

Ubiquitous Monitoring and Human Behaviour in Intelligent Pervasive Spaces

Stuart Moran and Keiichi Nakata

Informatics Research Centre
University of Reading,
Reading, UK

stuart.moran@reading.ac.uk, k.nakata@henley.reading.ac.uk

Abstract — we are soon approaching the pervasive-era of computing, where computers are embedded into objects and the environment in order to provide new services to users. Significant levels of data are required in order for these services to function as intended, and it is this collection of data which we refer to as ubiquitous monitoring. Existing monitoring techniques have often been known to cause undesirable effects, and it is anticipated that ubiquitous monitoring, with its increased coverage, will lead to increases in their occurrence and impact. To-date, the effects of ubiquitous monitoring on human behaviour has not been sufficiently investigated, further increasing the risk of undesirable effects. We propose a preliminary model consisting of a series of factors believed to influence behavior and is augmented by the theory of planned behavior. This model may allow us to understanding, predict, and therefore preventing any undesirable effects caused by ubiquitous monitoring.

Behaviour; Modelling; Monitoring; Pervasive; Ubiquitous

I. INTRODUCTION

Communities are groups of people who share needs, interests or practices. Such communities could include sports teams, employees in a workplace, families and hobbyists. Advances in wireless, mobile and sensor technologies enable ubiquitous access to information that could benefit these communities.

As this trend increases and technology advances further, the ‘pervasive-era’ of computing will soon become a reality. Mark Weiser [1] is generally considered the visionary who realised the potential of ubiquitous/pervasive computing, embedding computers into the environment so they are invisible from view, while still able to provide their intended services and functions. This means computers will become less of a focus in our daily lives, freeing us from the current mentality towards computers which is that direct interaction is necessary.

Intelligent Pervasive Spaces (IPSs) and their manifestations such as Intelligent Buildings (IBs) will be some of the first adopters of ubiquitous technologies. IPSs could facilitate the interaction between members of a community, although the functionality it provides will be entirely dependent on the context in which it resides. In order for information to be meaningful in an IPS and to provide other intended services, large amounts of data must be collected about users

continuously and ubiquitously [2]. It is this unbound collection of data in this way which we refer to as Ubiquitous Monitoring (UM).

Many different data types are collected in an IPS, and could augment and enrich communities. One example is the use of location data to increase sociability. Systems such as CitySense [3], 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 most people congregate indicating a popular area and therefore a place they are likely to enjoy. Other uses of location data have been in simplifying rendezvous behaviour between two or more people [4].

In order to make use of these applications, and other functions of IPS, users will have to sacrifice some of their privacy [4]. When location data is used in conjunction with additional contextually rich information, algorithms could be used to infer the context in which any user actions take place. Such functionality could lead to profound changes in our daily lives. Almost any type of information could be considered useful in an IPS given the potential scale at which these systems will function [5].

Monitoring is used extensively in society for healthcare, security and safety. Even though widely used, monitoring has often been known to cause problems such as increases in stress in those being observed [6]. UM differs from these methods as it has increased coverage, and is not physical restricted by walls or buildings.

Many of the same effects caused by current monitoring methods are still likely to occur in UM, while others will provide insights into the unexpected effects [7, 8]. These effects are likely to be enhanced due to the increased number of social contexts in which the monitoring takes place and across which the data is shared [9].

To date, the use of UM and its effect on human behaviour has not been sufficiently investigated [10, 11]. This means existing and future UM systems may cause undesirable side-effects, which may prevent the system from achieving its intended purpose. Should the system fail, it could negatively affect those who make use of it, both individually and as a community.

In this paper we present a model which could allow us to understand, predict and therefore prevent the undesirable

behavioural changes caused by UM. This model consists of a series of factors believed to influence behaviour related to UM and include: the *context* in which the monitoring takes place, whether or not it has been *justified*, the levels of *awareness*, *intrusion* and *control* implied by the technology used, the *boundaries* of the monitoring and whether those being monitored *trust* who is collecting the data and how it is used.

Ubiquitous computing consists of three interrelated environments, namely: physical, social and technical [12]. Each of the factors has influence in at least one of these environments. Context, control, intrusion, boundaries and awareness have influence in all of the environments, while the effects of justification and trust are confined to the social level. In terms of communities, it is anticipated that most of the significant behavioural changes will occur within the social environment.

The model is augmented by the Theory of Planned Behaviour [13] which forms a theoretical link between the factors and behaviour, while also providing a basis for the predictive potential of the model. By understanding and predicting the undesirable effects of UM, designers may be able to improve existing and future IPS systems, thus preventing any of the potential undesirable effects likely to be caused by UM [5, 11, 14].

II. BACKGROUND

A. Intelligent Pervasive Spaces

In this paper we use a working definition of an IPS *as an adaptable and dynamic area that optimises user services and management processes using information systems and networked ubiquitous technologies*. IPSs are often controlled by software known as intelligent agents which monitor the users and alter the environment according to ‘perceived’ or stated preferences, such as those related to temperature, lighting and humidity. The users can interact with the IPS in a multitude of ways including mobile devices and desktop computers. This is enabled by ubiquitous computing technology, where computers are everywhere and disappear into the environment.

Once sufficient data has been collected, the system takes into account the requirements of all the users and attempts to accommodate everyone in the changes made to the environment. Monitoring users and their preferences ubiquitously, in real time, is necessary for some features of IPS and other ubiquitous systems to function effectively.

B. Ubiquitous Monitoring

Surveillance and monitoring are terms which are often used interchangeably, but a distinction can be made between them: surveillance can be considered a form of monitoring, whereby an observers intention is to prevent certain user behaviours through risk of punishment [15]. Monitoring, on the other hand, is a generic term that describes the collection of information for any purpose [16], and so it is the intention of the monitoring which defines whether or not it can be considered surveillance. It is for this reason we use the term

‘ubiquitous monitoring’ as opposed to ‘ubiquitous surveillance’.

UM is the use of pervasive devices for monitoring in an IPS or other environment. These devices will generally be unrestricted by physical boundaries, and so their range will be significantly greater than that of existing monitoring technologies.

Most research to date that has investigated the effect of monitoring on human behaviour has mainly been conducted in the workplace [17]. The well known conclusion from this research is that monitoring causes some change in behaviour [18]. While these studies do provide an insight into the likely effects of UM [7], particular factors such as boundaries and ubiquity will not have been considered, limiting their use.

Among existing IPS and UM work, Tiburcio and Finch [19] looked at the positive impact an intelligent classroom has on pupil behaviour, and Clements-Croome et al. [20] conducted a study which found that occupants like their environments to be both controllable and adaptable.

Live-in laboratories such as the Place Lab [21], have been constructed in an attempt to create a naturalistic environment in which to study the behaviour of individuals in intelligent homes, a form of IPS. Some of the data collected through laboratory studies has shown that ubiquitous technology does cause a change in human behaviour [22]. There are, however, limitations to this method of study as the environment places constraints on behaviour variability [21] and is unlikely to generate many behaviours that would occur in real life scenarios [23].

UM systems are also being developed as a research method for observing natural behaviour [24]. It can be argued that without understanding the influence of UM on behaviour, any observations made using this method are unlikely to be truly natural.

III. BEHAVIOUR INFLUENCING FACTORS

“First we must understand the behavior of people and then develop the technology” [24, p2]. Without doing this prior to installing ubiquitous technologies, unintended effects may occur, and this is especially so with UM systems. Based on the examination of the monitoring and ubiquitous/pervasive computing literature, a series of seven factors related to UM were identified that are believed to affect human behaviour. Table 1 summarises the relationships between them found in the literature.

A. Trust

Trust is an essential factor when designing IPSs, and sufficient levels are required for an IPS to be successful [25]. UM will enable the collection of various types of data about the users, and should it be introduced without justification, levels of trust are likely to decrease [26].

According to [27] trust in ubiquitous environments is composed of three elements: privacy, awareness and control. 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 [7], potentially resulting in unintended side-effects.

As mentioned earlier, UM will extend or eliminate the boundaries of existing monitoring and such systems could cover multiple contexts, including both public and private spaces. Information is likely to be shared across these spaces and if users do not trust or understand what information is shared and with whom, issues regarding privacy and security are likely to arise [28].

B. Intrusion

UM systems make use of a range of technologies, with multiple ways in which to collect different types of data and varying forms of intrusiveness implied by each device [29] e.g., compare a CCTV camera with a wearable temperature sensor. Melenhorst et al. [29] define the intrusiveness of a ubiquitous device using three different perspectives: as a physical obstruction, a privacy invasion and a security risk. UM devices can be studied from all of these perspectives, but the most profound effect on behaviour is most likely to come from physical and privacy intrusions.

If UM technologies are to be accepted and used for lengthy periods they must not be perceived as intrusive [24, 29]. This perception is influenced by the familiarity and pervasiveness of the device, and the level of user control over the monitoring [26]. It should be noted that provided there is trust, *some* level of intrusion can be accepted [7].

In order for certain devices to be used for UM, a trade-off must be made, by the users, between its intrusiveness and its usefulness.

C. Control

There are two means of viewing control in UM. Firstly, there is control over the monitoring itself and secondly there is control over how the data is collected and used, and to whom it is made available. Entirely autonomous environments are likely to find undesirable responses from users [24], meaning IPSs should provide a means of interactive control.

With this interactive control will come an increased sense of awareness of both the monitoring and the environment, potentially altering users behaviour [30]. Having control over monitoring has been shown to be beneficial to users [26]; but with increased ubiquity and the level of data collection, there is the question of how much control a user should be given. High increases would actually contradict one of the principles of ubiquitous computing [31], bringing computers back into the foreground and losing any sense of invisibility.

D. Awareness

“The embeddedness characterizing ubiquitous technology makes it difficult for users to be aware of the monitoring possibility” [10, p22]. This implies in an IPS, users may not know why they are being monitored or what data is being collected, causing problems.

An obvious solution is to attempt to increase the awareness of users of the UM. However, there is suitable evidence to suggest that being aware of any monitoring can cause changes in user behaviour and attitude [17]. The more intrusive an UM device the more aware a user will be of the monitoring. Consider the intrusiveness of wearable temperature sensors: a

user could not wear such a device without having an increased awareness of the monitoring taking place.

The main issue here is how aware users should be made of the systems that are monitoring them and the data they collect. Another compromise must be made between user privacy and the risk of the undesirable behavioural effects that come with an increased awareness of monitoring.

E. Boundaries

Current monitoring technologies are restricted to defined boundaries, whether this be the view of a CCTV camera or the actions carried out on a desktop computer. With the introduction of UM these boundaries are extended and in some cases even eliminated.

An intrusive UM device could be seen as an invasion of personal space. UM is not restricted by walls and other physical objects and forces a decrease in personal space. When the boundaries between public and private spaces begin to blur information will be shared across them; and should people not understand what information is shared [28], behavioural changes associated with privacy invasion are expected to occur.

Marx [32] describes four types of borders including natural borders, social borders, spatial/temporal borders and ephemeral/transitory borders. Data can be shared across these borders and this will cause people to feel their privacy is invaded [32]. UM is likely to increase the number these border crossings [9] and therefore increase privacy invasion. By understanding the boundary violations caused by UM we are able to prevent these privacy concerns through identifying acceptable boundaries in which the monitoring can take place [7].

F. Context

In order to understand the true consequences of ubiquitous computing and UM, studies must be conducted in multiple contexts [33]. IPSs can be designed to function in almost any context [34], 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.

Capturing context is not always straightforward. Some IPSs such as new developments in hospitals may represent multiple contexts: not only is a hospital a specialised IPS in terms of healthcare, but it also acts as a workplace for staff, a public place for visitors and potentially a place of education and research. As users move from context to context in any IPS their experience of the system and the services provided will change [35], as such, a hospital would be a particularly interesting environment in which to study all of the factors mentioned.

G. Justification

Justification depends strongly on the context, for example monitoring in a prison is justified as it ensures that people are prevented from committing further crimes. However, monitoring shopping habits cannot be as easily justified and is therefore not as readily accepted. Without justification, levels of trust are likely to decrease [26].

A method of monitoring may be justified in its purpose, but the data collected may not. A good example of this would be whether or not CCTV cameras should record audio as well as video.

TABLE I. EXISTING POSITIVE AND NEGATIVE INFLUENCES AMONG FACTORS IDENTIFIED IN THE LITERATURE

<i>Influence of factors on</i>	<i>Trust</i>	<i>Intrusion</i>	<i>Control</i>	<i>Boundaries</i>	<i>Awareness</i>
<i>Factors</i>					
<i>Trust</i>		[7]		[28]	
<i>Control</i>	[36]	[29] [26]			[31] [30] [8]
<i>Boundaries</i>		[9] [37] [32] [28]			
<i>Awareness</i>	[8] [36]	[27] [38]	[12] [8] [39]		
<i>Justification</i>	[26]	[29]			

IV. BEHAVIOUR MODELS

What we are interested in is how UM affects the behaviour of those being monitored. Arguably, the effects on behaviour can be analysed by studying whether ubiquitous technology is accepted by users. As such, we examined the approaches in technology acceptance studies as the method of modelling user behaviours. We assume that, if systems are not accepted, they are unlikely to be used as intended or if at all.

The Technology Acceptance Model (TAM) [40] is an influential theory which models how users come to accept and use a technology. While the model initially seemed an appropriate choice to theoretically link the factors to behaviour, in the context of this research there are more behaviours other than acceptance that could be displayed in a ubiquitously monitored environment.

TAM is an extension of the Theory of Reasoned Action (TRA) [41], which itself was extended to incorporate perceived control to form the Theory of Planned Behaviour (TpB) [13]. The TpB can be used to predict and explain human behaviour by examining its relation to intentions, attitudes and beliefs. A person's intention to perform a behaviour is influenced by their attitude, subjective norms and perceived control over that behaviour. These are in turn determined by behavioural, normative and control beliefs respectively. When predicting behaviour, empirical evidence must be collected to support the relations between variables. The model presented in depicts the relationship between these factors and the TpB. Using this model we are able to explain why a behaviour has occurred by investigating how the factors, which act as external variables, influence salient beliefs. Including the TpB not only creates a more relevant behavioural analysis tool but may also provide more insights into why a behaviour has occurred in the first place.

V. UBIQUITOUS ENVIRONMENTS

Ubiquitous computing consists of three interrelated environments: social, technical and physical, where a change in one will affect the other [12]. Analysing the problem using this framework creates the opportunity to view it from different levels. Each factor described above influences behaviour in different ways and can be categorised into the three different levels based on these environments.

The physical level focuses on the physical attributes and initial effects of UM, the technical level examines the functions of a device and what data is collected, and the social level focuses on the social attributes and use of the data. Categorising the influence of each factor in this way gives them a wider scope and allows the model to be used generically, while still leaving open the option of focusing on a specific context or system.

A. Physical Level

Pervasive sensors and other devices are used for UM, and their physical presence will act as visual cue of the monitoring and data collection taking place. As devices become smaller, unobtrusive monitoring becomes more realistic; however, the physical actuations as a result of the monitoring will still act as a sign of the monitoring taking place. The physical boundaries of ubiquitous devices could also cause decreases in perceptions of private space. Whether in a building, outside or even in a vehicle, the physical context of the monitoring could influence behaviour.

B. Technical Level

The devices used for UM vary in their purpose and functions. Different types of data are required for automating particular aspects of a person's life, and require different methods of collection. Such data could include user's preferences on heating, their natural behaviours or even their bank account details; no information in an UM environment need be considered useless. Ideally this data should be collected passively but in some cases the devices will be placed near or on a user, and this presence could be perceived as an intrusion of their personal space. Even when data is collected passively, the data itself could equally be considered intrusive of personal privacy. In some scenarios, UM devices will provide or restrict user control over the environment and other variables and perhaps even the monitoring itself.

C. Social Level

One of the major social issues related to any form of monitoring is whether or not it can be justified. Further to this, the types of data, levels of data collection and who has access all need justification. This is also dependent on the nature of the people being monitored, and the shared understanding of what is and is not *normally* accepted in the society and social context to which they belong. In relation to the data, people should be aware of, have control over and trust how much data is collected, who has access to this data, the types of data and how it is used. Some of the data collected could be perceived as intrusive of personal privacy. This data is likely to be made widely available in a person's life, shared across home and

work environments causing issues with data access. Hospitals, schools, workplaces, shopping centres and the home are all social contexts in which UM may occur, and will have a significant impact on users' behaviour and acceptance of the monitoring.

By examining the influence of each factor in the three different environments of ubiquitous computing, it is clear that certain factors are likely to have a greater impact than others. *Intrusion, awareness, control* and *boundaries* are factors that have some influence across all three environments, while *context, justification* and *trust* generally see influence in only the social environment. An individual's behaviour is most likely to change as a result of the physical and technical environments. When acting within a community, it is expected that it is in the social environment where the majority of behavioural changes will occur.

VI. PROPOSED MODEL

Based on the factors identified above, and the relationships proposed among them, Figure 1 describes the model for understanding the effects of ubiquitous monitoring on human behaviour. The context in which monitoring resides and the justification behind it will affect which technology is chosen for monitoring users. Justification is only likely to be meaningful if it is trusted. Levels of awareness, control and intrusion felt by the user, as well as the boundaries of the monitoring are all defined by the technology itself. These factors in turn are believed to influence user behaviour through their salient beliefs.

What follows is a description of how the identified behavioural factors relate to the TpB and salient beliefs:

- *R1 and R2*: Depending on the *context*, the consequences of certain behaviours may change, and through this, a person's behavioural beliefs can be explained. Different contexts may also encourage or

prevent particular behaviours, thus influencing control beliefs.

- *R3*: 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.
- *R4 and R5*: *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.
- *R6 and R7*: 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.
- *R8*: UM is potentially *unbound* 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
- *R9*: 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.

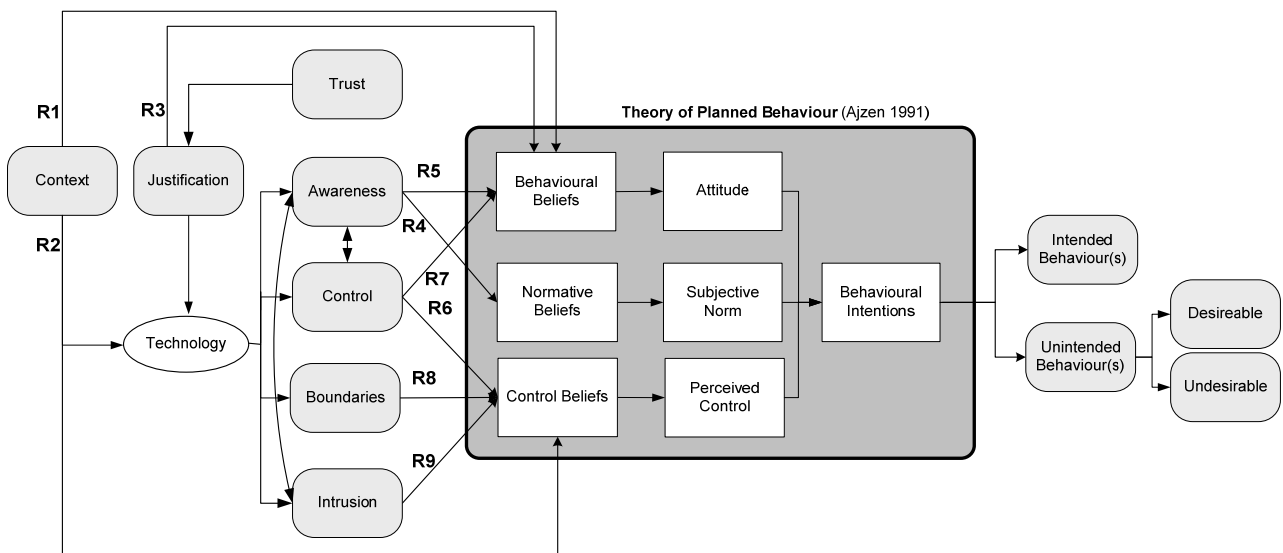


Figure 1 Model for understanding the effects of ubiquitous monitoring on human behaviour

There is perhaps an inherent relationship between levels of intrusion and awareness, where intrusive methods of monitoring result in a greater sense of awareness than unobtrusive methods. Having control over the monitoring or the environment is also likely to have the same effect on awareness. The behaviours displayed by users of an IPS are either. The outcome of the TpB is behaviour, which was 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 behaviour needs to be developed. Past experience, 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 intrusiveness. This can be represented through weakening the weight between intrusion and the factors it's related to.

VII. DISCUSSION

The model presented in this paper uses the TpB to link a series of factors which are believed to influence behaviour in UM environments and the behaviours exhibited by their occupants. These factors act as external variables, explaining salient beliefs and therefore behaviour. The model also describes how these factors relate to one another.

Our model acts as a first step to identifying the likely impact of particular factors on human behaviour, establishes a means of understanding this behaviour and provides a basis for investigating how these factors can be used to predict behaviours. The current model is limited in the sense that it only identifies the potential relationships between the factors and the TpB based on the literature, without empirical evidence to support them. In order to enhance the model, a series of experiments and surveys will be conducted to discover to what extent the factors discussed affect behaviour and the strength of the relationships between each factor. Since the model has the characteristic of system dynamics, software such as VenSim [42] could be used to carry out a preliminary simulation examining the effects of propagation on factors in the model.

A. Application of the model

Imagine that an undesirable behaviour has occurred in an IPS. In order to use the model in Figure 1 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 rendezvous behaviour could be attributed to a worker's understanding that their employer is able to view their schedule details, influencing their normative beliefs. When enough empirical evidence is collected about

the influence of these factors on salient beliefs, the model can then be used for predicting behaviours in UM.

B. Other potential factors

Some additional factors have been identified which could cause behavioural changes in an IPS. *Privacy, Ethical, Economic 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 represented within one or more of the other factors.

VIII. CONCLUSIONS

Intelligent pervasive spaces are fast becoming a reality, and monitoring technologies and techniques are likely play an essential part in their success. Monitoring has often been known to cause undesirable effects on people. Ubiquitous monitoring differs from existing monitoring methods with its distinct lack of physical boundaries. Even this difference, it is likely to cause not only the same effects as existing methods, but also the more disconcerting unexpected or unseen effects. To date, there has been a lack of systematic study into the impact of this type of monitoring on human behaviour. This means existing and future systems could cause undesirable effects.

In this paper we propose a model which consists of a series of factors related to ubiquitous monitoring, namely: trust, control, boundaries, intrusion, awareness, context and justification identified through literature. The model depicts the relationships between these factors, and is augmented by the Theory of Planned Behaviour which provides a theoretical link to behaviour. By understanding and predicting the potential undesirable effects of UM it will be possible to prevent them from occurring

REFERENCES

- [1] M. Weiser, "The Computer for the 21st Century," *Scientific American*, vol. 265, pp. 94-104, 1991.
- [2] A. Albrechtslund, "House 2.0: Towards an Ethics for Surveillance in Intelligent Living and Working Environments " presented at Computer Ethics Philosophical Enquiry, San Diego, USA, 2007.
- [3] 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 " presented at In Proceedings of the 2008 IEEE International Conference on Technologies for Homeland Security, , Waltham, MA, 2008.
- [4] D. Dearman and K. Hawkey, "Exploring the Behavioural Effect of Location-Awareness within the Social Context of Rendezvousing," presented at First Annual Workshop on the Social Implications of Ubiquitous Computing, CHI, 2005.
- [5] M. Langheinrich, "Personal Privacy in Ubiquitous Computing: Tools and System Support," in *Swiss Federal Institute of Technology Zurich: University of Bielefeld*, 2005, pp. 336.
- [6] M. Vorvoreanu and C. H. Botan, "Examining Electronic Surveillance In The Workplace: A Review Of Theoretical Perspectives And Research Findings," presented at the Conference of the International Communication Association, Acapulco, Mexico, 2000.

- [7] 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.
- [8] 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.
- [9] 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.
- [10] K. Jonsson, "The Embedded Panopticon: Visibility Issues of Remote Diagnostics Surveillance," *Scandinavian Journal of Information Systems*, vol. 18, pp. 7-28, 2006.
- [11] 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.
- [12] D. H. Nguyen and E. D. Mynatt, "Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems," Georgia Institute of Technology June 2002.
- [13] I. Ajzen, "The Theory of Planned Behavior," *Organizational Behaviour and Human Decision Processes*, vol. 50, pp. 179-211, 1991.
- [14] G. B. Davis, "Anytime/Anyplace Computing and the Future of Knowledge Work," *Communications of the ACM*, vol. 45, pp. 67 - 73, 2002.
- [15] J. Rule and P. Brantley, "Computerized Surveillance in the Workplace: Forms and Distributions," *Sociological Forum*, vol. 7, pp. 405-423, 1992.
- [16] 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.
- [17] 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.
- [18] J. R. Larson and C. Callahan, "Performance monitoring: how it affects work productivity," *Journal of Applied Psychology*, vol. 75, pp. 530-538, 1990.
- [19] T. Tibúrcio and E. F. Finch, "The impact of an intelligent classroom on pupils' interactive behaviour," *Facilities*, vol. 23, pp. 262 - 278, 2005.
- [20] D. Clements-Croome, P. Noy, and K. Liu, "Occupant Behaviour Analysis," in *IDCOP Scientific Report Series*, 2006.
- [21] 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)," presented at Proc. of Pervasive 2005 Video Program, 2005.
- [22] J. Beaudin, S. Intille, and E. M. Tapia, "Lessons Learned Using Ubiquitous Sensors for Data Collection in Real Homes," presented at CHI 2004, Vienna, Austria, 2004.
- [23] 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.
- [24] 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," presented at Proceedings of UbiComp 2003, Berlin, 2003.
- [25] J. S. Valacich, "Ubiquitous Trust: Evolving Trust into Ubiquitous Computing Environments," presented at Workshop on Ubiquitous Computing Environment, Washington State University, 2003.
- [26] J. M. Stanton, "Reactions to Employee Performance Monitoring: Framework, Review and Research Directions," *Human Performance*, vol. 13, pp. 85-113, 2000.
- [27] J. Scholtz and S. Consolvo, "Toward a framework for evaluating ubiquitous computing applications," *Pervasive Computing, IEEE*, vol. 3, pp. 82-88, 2004.
- [28] S. Lahlou, M. Langheinrich, and C. Roecker, "Privacy and Trust Issues with Invisible Computers," *Communications of the ACM*, vol. 48, pp. 59-60, 2005.
- [29] A.-S. Melenhorst, A. D. Fisk, E. D. Mynatt, and W. A. Rogers, "Potential Intrusiveness of Aware Home Technology: Perceptions of Older Adults," presented at Human Factors and Ergonomics Society 48th Annual Meeting 2004.
- [30] S. Dawson, B. Burnett, and F. McArdle, "Watching Learning From Behind Closed Doors: The Impact of Surveillance on Student Online Behaviour," presented at ELearn 2005: World conference on E-learning in corporate, government, healthcare and higher education, Vancouver, Canada, 2005.
- [31] 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.
- [32] G. T. Marx, "Murky Conceptual Waters: the Public and the Private " *Ethics and Information Technology*, vol. 3, pp. 157-169, 2001.
- [33] 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.
- [34] J. Cas, "Privacy in Pervasive Computing Environments - A Contradiction in Terms," in *IEEE Technology and Society Magazine*, vol. 24, 2005, pp. 24-33.
- [35] Y. Yoo and K. Lyytinen, "Social impacts of ubiquitous computing: Exploring critical interactions between mobility, context and technology," *Information and Organization*, vol. 15, pp. 91-94, 2005.
- [36] J. Scholtz and S. Consolvo, "Towards a Discipline for Evaluating Ubiquitous Computing Applications," *Intel Research*, 2004.
- [37] 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.
- [38] V. Kostakos and L. Little, "The social implications of emerging technologies," *Interacting with Computers*, vol. 17, pp. 475-483, 2005.
- [39] 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.
- [40] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology. ," *MIS Quarterly*, vol. 13, pp. 319-340, 1989.
- [41] I. Ajzen and M. Fishbein, *Understanding Attitudes and predicting Social Behavior*: Prentice-Hall, 1980.
- [42] Ventana, "Vensim PLE," Ventana Systems Inc., 2008.