of the system concerned the driven inspections, and was explained to me by Q., who managed the district inspectors' work and was K.'s superior. When using the new GPS system inspectors were expected to stand directly at the location of the defect in order to 'click the button' and get the exact location reading. Q. explained that in cases where they would previously have done driven inspections, inspectors could be "standing on the kerb as well", if it was not safe to be directly at a defect location. However, inspectors would not be able to put in the location later on (e.g. in the van or in a café), as company X "…want to get away from this". One additional factor that further complicated the discussion concerned the accuracy of the planned GPS system. The system could only fix a point on the ground within ten metres. Therefore, on the one hand inspectors could indeed sensibly stand away from a defect in certain unsafe situations, but on the other hand the problem of reliably identifying a defect would not typically be solved for the patching crews.

8.4 Discussion of case 2: the management aiming to control work practices?

There was a distinct conflict between the management and the district inspectors about the GPS system that mainly concerned issues of independence and control. K. interpreted the planned GPS system as an attempt by the management to take away control from himself and the inspectors who had developed highly efficient practices that "got the work done". The inspectors saw the new system as one in a line of events (such as the move to a smaller office) that had led to a steadily worsening work environment. In their view the management were trying to put a stop to individual preferences that often relied on very specific local knowledge such as the length or busyness of a road. The management, on the other hand, were indeed aiming to improve procedures and health and safety by ensuring a high level of control. Management had to take into account the bigger picture that pertained to all of the various actors within the organisation such that it was trying to improve a complex situation involving not only the inspectors but also patching crews and other operatives.

Both the management and the inspectors were using health and safety to support their argumentation. K. argued that the GPS would make his work less safe as it would make driven inspections impossible. The management on the other hand were—for safety reasons—aiming towards reducing the time workers had to spend

on the road by introducing clearer descriptions of defect locations. Thus, health and safety arguments were being used to achieve different aims (even contradictory ones). In this way, logics such as those reflected in health and safety discourse could be utilised by everyone to further their own goals: The management used health and safety arguments to impose structure on the workplaces, and the inspectors used health and safety arguments to legitimise the way they carried out their work.

The management were trying to control work practices and to improve efficiency and accuracy. They aimed to achieve this with a technology that would not allow users to deviate from prescribed work procedures. However, this was only one element in a continuous effort to improve health and safety, streamline practices and improve efficiency. This impetus was the background in front of which a technology such as the GPS button became meaningful; the conflict of control and independence did not arise with the new button technology, but was already part of the interaction between inspectors and management.

Whether the technology would work as intended by the management or as feared by the inspectors was unclear at this point in the research. However, there were many factors making it very unlikely that the system would improve control to the degree intended by the management: First, there was the lack of accuracy of the GPS location system. Also, there was the resistance from inspectors who were trying to keep to their individual work practices. Their arguments were fuelled by technical disadvantages of the PDAs such as the bad display. Also, the existing PDA system had, in fact, created a variety of possibilities as to how input could happen, making inspectors develop different styles, workarounds and techniques when dealing with the technology. Therefore it would be very likely that the new system would not be a controlling and accurate system as envisioned by the management. Rather, the new button system would be more likely to support a way of working that was very similar to the current one, instead of controlling inspectors and forcing them to adhere to a completely different way of working.

8.5 Case 3: a GPS tracking system in gritting vehicles

The second system we looked at was a GPS tracking system for gritting vehicles, which Company X recently had introduced in one area. The aim of this system was to be able to track stolen vehicles and to prove to customers what work had been carried out as well as when it had been undertaken. I talked to U., who had been managing the deployment and installation of the new GPS system. There had been two ways in which the new GPS system had been used differently from the way it had been intended, since opportunities of use had emerged after the installation, resulting in modes of use that could be both disadvantageous and advantageous to drivers.

Initially, the drivers of the gritting vehicles were told that the system had been installed in order to win bids for contracts. When a trial version of the system was first installed, U. was approached by some of the drivers who inquired about the type of information that the system would record. They wanted to know who would have access to the collected data and what it would be used for. U. had explained to

them that the system was part of the efforts to win bids for contracts and was in place as a service for the client. The client would then be able to see what work had been carried out whereas company X was making an effort to become more transparent. U. placated the drivers as follows:

> "I said there's no one sat there all day looking at this tracking data, it's only when there's an issue that people look at it".

Some of the drivers were concerned that the system would not work correctly because they had witnessed faults occurring during the trial phase. During the initial tests the system had not been very reliable, frequently locating vehicles in wrong places. However, as they perceived their manager as a very reasonable and supportive person, they did not generally view the system as a problem. For example, drivers would call their manager and tell him when they needed to go somewhere unexpectedly or not work related and the manager would support their decision. This laissez-faire attitude changed, however, when the system caught some drivers 'speeding'. Company X's management used the data gathered by the GPS as proof to discipline the drivers. Since drivers had witnessed the system working very inaccurately during the test phase, they questioned that the data was accurate and U. was asked to verify the accuracy of the data. However, when the data and an explanation about how the system calculated speed were presented to the drivers in question, they conceded. U. put it this way:

> "The data was presented to them and they were happy then".

In another case the system was used again in a way not intended or foreseen when the system had first been installed. This time, however, it worked in favour of a driver, who had been involved in an accident. The system confirmed that the driver had never been driving over the speed limit. This had an impact on how gritter drivers viewed the system as a whole, with many of them perceiving the system far more positively after this event.

8.6 Discussion of case 3: for whose benefit is the system?

The new GPS technology was introduced into gritting vehicles because there was a need to prove what work company X had carried out as well as the time and location of gritting activities. The system then had an impact on typical situations at company X, such as disciplining employees or having to deal with being sued by third parties. This was because the system provided data capture in relation to previously inaccessible domains. Such data could then be used in ways that may not have been completely surprising but that nevertheless had not been the main focus when the technology was first considered. The technologies were used in unexpected ways and the possibilities to do so only emerged with their implementation. These unexpected modes of use could work both for and against employees and management. Both the surveillance aspect and the proof-of-innocence aspect appeared equally strong, and benefits and losses that arose with the new system were not easy to measure. However, the system was introduced by the

management who ultimately could decide which technologies and procedures were being used. Employees could subvert these efforts by refusing to do work that was unsafe or they could profit from a system that was able to prove their innocence. But considering the fact that the decisions about which technologies were being used rested with the management, we wanted to explore the managements' (paternalistic) argument that the GPS systems were 'also for the employees' own good' in another setting.

8.7 Case 4: a control room for monitoring with CCTV and GPS systems

For this I visited a control room in which the high-speed roads of a whole area were monitored. Company X's contract for this area was with the Highways Agency and therefore concerned only high-speed roads. I talked to B., who showed me the system and explained how everything worked. A huge wall-mounted screen showed a live feed from one of many stationary motorway CCTV cameras. These cameras were mainly used to monitor congestion. There were also several smaller screens for other cameras, including those for the depot security cameras which were located in one corner. B. showed me how specific cameras could be moved and how control centre personnel were able to zoom in on areas of interest. The control room received calls from RCCs (regional control centres) and the police, and if there was an incident they would send out ISUs (instant support units). There were eight ISUs stationed throughout the network that normally responded to an accident within 22 min. They were the first ones to report to any incident that happened and were responsible for securing the site, requesting further assistance and generally making the first assessment of any incident. Each ISU had their 'patch' on which they normally had to stay, although they sometimes would leave their patch, for example to pick up equipment. B.'s computer screen showed a map and the positions of all ISU vehicles in the area. All ISU units were monitored by a GPS location system that reported their location to the control room and provided the area map with the ISUs symbolised by little pictures of vans moving around it. There was also a log so that vehicles' movements could be 'replayed' on the map. In case of an incident the control room could determine which vehicles were closest and then send those to a specific location. However, the first action would often be to call the ISU responsible for the specific area on their mobile phone. In fact, most of the communication was done by mobile phone and the GPS and cameras mostly served as a backup system. A GPS system for gritting vehicles was still being tested but would eventually provide the same information about these vehicles, whose settings, locations and speed would all be logged. As there were some roads where no stationary CCTV cameras were installed, one ISU had been fitted with a mobile camera. At the point of my visit this system was still in its trial phase and had only been fitted to one vehicle.

B. was very enthusiastic about the benefit of the data gathered by the cameras and GPS for her work, which included controlling all vehicles and work going on in the area. She said: "You can actually see what is going on" and stated that this was "such a benefit". In order to carry out their work better, the control centre

employees wanted as much data as possible and were very keen on accessing areas that had previously been inaccessible for data capture, such as motorways without cameras. For example, B. suggested that a GPS system for other vehicles could also be very beneficial, especially one in the general foremen vehicles, who often could get to an incident quicker than an ISU that was stuck in traffic. I asked B. whether the systems sometimes showed that people were not where they were supposed to be and she confirmed this and said that the system would do this, especially when people were on "off record" time. As in the previous example, the system would also record whether ISUs or gritting vehicles were moving at a speed above the set limit. When the system had been introduced there had apparently been some resistance from the drivers of the ISU vehicles but B. explained that now there was a consensus that "it protects the guys as well". This was deemed to be especially the case when there were incidents such as residents making insurance claims, for example, about damage such as windscreens having been smashed by gritting vehicles or roads not having been gritted. Using the system company X could prove where vehicles had been at all points in time. However, it later turned out that—contrary to B.'s claim that drivers viewed the system as beneficial—this was not actually the case. When I talked to the ISU crew on whose vehicle the camera was fitted they told me that they in fact did not like the system. Although the control room claimed that the new system was intended for traffic control they were convinced that it was actually intended to watch and control them at work.

8.8 Discussion of case 4: 'It is also for their own good!'

As in the previous example it at first seemed as if the new monitoring systems brought both advantages and disadvantages to all involved. Drivers would be able to prove their innocence and the control room would be able to expedite processes. On the other hand, drivers could be disciplined because the system picked up instances of speeding. In addition, the control room might have to deal with yet more unreliable and complicated technology and not be able to access the desired data. Furthermore, the claim that the systems were beneficial for the drivers seemed rather hollow for several reasons: First, company X—and not the drivers—were liable for any damage that was caused (e.g. by gritting vehicles), although disciplinary actions could be taken against drivers internally. Second, the decision to introduce the system had been made by the management and not by the drivers lobbying for protection. Third, the drivers themselves did not appear to like the system. This resistance was underestimated by the management as the system was deemed to be clearly "for their own good as well".

9 General discussion

Company X had a very understandable and laudable interest in improving health and safety for their employees. But this interest also served to reproduce—and even enhance—existing power structures, allowing managers and administrators to

extend their control over employees' work practices by introducing technologies into environments (e.g. roads or vehicles) that previously had not been accessible for data capture. The paternalistic stance as it was employed by the management could thus serve to legitimise introducing ubiquitous technologies. The technologies then functioned within the pre-existing paternalistic system and enhanced and extended it. But what is it, then, that is *different* about ubiquitous computing and the new 'technology paternalism' that comes along with it? At this point in time this seems to be a hard issue to judge—but maybe this is symptomatic of this kind of technology itself, which is both complex and continuously changing and part of an ill-defined field that is characterised by a wide variety of different applications.

Despite these conceptual difficulties, however, we believe that we can still draw some valuable conclusions from our observations of ubiquitous computing systems in the specific field of road maintenance and construction. First, we would argue that the deployed systems appear to be far less controlling than they were intended to be. The systems are relatively complex and error-prone and employees can, if they want to, find ways to work around them or even boycott them entirely. For example, health and safety arguments, which provide the very rationale and context for the introduction of these technologies, are seen to be used by everyone to further their own aims (e.g. workers frequently made recourse to health and safety discourse to legitimise their own actions and decisions, even when these were contrary to company policies). Second, it is very likely that although paternalism may be a problem (ethically, philosophically and practically), it still does not necessarily get a 'new' quality through its association with ubiquitous computing; rather ubiquitous computing is being introduced because of paternalism and then strengthens the existing system—with all its flaws and power struggles that continuously permeate, reshape and reconstruct people's workplaces and their roles, responsibilities and positions within the organisation. It is not merely a case of the management 'gaining power' since, in fact, management personnel themselves may be forced to adhere to more and more regulations (e.g. in the case of having to demonstrate improved health and safety practices in order to win bids for contracts).

Ubiquitous technologies play an important part in this complex situation of shared responsibilities and liabilities and they can neither be understood without it nor are they tools that merely serve to 'subject'. If there was no health and safety discourse first, the technologies would not be meaningful or interesting. Rather than the technologies bringing about a new kind of paternalism, it is because of paternalism being firmly embedded within the organisation, that the technologies are being introduced. We could easily imagine a completely different argument (and not health and safety) shaping the use of ubiquitous technologies—and also the meaning of health and safety for our society changes all the time. But at the moment no other topic seems to be powerful enough to shape technologies and their use. This is why everyone at company X aimed to theme situations with the logic of health and safety in a way that was beneficial to them.

By focussing on ubiquitous technologies and their impact there is a danger of overlooking the issue that a lot of developments associated with these technologies do not actually originate merely in the technologies themselves. Rather, the technologies fit into an environment that is concerned with an increased need for

liabilities, regulations and temporary contracts (bidding and subcontracting of specific work), and we cannot assume that things would be different without such technologies. It is necessary to see ubiquitous computing as a means in a general thrust towards increased liabilities, the need for cost-capturing and more health and safety measures. In fact, technologies and the social and cultural conditions out of which they emerge—and which they in turn influence—may best be seen as co-constitutive (Wajcman and MacKenzie 1998).

Introna (2007) has researched this co-constitutive relation in connection with surveillance technologies. According to his research, technologies such as CCTV cameras only become meaningful because there is a co-constitutive relation between all the actors that are involved (in this case the camera, its operator, the people being watched etc.). This means that the origin of agency is unclear and can only be located by revealing the circumstances under which behaviour is 'scripted' by the technologies, which in turn are only meaningful because we make them so (Introna 2007). In our case the necessary constitutive condition for the technologies is the paternalistic impetus that permeates the organisation of the workplaces into which the ubiquitous technologies are being introduced. If agency is something distributed and we are always already involved in situations, then paternalism is already in place and constitutes the technologies and their functions, as well as the reasons for their introduction and the means by which they are introduced. These technologies then have a specific impact on the people who are confronted with them, but this impact cannot be divorced from the paternalistic system, which they are part of. Rather than focussing on 'technology paternalism' we may need to realign our focus to examine 'paternalism and technologies'.

But what is it, then, that is different about ubiquitous computing in comparison to more traditional types of computing? The answer to this cannot be found without looking at the larger picture. We need to examine cultural logics such as the rise of health and safety discourse in the UK and its legal, economical and social impact in order to understand how specific technologies such as a GPS location system could be constituted and become meaningful. In this context the paternalism that the technologies assert and support may well be of a different quality, but then the whole system is of a new quality—and also is constituted by ubiquitous technologies. We found that people used technologies for their own ends when they were confronted with them. They were always already involved in the situations that made possible the emergence of new technologies such as surveillance systems. Due to this, the relations of power and control are very complex. In fact, technologies may contribute towards empowering people—who at first glance seem to be 'controlled' by a new technology—to stand up for their own interests (Kortuem et al. 2007). By theming situations with cultural logics such as health and safety when it promises to be advantageous, people confronted with ubiquitous technologies can further their own interests, and this process continues with cultural logics changing and emerging. Ubiquitous technologies emerge and change with them and cannot be understood without researching the cultural logics that make their emergence possible.

To conclude, we agree with Spiekermann and Pallas (2006) that a wide discussion about ubiquitous computing is necessary, but we suggest that instead of

merely focussing this discussion on the technologies themselves, we need also to address the specific conditions under which ubiquitous technologies emerge. In particular, we claim that the health and safety discourse that surrounds current work practices must itself take centre stage within ongoing debates surrounding the nature and role of ubiquitous technologies within contemporary life and work.

Acknowledgements This work has been supported by the UK Engineering and Physical Sciences Research Council (EPSRC) project NEMO (EP/C014677/1). We would like to thank Mike Chiasson (Lancaster University) for his very helpful comments and suggestions.

References

Adamowsky N (2000) Kulturelle Relevanz. Ladenburger Diskurs "Ubiquitous Computing", February 2000

Araya A (1995) Questioning ubiquitous computing. Proceedings of the 1995 ACM 23rd annual conference on computer science, pp 230–237

Bohn J, Coroamă V, Langheinrich M, Mattern F, Rohs M (2004) Living in a world of smart everyday objects—social, economic, and ethical implications. Hum Ecol Risk Assess 10(5):763–785

Brey P (2005) Freedom and privacy in ambient intelligence. Ethics Inform Technol 7:157–166

Bryman A (2004) The Disneyization of society. Sage Publications, London

Burrell J, Brooke T, Beckwith R (2004) Vineyard computing: sensor networks in agricultural production. IEEE Pervasive Comput 3(1):38–45

Davies N, Efstratiou C, Finney J, Hooper R, Kortuem G, Lowton M, Strohbach M (2005) Health and safety compliance in the field. Poster and Demo Abstracts, ACM MobiSys 2006, Uppsala, 19–22 June 2006

Deleuze G (1992) Postscript on the societies of control. October 59:3–7

Dourish P (2001) Where the action is: the foundations of embodied interaction. MIT Press, Cambridge

Downey GL (1998) The machine in me. an anthropologist sits among computer engineers. Routledge, London

Drugge M, Hallber J, Parnes P, Synnes K (2006) Wearable systems in nursing home care: prototyping experience. IEEE Pervasive Comput 3(3):8

Escobar A (1994) Welcome to Cyberia: notes on the anthropology of cyberculture. Current Anthropol 35(3):211–223

Fleisch E, Mattern F (2005) Das Internet der Dinge: Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen. Springer, Berlin

Galloway A (2004) Intimations of everyday life: ubiquitous computing and the city. Cult Stud 18(2/3):383–407

Greenfield A (2006) Everyware: the dawning age of ubiquitous computing. New Riders, Berkeley

Hannerz U (1992) Cultural complexity: studies in the social organization of meaning. Columbia University Press, New York

Hansen TR, Bardram JE, Soegard M (2006) Moving out of the lab: deploying pervasive technologies in a hospital. IEEE Pervasive Comput 5(3):24–31

Ilyes P (2003) "Technology is driving the future". Informationstechnologie und gesellschaftliche Veränderung aus der Perspektive lokaler IT-Experten. FB Sprach- und Kulturwissenschaften. Dissertation, JWG University, Frankfurt

Introna L D (2007) What surveillance does: exploring the ethics and politics of algorithmic surveillance systems. The new surveillance—a critical analysis of research and methods in surveillance studies. International Conference at the Centre for Technology and Society of the Technical University Berlin

Kortuem G, Alford D, Ball L, Busby J, Davies N, Efstratiou C, Finney J, Iszatt White M, Kinder K (2007) Sensor networks or smart artifacts? An exploration of organizational issues of an industrial health and safety monitoring system. In: Krumm J et al (eds) UbiComp 2007: Ubiquitous Computing. 9th International Conference, Innsbruck, Austria, September 2007, Proceedings, LNCS 4717, Springer, Berlin, pp 465–482

Kun A, Miller TW, Lenharth W (2004) Computers in police cruisers. IEEE Pervasive Comput 3(4):34–41
Ong A (1999) Flexible citizenship: the cultural logics of transnationality. Duke University Press, Durham
Rabinow P (1999) French DNA: trouble in purgatory. The University of Chicago Press, Chicago
Ritzer G (2004) The McDonaldization of society. Revised New Century Edition. Sage Publications, London
Roduner C, Langheinrich M, Floerkemeier C, Schwarzentrub B (2007) Operating appliances with mobile phones—strengths and limits of a universal interaction device. In: LaMarca A, Langheinrich M, Truong KN (eds) Pervasive Computing. 5th International Conference, PERVASIVE 2007, Toronto, Canada, May 2007, Proceedings. Berlin, pp 198–215
Rohs M (2002) Ubiquitous computing criticism. Seminar Ubiquitous Computing Information. Presentation at the Department of Computer Science, ETH Zurich, 6.2.2002, http://www.vs.inf.ethz.ch/edu/WS0102/UI/slides/ui_10critique.pdf
Roussos G, Moussouri T (2004) Consumer perceptions of privacy, security and trust in ubiquitous commerce. Pers Ubiquit Comput 8:416–429
Spiekermann S, Pallas F (2006) Technology paternalism—wider implications of ubiquitous computing. Poiesis & Praxis: Int J Technol Assess Ethics Sci 4(1):6–18
Stajano F (2002) Security for whom? The shifting security assumptions of pervasive computing. In: Okada M et al (eds) Software security—theories and systems. Mext-NSF-JSPS International Symposium, ISSS 2002, Tokyo, Japan, November 2002, Revised Papers. LNCS 2609, Springer, Berlin, pp 16–27
Stanford V (2002) Using pervasive computing to deliver elder care. IEEE Pervasive Comput 1(1):10–13
Stranks J (2005) Health and safety law. Prentice Hall, London
Wajcman J, MacKenzie D (eds) (1998) The social shaping of technology, 2nd edn. Open University Press, Buckingham
Want R, Pering T, Borriello G, Farkas K (2002) Disappearing hardware. IEEE Pervasive Comput 1(1):36–47
Weiser M (1991) The computer fort the 21st century. Sci Am 265(3):94–100
Weiser M (1993) Some computer science issues in ubiquitous computing. Commun ACM 36(7):75–84