Journal of Ambient Intelligence and Smart Environments 2 (2010) 67–80
DOI 10.3233/AIS-2010-0049
IOS Press

Ubiquitous monitoring and user behaviour: A preliminary model

Stuart Moran[*] and Keiichi Nakata
Informatics Research Centre, University of Reading, Reading, UK

Abstract. Recent advances in ubiquitous computing are turning our environments into smart spaces, where technology is embedded into the physical environment. Significant levels of data must be constantly and ubiquitously collected to provide much of the new functionality; a process we refer to as ubiquitous monitoring. Existing research has shown that monitoring can often cause undesirable effects, such as increases in stress, and with the increased coverage of ubiquitous monitoring, we anticipate an increase in the impact of such effects. So far, a limited amount of research has investigated the impact of this new technology on users. As such, we propose a preliminary model consisting of a series of factors believed to influence user/occupant behaviour and augmented by the Theory of Planned Behaviour for explaining and potentially predicting any undesirable effects. As the model has the characteristic of system dynamics, a preliminary (proof of concept) simulation was carried out to examine the influence of each factor on one another, both directly and indirectly.

Keywords: Behaviour, modelling, monitoring, simulation, ubiquitous

1. Introduction

Observation can perhaps be considered one of the simplest and earliest forms of monitoring. Through time, advancements in electronics and computing have seen improvements to monitoring technologies, resulting in a change in their purpose, and an increase in their adoption and application. Technologies such as Electronic Performance Monitoring (EPM) and Closed-Circuit Television (CCTV) have replaced manual monitoring techniques. With increases in accuracy and autonomy it is clear why electronic monitoring has been so widely and readily adopted. While monitoring is successful in many forms, in some scenarios it has often been known to cause undesirable effects, such as increases in stress and distrust in those being observed [67]. Even patients in hospital, in what can be considered one of the most beneficial situations for being monitored, have felt increased stress caused by the lack of privacy brought about by continuous observation and intrusion of personal space [57].

Technology is constantly advancing and evolving, with two eras of computing already passed: mainframe and personal computing. With further advancements in network, mobile, wireless and sensor technologies, we are soon approaching what can be referred to as the ‘pervasive era’ of computing. Mark Weiser, who is generally considered the founder of ubiquitous/pervasive computing, explains that “*the most profound technologies are those that disappear*” [68]. The principle of ubiquitous computing is to embed computers into physical objects and the environment itself, while still providing the originally intended and more advanced new services, such as context awareness. This removes the computer from the main focus of our lives, creating a sense of ‘calmness’ in the environment. By automating and simplifying daily and other complex tasks, the impact of this type of computing will be vast.

In order to fully achieve much of the potential functionality of ubiquitous computing, there is a fundamental reliance on the constant and ubiquitous collection of significant levels of data [5,16,40] by large numbers of sensors and other monitoring devices [15]. It is this ubiquitous collection of data that we refer to as ubiquitous monitoring (UM). UM differs from existing monitoring technology mainly due

[*] Corresponding author. E-mail: stuart.moran@reading.ac.uk.

to the absence or weakening of physical restrictions, such as walls and other attributes of the environment, increasing its capabilities [16,41].

UM at its core is still a monitoring technology, and it is anticipated that many of the same effects caused by existing monitoring methods will be enhanced due to the increased coverage [5,20,35]. Other factors which may contribute toward an increase in the impact of these effects include increases in the number of people being monitored and the social contexts in which the monitoring takes place [11].

To date, concerns have been raised that the use of UM and its effect on human behaviour have not been thoroughly investigated [10,32,71]. This implies that current and future intelligent pervasive space (IPS) system designs may cause (preventable) undesirable effects, leaving the systems unable to provide their intended services. This gap in the literature may be attributed to the rapid development of these technologies, with their numerous advantages overshadowing their possible negative implications. Thus far, speculation about the effects of this technology has been the only option for researchers [18], and given its potential serious implications [39], it is necessary to attempt to anticipate, understand and predict the effects [6,58]. Only then can action be taken to prevent any undesirable effects.

As a first step toward understanding and predicting the effects of UM, we have identified a series of factors believed to influence behaviour and how they relate to one another. The Theory of Planned Behaviour [4] was used to theoretically link these factors to behaviour, and these relationships are described using a model. In its current form, the model can be used to explain behaviours caused by UM. When empirical data is collected, the model could be used to predict and prevent the undesirable effects of UM.

This paper is structured in the following manner; Section 2 presents some background work. Section 3 describes the seven factors believed to influence behaviour. Section 4 provides details on the preliminary model and simulations. Section 5 is a brief discussion of the potential application of the model and future work. Section 6 concludes the paper.

2. Background

2.1. Intelligent Pervasive Spaces

Intelligent Pervasive Spaces (IPSs), and their manifestations such as Intelligent Buildings (IB), are environments designed to make life more efficient and comfortable for people, and will be some of the first adopters of pervasive technologies. We define an IPS *an adaptable and dynamic environment that optimises user services and management processes using intelligent systems and ubiquitous technologies*. IPSs are often controlled by software known as intelligent agents which monitor the users and alter the environment according to contextual data and user stated preferences on controllable variables. A vast number of sensors and monitoring devices are used to collect the large levels of data required [5,15] for automating (and enhancing) daily and specialist tasks in an IPS. This forces them into the background, and therefore contributes toward Weiser's vision of invisibility. While existing monitoring technologies and techniques can be used to accomplish this to a certain degree, in order to achieve true pervasiveness and invisibility, the monitoring devices themselves must act, in some sense, ubiquitously.

Almost any type of information could be considered useful in an IPS, particularly when considering the scale at which such systems could potentially operate [40]. Data on a user's location, and the physical and social contexts within which they reside, will be essential in providing certain services. Systems such as CitySense [47], offer users the ability to view the location data of others with similar interests or needs. The coverage potentially spans across entire cities, allowing users to see where the majority of people with shared interests congregate, indicating a popular area a user is likely to enjoy.

There are doubts as to how positive the outcome of such high levels of monitoring can be in IPSs [72], with concern already being shown that collecting user location data may cause user discomfort [44]. User anxiety about the surveillance potential of UM is only natural, but by sacrificing some level of data, there are great possibilities for personal gain [49].

Our questions regarding the effects of UM were initially formed through examination of some of the basic working principles of IPSs and IBs. Users of an IB may be required to state their preferences on variables such as lighting and temperature in order to intelligently provide heating, ventilating and conditioning services. It is questionable whether a user can know an accurate value for their preference on these. One solution to this is to monitor user behaviours over long periods of time, learning their preferences and then automatically controlling and altering the environment based on the data collected [5]. There are two key ways in which to achieve this: provide a means of interacting with the system where the user states their preference in a simplified form, or create a more passive environment where the user's behaviour is learnt through recognition algorithms with minimal user interaction. An issue that undermines both of these methods is the user's awareness of being monitored. The system is likely to increase a user's awareness of both the temperature and the monitoring itself: consider a ticking clock, after becoming aware of the sound, it is often perceived to become louder, and as such no longer reflects a person's natural perception of it. The same effect may occur when collecting a user's preference on the temperature and other variables i.e., users genuine preferences on these variables may not be collected, preventing the system from working correctly. If the devices used for monitoring are not passive, they will themselves act as a sign of data being collected, further increasing the user's awareness of the monitoring. It is the impact of awareness in IPSs which directed the initial motivation for this research, and eventually lead to the questions regarding the impact of UM on occupant behaviour.

When users are presented with a new technological experience, they often refer back to their past experiences with similar technologies [27]. Understanding how people react to existing monitoring technologies is therefore a valuable means of drawing parallels to UM, providing an insight into the possible desirable and undesirable effects on users [20,27,34].

2.2. Monitoring

Monitoring and surveillance are terms that are often used interchangeably, but a distinction can be made between them. Surveillance can be considered a form of monitoring, whereby an observer's intention is to prevent certain user behaviours through risk of punishment [53]. Monitoring, on the other hand, is a generic term that describes the collection of information for any purpose [13]. Hence, arguably it is the intention of the monitoring which defines whether or not it can be considered surveillance.

Research investigating the effect of monitoring on human behaviour has been conducted in many areas including the workplace [2,26], and schools [21]. The conclusion from much of this research is that monitoring often causes an undesirable change in behaviour [42,52], which in turn can often be found to outweigh the benefits of such systems, creating an overall negative impact [13].

Awareness of being monitored changes behaviour, and a well known classic, albeit often contested, example of this is the Hawthorne effect [51]. Employees in the Hawthorne works were monitored as part of an experiment to establish a relationship between their productivity and lighting levels. The employees' productivity was unexpectedly found to increase regardless of the light intensity; this was attributed to the fact that they were aware that they were being observed. Awareness of monitoring has even been shown to change a person's writing style and internet browsing habits [21].

2.3. Ubiquitous monitoring

UM is the use of pervasive devices for collecting data in an IPS or other ubiquitous environments. These devices are generally unrestricted by physical boundaries, and so their capabilities are significantly greater than existing monitoring technologies [8]. There are five main characteristics which differentiate UM from other forms of monitoring [6]: *Collection Scale, Collection Manner, New Types of Data*, *Collection Motivation* and *Data Accessibility.*

Among existing work related to IPS and UM, Tiburcio and Finch [64] have looked at the positive impact an intelligent classroom has on pupil behaviour, and Clements-Croome et al. [17] conducted a study which found that occupants like their environments to be both controllable and adaptable. Live-in laboratories such as the Aware Home [33], the Place Lab [29] and iDorm [14] have been constructed in an attempt to create a naturalistic environment [31] in which to study the behaviour of individuals in intelligent homes, a form of IPS. In these homes, occupants' activities, location and even health are constantly monitored. Some of the data collected through laboratory studies have shown that ubiquitous technology does cause a change in human behaviour [7,62]. Even though such studies provide useful results, there are limitations, and generalising the results from these artificial environments is unlikely to provide adequate evidence for studying behaviour [35]. The environment also places constraints on behaviour variability [29,35], is unlikely to generate many of the behaviours that would be exhibited in real life scenarios [35] and generally focuses on the impact on behaviour in only domestic contexts [31]. Portable UM systems [62] are also being developed as a research method for observing natural behaviour in natural settings, such as the home [30].

3. Behaviour influencing factors

After examining the monitoring, surveillance and ubiquitous/pervasive computing literature, a series of seven recurring factors related to UM were identified, that are believed to influence human behaviour: *Intrusion, Awareness, Boundaries, Control, Trust, Justification* and *Context*. In order to understand the true consequences of ubiquitous computing, the effects must be studied at multiple levels [70].

Each behavioural factor influences behaviour at two different levels: physical and social. The physical level focuses on the physical attributes, functions and effects of a device (as an object). Elements of a monitoring system within this level are directly controllable by the designer, and as such form the core areas with which design changes are made. The social level focuses on social norms, and the interpretation, use, control and dissemination of the data collected. Unlike the physical level, not all of the social elements are directly controllable, but can be influenced by design choices made at the physical level.

Another aspect which may initially be only considered in the social level is user cognition, or perception. This perception also has an effect at the physical level, in terms of a user's understanding of what a device is capable of and whether or not it is intrusive to them. In this respect, perceptions actually act as a boundary between the two levels; where a user's perception of a factor at the physical level, may influence their perception of a factor at the social level, and vice versa. A designer is then able to influence a user's perception by informed changes to those factors over which they have control. This link between the factors and user perceptions is an area that will be further considered in the future.

In the following sections, each of the seven factors are discussed, where, unless explicitly stated, 'users' in this context are occupants. Many of these factors are accompanied by a series of propositions, which detail hypotheses regarding influential links between the factors. The propositions were inferred from the literature, and in some cases, from our own understanding of the workings of such systems. Some factors have evidence, found in the literature, supporting existing influential relations between them, in which case, there are no accompanying propositions.

3.1. Intrusion

UM systems make use of a range of technologies, each with varying levels of intrusiveness, perceptions of which can be examined from three viewpoints: as a physical obtrusion, a privacy invasion and a security risk [46]. These perceptions are influenced by the familiarity and pervasiveness of the device, and the level of user control over and regularity of the monitoring [24,60]. From a physical perspective, when using wearable sensors, there is a risk of intruding a user's personal space [56] and causing discomfort [44]. It is also possible that a user would experience a heightened awareness of the device and the monitoring taking place, potentially altering their behaviour.

Proposition 1. *Increases in the physical intrusiveness of a device will lead to increases in a user's physical awareness of the monitoring.*

From a social perspective, one of the major concerns users have regarding intrusiveness is related to who has access to their information [8,46] and how it is used. Depending on their past experiences with monitoring, they may perceive a physically intrusive device to be a sign of an intrusive use of data at the social level.

Proposition 2. *The more a user perceives a device to be physically intrusive, the more likely they are to infer that the intentions of the monitoring are socially intrusive.*

It should be noted that provided there is trust between the observer and the observed, some level of intrusion can be accepted [72].

3.2. Awareness

"*The embeddedness characterizing ubiquitous technology makes it difficult for users to be aware of the monitoring possibility*" [32, p. 22]. This means in an IPS users may not know why they are being monitored, what data is being collected, or even how to control the technology [1,12,23,27,36], resulting in undesirable effects such as stress. One solution is to attempt to increase user-awareness of UM [48], using signs or tags indicating that monitoring is taking place. However, it is possible that using such indicators could have an inverse effect to what is expected. The intention is to create an awareness and sense of trust between the observer and the observed; however this may remove the opportunity for trust to be formed via more natural means e.g. in person, over an extended period [27]. Even if this could be avoided, informing users constantly of how and when they are being monitored is impractical [16]; the intrusiveness would detract from the passive goal of ubiquitous computing. This leaves users in an IPS with the only option of initially assuming that their activity or inactivity is being monitored [16], without necessarily understanding why.

Proposition 3. *An increase in physical awareness of the monitoring will initially increase user perceptions that the monitoring is socially intrusive.*

Through increases in awareness and understanding of a system, a user can control the workings of their environment to better suit them [15,48].

3.3. Boundaries

Current monitoring technologies are restricted to defined boundaries, and with the introduction of UM these boundaries are extended and in some cases even eliminated. UM's coverage (sensory range) makes it potentially difficult for users to find areas they perceive to be private [50], particularly if they are wearing the devices.

Proposition 4. *Increases in the sensory range of a device, or boundaries, will lead to perceptions of physically intrusive monitoring.*

Marx [45] describes four types of border including natural borders, social borders, spatial or temporal borders and ephemeral or transitory borders. Data can be shared across these borders and this will cause people to feel their privacy is invaded [45]. UM is likely to increase the number of these border crossings [11,50], sharing information across them [38], potentially causing behavioural changes and increases in perceptions of privacy invasion.

Proposition 5. *Increases in the sensory coverage of a device will lead to an expansion in the social boundaries across which the monitoring can be implemented, and data shared.*

Only by understanding the boundary violations caused by UM are we able to prevent any privacy concerns by identifying acceptable boundaries in which the monitoring can take place [72].

3.4. Control

"W*hen and how can a user turn off monitoring in a smart space*?" [54, p. 8] is a question that requires much needed attention. Control is an important aspect of ubiquitous computing [39], and simply being aware of or understanding the system often provides the user with some control over it [15,48]. In IPSs, control can be defined as the ability of users to manage how and by whom their data is controlled and used; changing users' perception of intrusion [60] and often leading to increases in user trust [56]. Having physical control over the monitoring could be considered as having control of the boundaries of the monitoring, as switching off the monitoring device reduces the range of data collection. Physical control also provides direct control over the use of the data and its access, as if the monitoring is not 'on', then no one is able to collect data or make any observations. This is similar to the relationship at the physical level where if there is control over who is watching, and how the data is used and shared, then there is control over the range of social boundaries across which the monitoring takes place.

Proposition 6. *An increase in physical control over the monitoring will result in a decrease in its sensory range or boundaries.*

Proposition 7. *Any increase in physical control of the monitoring will directly increase control over the social elements of UM.*

Proposition 8. *Increases in control over social elements of UM, will lead to decreases in its coverage and use across social boundaries.*

With this control will come an increased sense of awareness of both the monitoring and the environment, potentially altering users' behaviour, such as increasing users' self-consciousness [21,27].

Proposition 9. *Increases in physical control over the monitoring will lead to increases in users' physical awareness of the monitoring.*

However, any significant levels of control would also contradict one of the principles of ubiquitous computing (invisibility) [59], bringing computers back into the foreground, losing any sense of invisibility. Equally, entirely autonomous environments are likely to elicit negative responses from users, such as increases in anxiety [15,28,30], meaning IPSs must find a balance between manual and automated control.

3.5. Trust

Sufficient levels of trust are required for a successful deployment of an IPS [15,65]. Scholtz and Consolvo [56] define trust in ubiquitous computing as "*a user belief that a system will use the personal data it collects appropriately and not to cause harm*" (p. 86). Unless a user trusts who is carrying out the monitoring, how the data is collected and for what purpose, the monitoring is unlikely to be accepted [46,72], potentially resulting in undesirable effects. Information is likely to be shared across several social borders and if users do not trust or understand what information is shared and with whom, issues regarding privacy and security are likely to arise [38].

3.6. Justification

Justifying the reason for monitoring may encourage user acceptance. Such acceptance is often dependent on the context; for example monitoring in a prison is justified as it ensures that people securely isolated from the public are prevented from committing further crimes. Without justification, levels of trust are likely to decrease [60]. If the intention of the monitoring is not clearly understood, a user could interpret the monitoring to be surveillance, and any suspicion of surveillance can generate undesirable effects [12].

3.7. Context

IPSs can be designed to function in almost any context [16] (e.g. healthcare, workplaces, homes, transport/vehicles, shopping centres and public spaces), and with these come specific goals and tasks carried out by people in different roles. The UM technology used is thus dependent on the context, and if the functionality does not match the context, then users may not perceive it to be useful [59]. Privacy depends on situation and context [48] and when taking the view point that privacy is essentially about having control over the collection and use of data, control can be considered to have a similar dependency relation with context.

Table 1
Summary of literature

Factor	Research that addresses this factor
Intrusion	[8,16,24,30,33,44,46,56,57,60,61,72].
Awareness	[1,12,15,16,21,22,23,27,32,36,37,46,48,51,54, 55,59].
Boundaries	[5,6,11,16,20,35,37,41,45,50, 72].
Control	[1,15,17,20,24,25,27,28,30,33,37,39,43,46,48, 50,54,56,59,69,60,72].
Trust	[15,25,27,38,46,48,50,55,56,60,63,65,69,72].
Justification	[1,27,36,60].
Context	[1,9,16,27,37,48,56,70].

Table 1 summarises the existing research related to each factor and Table 2 summarises the research that identifies the relationships between each factor. Given that context affects all of the factors, and the complexity of such relations, it is not included in Table 2. In addition, as no evidence was found in the literature regarding the influence of the factors over justification, it was excluded as a column from Table 2.

4. Model

As stated earlier, many of the factors can influence behaviour in both the physical and social environments (represented in Fig. 1 by the light and dark rectangles). The factors context, awareness, intrusion, boundaries and control all have influence within *both* the physical and social environments, while justification and trust are limited to the social world.

Table 2
Existing positive and negative influences among actors identified in the literature and through own propositions (Px)

Influence of factors on Factors	Intrusion	Awareness	Boundaries	Control	Trust
Intrusion	*Positive* (+) P2	*Positive* (+) P1			
Awareness	*Positive* (+) [37,56], P3			*Positive* (+) [15,27,48]	*Positive* (+) [27,55]
Boundaries	*Positive* (+) [11,38,45,50], P4		*Positive* (+) P5		
Control	*Negative* (–) [46,60]	*Positive* (+) [21,27,59], P9	*Negative* (–) P6, P8	*Positive* (+) P7	*Positive* (+) [55]
Trust	*Negative* (–) [72]		*Negative* (–) [38]		
Justification	*Negative* (–) [46]				*Positive* (+) [60]

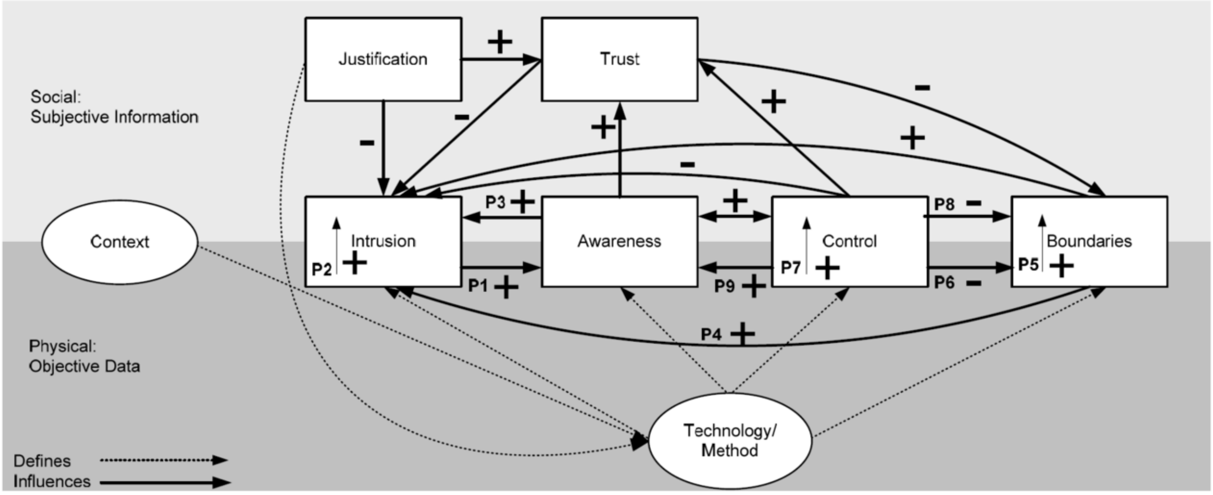

Fig.1. A model depicting the relation between factors in terms of physical and social worlds.

The purpose of the model in Fig. 1 is to visualise the positive and negative relations between factors, where each relation is either already hypothesised and tested in the literature (see Table 1) or is generated through the previous propositions. A positive influence is identified using a '+', and a negative influence using a '–'; those factors which cross the physical/social (world) line are considered to have influence in both realms.

The context, within which the monitoring takes place, influences what technology can practically and justifiably be used. The technology itself, a purely physical system, then defines the level of control a user has over the monitoring, the boundaries within which the monitoring takes place and the level of awareness and intrusion felt by the user. In turn, these influence the other factors as proposed, and ultimately determining how 'socially' intrusive the monitoring is.

4.1. Simulation

Understanding and appreciating the influence of each factor directly on one another, and indirectly though propagating the effects, is not easily achieved through examining the static model (Fig. 1). Since the model has the characteristic of system dynamics, the vensim program [66] was used to carry out a preliminary simulation in order to examine the impact of influence throughout the model.

Factors which vary depending on the technology selected (control, boundaries, intrusion, awareness) and which change subjectively with each user (trust, justification) were assigned starting values representing the strength of their presence in terms of the design, where S1 represents the social effects of a factor and where P1 represents the physical effects of a factor. Vensim allows these starting values to be manually changed during run time using slide bars, in the defined scale of 0 to 10 e.g. 0: no awareness to 10: total awareness. Such values were used to simplify the simulation, as no true scales have yet been developed.

In system dynamics, it is the change (increase or decrease) in a variable which is of interest, rather than the values themselves. Social intrusion was not given a starting value (i.e. set to 0), as it is a both a function of the other factors and is the means by which we judge the success of a system. Physical Awareness was also not given a starting value as it too, is purely a function of certain factors. The effect of changing these variables is propagated, enabling us to view the indirect effects of factors on others.

A positive influence from one factor to another is represented through adding the assigned values together. This then forms the new 'current' value of a factor, which is then propagated further. A negative influence is represented in a similar way by using subtraction. Thus the value for a factor consists of the value assigned to it (at runtime), in addition to the values that join to/influence it. This allows the influence of one factor further down the chain to show its influence towards the latter end. During run time the initial values representing the factors can be changed. When this occurs, a horizontal line within each rectangle will rise or fall depending on the sum of the

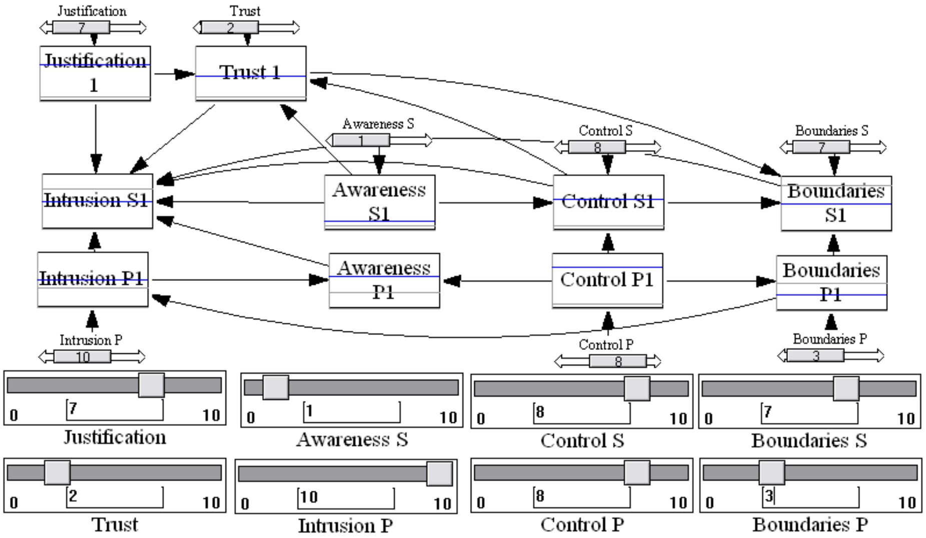

Fig. 2. A dynamic simulation of the relations between factors.

values being propagated and the relationships between factors. The output of the simulation is the final position of this line. As a result of the addition/subtraction method, the further into the model the values propagate, the greater their change will be (positive or negative) in comparison to the initial values.

In future simulations, the use of weighted links and averages will be considered, in addition to the possibility of using auxiliary variables with look ups to simulate changes in the polarity of specific relations. In such a case, a device may become totally unobtrusive, but this unobtrusiveness may unexpectedly be perceived as intrusive by a user, and so the positive relation between obtrusion and privacy invasion may become negative when a certain condition is met.

Social awareness (Awareness S1) appears to have four paths of influence to social intrusion (Intrusion S1), all of which are positive, that is, an increase in Awareness will have an overall positive propagation effect on Intrusion. These paths are as follows:

- Awareness S1, Control S1, Trust 1 to Intrusion S1
- Awareness S1, Control S1, Boundaries S1 to Intrusion S1
- Awareness S1 to Intrusion S1
- Awareness S1, Trust 1 to Intrusion S1

Physical control (Control P1) appears to have influence, directly and indirectly, to the majority of the other factors, thus confirming itself as one of the more prominent influencing factors. Two simulations were carried as an examination of how the completed model may be used, each representing a different scenario an IPS designer may face with different levels of experience of using the model. The values of this simulation may not currently prove to be entirely accurate; even so, the simulations act as a proof of concept in the process of building the final model. The results from the following simulations are not depicted.

4.1.1. Scenario 1: Exploratory assessment of two workplace monitoring systems

The purpose of this simulation is to mimic a designer exploring the effects of the types of monitoring devices that they intend to use. When seeing the effects of the factors on one another, it may assist the designer in making design decisions. The first simulation used input values which describe a hidden device in an office environment. These values were determined using simplistic scales whereby one of three values can be chosen, 0 (None), 5 (Moderate) or 10 (Total). As these simulations were intended as a proof of concept, this simplicity allowed us to explore controlled propagations. The input values are not limited to these scales, and when further scales are developed the propagated values will reflect this.

In this case, employees have been given some justification behind the monitoring, but as the device is hidden, are unlikely to trust the monitoring or have much control over its use. In addition (based on our current assumptions), the monitoring is likely to be perceived as physically intrusive, have a large sensory range, and employees are unlikely to be aware of or have control over the data collected (social level). The end result of the simulation is that the monitoring is perceived as intrusive, even though the device itself has been hidden from view. This is an interesting result since invisibility is one of the core principles of pervasive computing.

The second simulation used input values for a visible device, a camera, in an office environment. The familiarity of the device is likely to increase a user's awareness of the device's capabilities and their trust in it. As the device can be physically seen, and is restricted by walls and floors, levels of intrusion and boundaries are decreased, while levels of control are increased. The end result is a system which is perceived as slightly less intrusive. In terms of assessment, the second system appears to have an increased likelihood of acceptance and less of undesirable behaviours. This conclusion was reached by examining the value of social intrusion, which was the attribute used to assess the acceptance/desirability of a system (one of several possible behaviours which may occur in an IPS).

4.1.2. Scenario 2: Positive redesign of an airport monitoring system

The third simulation used input values from a preliminary design for an airport monitoring system to improve security. The design proposes that staff and visitors wear a clip-on RFID tag that must not be removed for their entire duration in the building. In this case, physical intrusion is high, physical control is low and physical boundaries are high – the device effectively has no boundary since it always monitors the wearer. The current design leads to a system which is perceived to be intrusive. A designer with experience with the model would understand that there is a strong link between physical intrusiveness (Intrusion P1) and social intrusiveness (Intrusion S1); and may decide to use a camera for security instead. The device may have reduced collection coverage when compared to the RFID tag, but it will most likely be interpreted as less intrusive by the occupants. In one instance, the designer could attempt to change the technology to be less physically intrusive with a decreased sensory range (physical boundaries), in this case a camera. Additionally, the designers may inform the users as to exactly who has access to the data collected, how it is used and what types of data are being collected. Couple this with the familiarity of a camera device and there are likely to be increases in trust in the system, and a small increase in control over the device. This all leads to a less intrusive system, which will ultimately lead to a wider acceptance and less undesirable behaviours. Even without sufficient empirical evidence for supporting and weighting the links between factors, the simulations provide some useful insights into the influential relations and therefore the impacts of the technologies used; while also allowing us to investigate the potential final application of the model.

4.2. Enhancing the model

We are interested in how UM affects the behaviour of those being monitored, and examined the approaches in technology acceptance studies as a method of modelling user behaviours. We assume that, if systems are not accepted, they are unlikely to be used as intended. The Technology Acceptance Model (TAM) [19] is an influential theory, based on the Theory of Reasoned Action (TRA) [3], which models how users come to accept and use a technology. While the model may initially seem an appropriate choice to theoretically link the factors to behaviour, in the context of this research there are other behaviours, in addition to acceptance, that could be displayed in a ubiquitously monitored environment.

TAM is an extension of the Theory of Reasoned Action (TRA) [3], which in turn was extended to incorporate perceived control to form the Theory of Planned Behaviour (TpB) (Fig. 3) [4]. The TpB can be used to predict and explain *any* human behaviour by examining its relation to intentions, attitudes and beliefs; this being its main strength over TAM.

The TpB works as follows: a person's intention to perform a behaviour is influenced by their attitude, subjective norms and perceived control over that behaviour (see Fig. 3).

Attitudes are an individual's positive or negative evaluation of the performance of behaviour, and are formed through beliefs about the consequences of a behaviour (behavioural beliefs).

Subjective norms are formed from beliefs concerning the perceived views of others regarding behaviour (normative beliefs) and a willingness to conform to those views.

Perceived control is constructed from beliefs about factors that may enhance or hinder performance of the behaviour (control beliefs) and the perceived power of these factors.

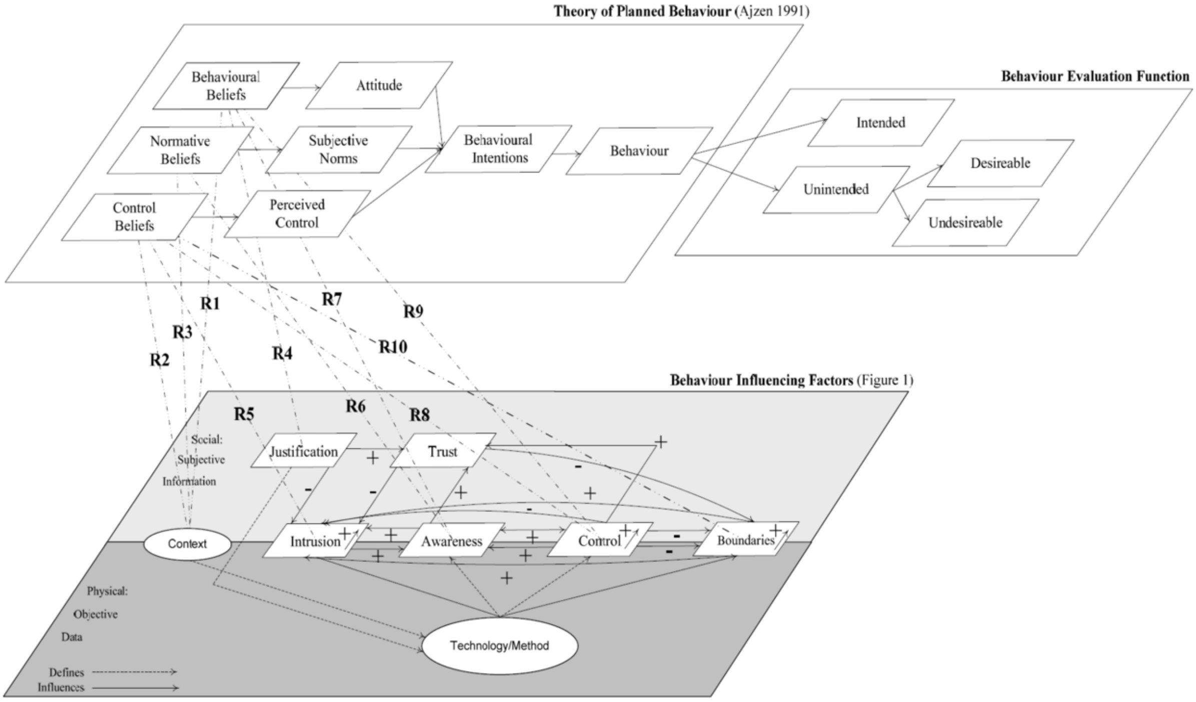

Fig. 3. A model for understanding, and potentially predicting, the behavioural impact of UM.

Subjective norm and perceived behavioural control can be used to predict intention, and therefore behaviour, provided empirical evidence is used to support the links [4]. The TpB can be linked to the existing model (Fig. 1) by examining how the behavioural factors influence salient beliefs (normative, behavioural, control) regarding a specific behaviour, such as acceptance e.g. high levels of social awareness will influence a persons normative beliefs, as they understand who is able to view their data/behaviours. Such influence can be propagated through the readily established links in the TpB producing a prediction for a behaviour. What follows is a description of how the identified behavioural factors (found in Fig. 1) relate to the TpB and salient beliefs, where Rx stands for Relation x.

R1, R2 and R3: Depending on the *context*, the consequences of certain behaviours may change, and through this, a person's behavioural beliefs can be affected/influenced. Different contexts may also encourage or prevent particular behaviours, thus influencing control beliefs. In addition, the importance of a person's opinion regarding a behaviour may change depending on the context (normative beliefs).

R4: Whether or not the monitoring can be *justified* may impact a person's behavioural beliefs, as should someone know why they are being watched, they are more likely to have an increased awareness of the consequences of particular behaviours.

R5: With different technologies come different levels of *intrusion*, changing a user's perception of how much control they have over the monitoring, and therefore their behaviour.

R6 and R7: *Awareness* of being watched could influence a person's normative beliefs, with the identity of the person/machine carrying out the monitoring altering their subjective norms. Without an awareness of being monitored, the user is likely to be less aware of the consequences of certain behaviours.

R8 and R9: Having *control* over aspects of an environment, or even the monitoring itself, could be seen as having control over behaviours and even control over their consequences, explaining both behavioural and control beliefs, e.g., if a person has control over heating and lighting it is likely to affect their energy saving behaviour.

R10: UM is potentially not restricted by physical constraint*s* and with this comes a lack of personal space, which is likely to influence a user's perception of how much control they have over a behaviour.

The outcome of the TpB is the behaviour of users, which are either intended or unintended from the designer's perspective. Depending on the user, the unintended behaviour can be interpreted as desirable or undesirable, and so a function for evaluating the behaviour needs to be developed. Past experience, and temporal and learning effects can be incorporated into the model through relaxation or strengthening of the relations between factors. For example, over time a user may become accustomed to a device, reducing their perception of its intrusiveness. This can be represented through weakening the relational weight between intrusion and the factors it is related to.

5. Discussion

5.1. Application of the model

Imagine that an undesirable behaviour has occurred in an IPS. In order to use the model in Fig. 3 to explain this behaviour, we must consider the users behavioural, normative and control beliefs about this behaviour. That is, beliefs about the consequences of this behaviour, the opinions of others about this behaviour and beliefs about factors that may encourage or prevent this behaviour.

These beliefs can be defined by moving backwards through the TpB, identifying user intentions, attitudes, subject norms and perceived control. In order to relate these beliefs to UM, we then examine how the identified behavioural factors influence those beliefs. This then provides one possible explanation of why the behaviour has occurred. A change in punctuality could be attributed to a worker's understanding that their employer is able to view their schedule details, influencing their normative beliefs. The knowledge or awareness obtained by the worker may have been through the monitoring system sharing this information. When sufficient empirical evidence is collected about the influence of these factors on salient beliefs, the model can then be used for predicting behaviours in UM. In this case, high levels of awareness could be empirically found to result in changes in punctuality (via normative beliefs). Once this knowledge is embedded into the model, future system designs which show high levels of user awareness are perhaps likely to result in a change in punctuality. Depending on whether this change is perceived to be desirable, one method for preventing it from occurring would be to reduce user awareness through changes to the systems design.

In its current form, both designers and evaluators of IPS systems may use the literature supported links in the model to assist in design choices. For example, understanding that there is an influential relation between intrusion and awareness may lead to improvements in the acceptance of future systems. A designer may attempt to analyse their system in terms of the factors described above, and then observe how each component will influence the other. This may highlight particular areas of the system that may produce undesirable effects.

In addition, the means by which links are made to the TpB may be used to link the factors to other behavioural models, such as TAM and its variations. This may lead to a more refined means of predicting/explaining specific behaviours, and may prove a fruitful direction for other studies to take.

5.2. Additional factors

Some additional factors have been identified which could also cause behavioural changes in an IPS. *Privacy, ethical, economic, cultural* and *legal* issues are important topics which have been studied in various contexts. Unfortunately these are not easily separated from the other factors, and as such, are difficult to integrate into the proposed model. However, their influence can be captured within one or more of the identified factors. For example, when considering different cultures, interpretations of the purpose and intention of the monitoring are likely to vary. The impact of this can be explained via the social factors of trust and justification. The physical attributes of a technology, such as the level of control it provides or its physical boundaries, are purely objective and can be considered independent of culture.

6. Future work and validation

Future work will involve confirmation of the relations between factors, and identification of the strength of these relations. Ideally, experiments would be conducted with real people, with observations made of the effects of devices and systems on them. However, there are several constraints in time and costs. In addition such systems are not easily found in real-life settings, and any such studies would suffer from the observer's paradox; how does one observe the behaviour of people without that very process of observation having influence. These issues also plague testing of the links between the factors and the theory of planned behaviour, and also the final validation of the model's predictive capabilities.

Another approach to testing the relations and their strengths is the use of questionnaires. A system may objectively be unobtrusive (i.e. embedded devices) but this is meaningless if a user perceives this system to be intrusive. Therefore a user's perception of these systems is an area that needs to be given more attention. It is also the case that this mode of a study is more viable given the current scope of this research.

A questionnaire will be used to examine how users value certain elements of monitoring system (e.g. control/awareness), which aims to capture their personality/preferences. Their perceptions of a given monitoring system will then be collected using a 5 point Likert scale. This scale will capture not only the polarity of the users perceptions, but also the strength between relations. To make use of the TpB, a series of questionnaires can be developed to capture the necessary information to 'fill in' the links between its components.

An agent based simulation will be used to validate the completed model. Each agent in the simulation will be assigned a persona, based on information collected during the first set of questionnaires. Specific areas of a simulated environment will then be defined as being monitored, and the movement behaviour of the agents will be observed.

The design of the monitoring system used in the simulation will be captured by the completed model. Further research will be carried out to incorporate user perceptions into the model. This will then enable the model to better predict the behavioural actions of users with similar perceptions of the system. To validate the model, the predicted behavioural response by the model will be compared to the observations made in the simulation.

To validate the more practical application of the model, a change in the systems design may be necessary to prevent certain behaviours. This design change can then be implemented in the simulation, where the behaviours of the agents are observed. If the expected behavioural response occurs, then the preventative element of the model will have been validated. Temporal effects may also be incorporated into both the simulation and the model, through minor changes to the agent personas and the strengths of links in the model respectively.

7. Conclusion

We are soon approaching the pervasive era of computing, which is likely to have a significant impact on our lives. Existing monitoring technologies can often cause undesirable effects, and it is anticipated that the new ubiquitous form of monitoring will enhance these effects due to the increase in its coverage. In light of the insufficient research in this area, we have described a preliminary model, consisting of a series of factors believed to influence behaviour and augmented by the TpB, allowing us to understand and potentially predict, and therefore prevent, the undesirable behaviours displayed by users in these environments. A better understanding of these issues will enable us to pre-empt these undesirable effects, which is expected to lead to improved designs of IPSs and their acceptance by users.

Acknowledgement

The authors wish to thank Prof. Colin Gray, of the School of Construction Management and Engineering at the University of Reading, for many fruitful discussions and the two anonymous reviewers for their valuable comments towards earlier manuscripts of this paper. The first author of this paper is supported by an EPSRC Doctoral Training Grant.

References

[1] G.D. Abowd and E.D. Mynatt, "Charting Past, Present, and Future Research in Ubiquitous Computing," *Special issue on human-computer interaction in the new millennium,* vol. 7, pp. 29–58, 2000.

[2] J.R. Aiello and C.M. Svec, "Computer Monitoring of Work Performance: Extending the Social Facilitation Framework to Electronic Presence," *Journal of Applied Social Psychology*, vol. 23, pp. 537–548, 1993.

[3] I. Ajzen and M. Fishbein, *Understanding Attitudes and predicting Social Behavior*, Prentice-Hall, 1980.

[4] I. Ajzen, "The Theory of Planned Behavior," *Organizational Behaviour and Human Decision Processes,* vol. 50, pp. 179–211, 1991.

[5] A. Albrechtslund, "House 2.0: Towards an Ethics for Surveillance in Intelligent Living and Working Environments," in *Seventh International Conference of Computer Ethics: Philosophical Enquiry*, San Diego, USA, 2007.

[6] A.A. Araya, "Questioning Ubiquitous Computing," in *Proceedings of the 1995 ACM 23rd Annual Conference on Computer Science*, Nashville, Tennessee, United States 1995, pp. 230–237.

[7] J. Beaudin, S. Intille, and E.M. Tapia, "Lessons Learned Using Ubiquitous Sensors for Data Collection in Real

Homes," in *CHI 2004*, Vienna, Austria, 2004, pp. 1359–1362.

[8] J.S. Beaudin, S.S. Intille, and M.E. Morris, "To Track or Not to Track: User Reactions to Concepts in Longitudinal Health Monitoring," *Journal of Medical Internet Research,* vol. 8, p. 29, 2006.

[9] M. Benerecetti, P. Bouquet, and M. Bonifacio, "Distributed context-aware systems," *Human-Computer Interaction,* vol. 16, pp. 213–228, 2001.

[10] M. Boheln, "Second Order Ambient Intelligence," *Journal of Ambient Intelligence and Smart Environments*, vol. 1, pp. 63–67, 2009.

[11] J.u. Bohn, M. Langheinrich, F. Mattern, and M. Rohs, "Living in a World of Smart Everyday objects – Social, Economic and Ethical Implications," *Human and Ecological Risk Assessment,* vol. 10, pp. 763–785, 2007.

[12] C. Botan, "Communication Work and Electronic Surveillance: A Model for Predicting Panoptic Effects," *Communication Monographs,* vol. 63, pp. 293–313, 1996.

[13] C. Botan and M. Vorvoreanu, "What do Employees Think About Electronic Surveillance at Work?" in *Electronic Monitoring in the Workplace: Controversies and Solutions*, J. Weckert, Ed., Idea Group Publishing 2005, pp. 123–144.

[14] V. Callaghan, G. Clarke, M. Colley, H. Hagras, J.S.Y. Chin, and F. Doctor, "Inhabited intelligent environments," *BT Technology Journal,* vol. 22, pp. 233–247, July 2004.

[15] V. Callaghan, G. Clarke, and J. Chin, "Some socio-technical aspects of intelligent buildings and pervasive computing research," *Intelligent Buildings International,* pp. 56–74, 2009.

[16] J. Cas, "Privacy in Pervasive Computing Environments – A Contradiction in Terms," in *IEEE Technology and Society Magazine*, vol. 24, 2005, pp. 24–33.

[17] D. Clements-Croome, P. Noy, and K. Liu, "Occupant Behaviour Analysis," in *IDCOP Scientific Report Series*, 2006, pp. 2–3.

[18] K.C. Cousins and D. Robey, "Patterns of Use within Nomadic Computing Environments: An Agency Perspective on Access – Anytime, Anywhere," in *Workshop on Ubiquitous Computing Environments*, Case Western Reserve University, 2003.

[19] F.D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly,* vol. 13, pp. 319–340, 1989.

[20] G.B. Davis, "Anytime/Anyplace Computing and the Future of Knowledge Work," *Communications of the ACM,* vol. 45, pp. 67–73, 2002.

[21] S. Dawson, B. Burnett, and F. McArdle, "Watching Learning From Behind Closed Doors: The Impact of Surveillance on Student Online Behaviour," in *ELearn 2005: World conference on E-learning in corporate, government, healthcare and higher education*, Vancouver, Canada, 2005.

[22] D. Dearman and K. Hawkey, "Exploring the Behavioural Effect of Location-Awareness within the Social Context of Rendezvousing," in *First Annual Workshop on the Social Implications of Ubiquitous Computing, CHI*, 2005.

[23] A.K. Dey, "Modeling and intelligibility in ambient environments," *Journal of Ambient Intelligence and Smart Environments,* vol. 1, pp. 5–14, 2009.

[24] D.C. Dryer, C. Eisbach, and W.S. Ark, "At what cost pervasive? A social computing view of mobile computing systems," *IBM Systems Journal,* vol. 38, pp. 652–676, 1999.

[25] K. Ducatel, M. Bogdanowicz, F. Scapolo, J. Leijten, and J.C. Burgelman, "Scenarios for Ambient Intelligence in 2010," 2001.

[26] R.C. Grant, C.A. Higgins, and R.H. Irving, "Computerized performance monitoring systems: Are they costing you customers?," *Sloan Management Review,* vol. 29, pp. 39–45, 1988.

[27] G.R. Hayes, E.S. Poole, G. Iachello, S.N. Patel, A. Grimes, G.D. Abowd, and K.N. Truong, "Physical, Social, and Experiential Knowledge in Pervasive Computing Environments," *Pervasive Computing,* vol. 6, pp. 56–63, 2007.

[28] H.v.d. Heijden, "Ubiquitous computing, user control, and user performance: conceptual model and preliminary experimental design," in *Research Symposium on Emerging Electronic Markets*, U. Lechner, Ed., Bremen, Germany: University of Bremen, 2003, pp. 107–112.

[29] S. Intille, K. Larson, J. Beaudin, E. Tapia, P. Kaushik, J. Nawyn, and T. McLeish, "The PlaceLab: a live-in laboratory for pervasive computing research (Video)," in *Proc. of Pervasive 2005 Video Program*, 2005.

[30] S.S. Intille, E.M. Tapia, J. Rondoni, J. Beaudin, C. Kukla, S. Agarwal, L. Bao, and K. Larson, "Tools for studying behavior and technology in natural settings," in *Proceedings of UbiComp 2003*, Berlin: Heidelberg: Springer, 2003, pp. 157–174.

[31] S.S. Intille, K. Larson, E.M. Tapia, J. Beaudin, P. Kaushik, J. Nawyn, and R. Rockinson, "Using a live-in laboratory for ubiquitous computing research," in *Proceedings of PERVASIVE 2006*, vol. LNCS 3968, Dublin, Ireland, 2006, pp. 349–365.

[32] K. Jonsson, "The Embedded Panopticon: Visibility Issues of Remote Diagnostics Surveillance," *Scandinavian Journal of Information Systems,* vol. 18, pp. 7–28, 2006.

[33] C.D. Kidd, R. Orr, G.D. Abowd, C.G. Atkeson, I.A.Essa, B. MacIntyre, E. Mynatt, T.E. Starner, and W. Newstetter, "The Aware Home: A Living Laboratory for Ubiquitous Computing Research," in *Proceedings of the Cooperative Buildings, Integrating Information, Organization, and Architecture, Second International Workshop, CoBuild'99,* vol. 1670, Pittsburgh, USA, 1999, pp. 190–197.

[34] A. Kirkeby, "Social Impact of Technologically Mediated Omnipresence," Department of Information and Media Studies, University of Aarhus 2003.

[35] S. Konomi and G. Roussos, "Ubiquitous computing in the real world: lessons learnt from large scale RFID deployments," *Personal and Ubiquitous Computing,* vol. 11, pp. 507–521, 2007.

[36] V. Kostakos and E. O'Neill, "Designing Pervasive Systems for Society," in *Second International Conference on Pervasive Computing, First International Workshop on Sustainable Pervasive Computing*, vol. 2, Vienna, Austria, 2004.

[37] V. Kostakos and L. Little, "The social implications of emerging technolgoies," *Interacting with Computers,* vol. 17, pp. 475–483, 2005.

[38] S. Lahlou, M. Langheinrich, and C. Roecker, "Privacy and Trust Issues with Invisible Computers," *Communications of the ACM,* vol. 48, pp. 59–60, 2005.

[39] M. Langheinrich, V. Coroama, J. Bohn, and M. Rohs, "As we may live – Real-world implications of ubiquitous computing," Institute of Information Systems, Swiss Federal Institute of Technology, ETH Zurich, Switzerland 2002.

[40] M. Langheinrich, "Personal Privacy in Ubiquitous Computing: Tools and System Support (PhD Thesis)," in *Swiss Federal Institute of Technology Zurich*: University of Bielefeld, 2005, p. 336.

[41] M. Langheinrich, V. Coroamă, J. Bohn, and F. Mattern, "Living in a Smart Environment – Implications for the Coming Ubiquitous Information Society," *Telecommunications Review,* vol. 15, pp. 132–143, 2005.

[42] J.R. Larson and C. Callahan, "Performance monitoring: how it affects work productivity," *Journal of Applied Psychology,* vol. 75, pp. 530–538, 1990.

[43] K. Lyytinen and Y. Yoo, "Issues and Challenges in Ubiquitous Computing," *Communications of the ACM,* vol. 45, pp. 63–65, 2002.

[44] K. Lyytinen, Y. Yoo, U. Varshney, M.S. Ackrman, G. Davis, M. Avital, D. Robey, S. Sawyer, and C. Sorenson, "Surfing the Next Wave: Design and Implementation Challenges of Ubiquitous Computing Environments," *Communications of the Association for Information Systems,* vol. 13, pp. 697–716, 2004.

[45] G.T. Marx, "Murky Conceptual Waters: the Public and the Private," *Ethics and Information Technology,* vol. 3, pp. 157–169, 2001.

[46] A.S. Melenhorst, A.D. Fisk, E.D. Mynatt, and W.A. Rogers, "Potential Intrusiveness of Aware Home Technology: Perceptions of Older Adults," in *Human Factors and Ergonomics Society 48th Annual Meeting*, HFES Press, 2004, pp. 266–270.

[47] R. Murty, G. Mainland, I. Rose, A.R. Chowdhury, A. Gosain, J. Bers, and M. Welsh, "CitySense: A Vision for an Urban-Scale Wireless Networking Testbed", in *Proceedings of the 2008 IEEE International Conference on Technologies for Homeland Security,* Waltham, MA, 2008.

[48] D.H. Nguyen and E.D. Mynatt, "Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems," Georgia Institute of Technology, June 2002.

[49] C. Patrikakis, P. Karamolegkos, A. Voulodimos, M.H.A. Wahab, N.S.A.M. Taujuddin, C. Hanif, L. Pareschi, D. Riboni, S.G. Weber, A. Heinemann, S.-c.S. Cheung, J. Chaudhari, and J.K. Paruchuri, "Security and Privacy in Pervasive Computing," *IEEE Pervasive Computing,* vol. 6, pp. 73–75, 2007.

[50] Y. Punie, "A social and technological view of Ambient Intelligence in Everyday Life: What bends the trend?," *Key deliverable, The European Media and Technology in Everyday Life Network (EMTEL).* 2003.

[51] F.J. Roethlisberger and W.J. Dickson, "Management and the Worker," *Cambridge, Mass: Harvard University Press,* 1939.

[52] R. Rosenthal and L. Jacobson, *Pygmalion in the classroom: Teacher expectation and pupils' intellectual development*. New York: Irvington publishers, 1968.

[53] J. Rule and P. Brantley, "Computerized Surveillance in the Workplace: Forms and Distributions," *Sociological Forum,* vol. 7, pp. 405–423, 1992.

[54] M. Satyanarayanan, "Pervasive Computing: Vision and Challenges," *Personal Communications, IEEE,* vol. 8, pp. 10–17, 2001.

[55] J. Scholtz and S. Consolvo, "Towards a Discipline for Evaluating Ubiquitous Computing Applications," *Intel Research,* 2004.

[56] J. Scholtz and S. Consolvo, "Toward a framework for evaluating ubiquitous computing applications," *Pervasive Computing, IEEE,* vol. 3, pp. 82–88, 2004.

[57] R. Sommer and R. Dewar, *The Physical Environment of the Ward*, Free Press of Glencoe, London, 1963.

[58] C. Sørensen and Y. Yoo, *Socio-Technical Studies of Mobility and Ubiquity*, Springer Boston, 2005.

[59] S. Spiekermann and F. Pallas, "Technology Paternalism – Wider Implications of Ubiquitous Computing," *Poiesis & Praxis: International Journal of Technology Assessment and Ethics of Science,* vol. 4, pp. 6–18, 2003.

[60] J.M. Stanton, "Reactions to Employee Performance Monitoring: Framework, Review and Research Directions," *Human Performance,* vol. 13, pp. 85–113, 2000.

[61] E. Tapia, S. Intille, and K. Larson, "Activity recognition in the home setting using simple and ubiquitous sensors," in *PERVASIVE 2004*, Vienna, Austria, 2004, pp. 158–175.

[62] E.M. Tapia, N. Marmasse, S.S. Intille, and K. Larson, "MITes: Wireless Portable Sensors for Studying Behavior," in *UbiComp 2004*, 2004.

[63] M. Theofanos and J. Scholtz, "A Framework for Evaluation of Ubicomp Applications," in *First International Workshop on Social Implications of Ubiquitous Computing, CHI*, Portland, OR, USA, 2005.

[64] T. Tibúrcio and E.F. Finch, "The impact of an intelligent classroom on pupils' interactive behaviour," *Facilities,* vol. 23, pp. 262–278, 2005.

[65] J.S. Valacich, "Ubiquitous Trust: Evolving Trust into Ubiquitous Computing Environments," in *Workshop on Ubiqutous Computing Environment*, Washington State University, 2003.

[66] Ventana, "Vensim PLE," Ventana Systems Inc., 2008.

[67] M. Vorvoreanu and C.H. Botan, "Examining Electronic Surveillance In The Workplace: A Review Of Theoretical Perspectives And Research Findings," in *the Conference of the International Communication Association*, Acapulco, Mexico, 2000.

[68] M. Weiser, "The Computer for the 21st Century," *Scientific American,* vol. 265, pp. 94–104, 1991.

[69] N. Winters, "Personal Privacy and Popular Ubiquitous Technology," in *Ubiconf 2004*, Gresham College, London, 2004.

[70] Y. Yoo and K. Lyytinen, "Measuring the Consequences of Ubiquitous Computing in Networked Organizations," *Sprouts: Working Papers on Information Environments, Systems and Organizations,* vol. 3, pp. 188–201, 2005.

[71] D. Zweig and J. Webster, "Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems," *Journal of Organizational Behavior,* vol. 23, pp. 605–633, 2002.

[72] D. Zweig, "Beyond Privacy and Fairness Concerns: Examining Psychological Boundary Violations as a Consequence of Electronic Performance Monitoring," in *Electronic Monitoring in the Workplace: Controversies and Solutions*, J. Weckert, Ed.: Idea Group Publishing, 2005, pp. 101–122.