

Some Socio-Technical Aspects Of Intelligent Buildings and Pervasive Computing Research

Vic Callaghan, Graham Clarke, Jeannette Chin
lifestyles@essex.ac.uk
The Digital Lifestyles Centre, Essex University, UK
(<http://digital-lifestyles.essex.ac.uk>)

"You had to live--did live, from habit that became instinct--in the assumption that every sound you made was overheard, and ... every movement scrutinized"
- George Orwell 1984

Abstract:

Recent reports from the European Parliament Technology Assessment unit and the UK Information Commissioner's Office have highlighted the need for debate on how society should balance the convenience that new technology affords with the need to preserve privacy. To date, most of the debate has addressed the more visible aspects of technology and privacy such as surveillance cameras, identity/loyalty cards, internet search engines and RFID tags. In this paper we seek to use our experience as computer scientists to advance this debate by considering issues arising from our research related to intelligent buildings and environments, such as the deployment of autonomous intelligent agents. Intelligent buildings and environments are based on the use of numerous "invisible", omni-present, always on, communicating computers embedded in everyday artefacts and environments. Whilst most current intelligent building technology is based around automated reactive systems, research is underway that uses technology to gather personal information from people and use this information to deliver personalised services to them. While promising great benefits this technology, by being invisible and autonomous, raises significant new dangers for individuals and society as a whole. Perhaps the most significant issue is privacy - an individual's right to control the collection and use of personal information. Rather than focusing on the 'here and now', this paper looks forward to where this research could lead, exploring the issues it might involve. It does this by presenting descriptions of current work, interleaved with a set of short vignettes that are intended to provoke thought so that developers and the population at large might consider the personal and regulatory needs involved. We end this paper by offering a conceptual framework for situating multi-disciplinary socio-technical research in Intelligent Buildings.

Keywords: intelligent buildings, digital homes, pervasive computing, intelligent agents, socio-technical, privacy, ethics

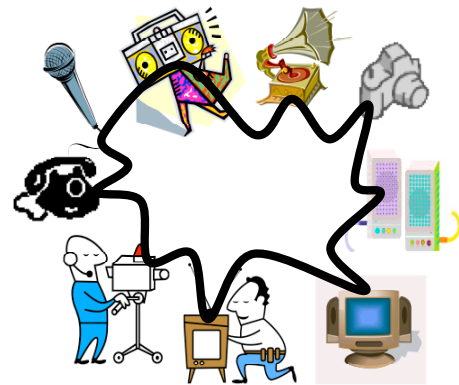
1.0 Introduction

Recent reports from the European Parliament Technology Assessment unit [EPTA 2006] and the UK Information Commissioner's Office [ICO 2006] have highlighted the need for debate on how society should balance the convenience that new technology affords with acceptable social ethics, such as the need to preserve personal privacy. To date, most of the debate has addressed the more visible aspects of technology and privacy such as surveillance cameras, identity/loyalty cards, RFID tags and internet search engines. In this paper we seek to extend this debate to address intelligent buildings and smart environments, in

particular the issues arising from the use of autonomous intelligent agents as part of such technology.

Existing intelligent buildings use computers to control building services such as heating and lighting. A vision for this technology is that, as networked computers become ever more pervasive, intelligent building technology will embrace any space that people inhabit extending from homes, offices, & factories through cars, aeroplanes & spacecraft to the ultimate vision for supporting mankind's long term habitation of deep space. In wholly technological environments such as spaceships and planetary habitats, computer controlled environment will be essential. [Clarke 00].

Technology View 1 – Research is challenging the nature of building technology. One possibility is that buildings will be populated with numerous networked functions (or services) which sense and communicate user behaviour. Agents or people will be able to combine these into coordinating groups to form traditional or novel appliances, applications or environments. Agent based environments will continually adapt to the users needs (Ambient Intelligence); user based environments will empower people's creativity to enable them to be the designers of there own building functionality.



In its most general sense, this vision underlies what is variously described by the terms intelligent buildings, digital homes, ambient intelligence, pervasive computing, ubiquitous computing and sensor networks. The International Telecommunications Union (ITU) released a useful description of this general vision in a report at the UN net summit in Tunis in November 2005 describing our future as “living in a new era of an Internet of Things” [ITU 05]. The report states that Radio Frequency Identification (RFID) tags, sensors and nanotechnology have made processing power increasingly available in smaller packages so that networked computing “dissolves” into the everyday objects around us forming a ubiquitous connected society; one in which networks and networked devices are omnipresent, offering new forms of collaboration and communication between people and “things”, and between “things” themselves, hitherto unknown and unimagined. One of the concerns that the report highlighted was privacy: “privacy protection should become part of the design itself of the technology, even before it makes it to market.” There are many indicators that such a world may not be that far away. For instance the Internet has grown from zero to over 200 million users in a little over 10 years. Even more remarkable, mobile phone use has grown from nothing to a truly massive 680 million worldwide users in a similar period [Chin 03]. However, these figures are dwarfed by the number of embedded processors (the components of intelligent buildings and pervasive computing); one report estimates a staggering 7 billion microprocessors were sold in 2001, only 2% of which were destined for PCs the rest being incorporated into embedded computing systems [Metcalf 01]. Predictions are that this trend will accelerate with companies such as Intel (the worlds largest chip manufacturer,) expecting that by 2010 that there will be around 1,000 microprocessors per person on this planet [DTI 06]. Sun, the inventors of Java, have seen such a massive use of Java in mobile phones that they have developed a new generation of innovative Java enabled wireless embedded computers to service this new market (Horan 05). These developments are but the forerunners of a massive, omni-present, always-on ubiquitous networking technology that promises to connect not just every citizen of this

planet, but ultimately every artefact in the world. The forces propelling this technology forward are massive, for instance, in terms of national economies, according to Japan's General Affairs Ministry, Japan's pervasive computing market will grow to over \$760 billion (84 trillion Yen) by the year 2010 [DTI 06]. Not only are there large commercial interests involved but in an age of terrorism, significant political pressures too.

Thus, locating such systems in personal, political and commercially sensitive areas of society as part of intelligent buildings will have significant consequences for individuals and society. Clearly, with such a massive connected sensory network in place there will be opportunities for the misuse by companies, governments and individuals of information. Such pressures are already evident, such as the release for 'research purposes', of twenty million of ordinary peoples' online search queries from AOL in August 2006 [Barbaro 06].

In the following pages, we will seek to explain what this technology is, how it might develop and the ramifications for the individual and society. In doing this we combine factual accounts of the technology with short stories that are intended to stimulate further thought.

2.0 Pervasive Computing & Intelligent Embedded Agents

Pervasive computing describes the distribution of service providing embedded networked computers on such a massive scale as they pervade all areas of our lives, in particular, forming the invisible technical infrastructure. Lou Gerstner, CEO of IBM, described pervasive computing as a vision where "... *a billion people will interact with a million e-businesses via a trillion interconnected devices*" [Gerstner 99]. Embedded Computers are processors that are integrated into appliances and machines. Intelligent embedded agents are reasoning, planning and learning processes that run on embedded computers (i.e. processors that are able to mimic some of the qualities we associate with intelligence in ourselves) [Callaghan 04]. Intelligence is regarded as being important in creating future generations of intelligent buildings and environments as it provides a way of managing the complexity associated with configuring and programming the large numbers of connected devices and enabling the systems to adapt over time to meet peoples changing needs and the changing environment. Intelligent agents are intended to remove the cognitive load from people by assuming some of the technically sophisticated decision-making. They filter information provided by their human users based upon sensing and reasoning about what the user is seeking to achieve, freeing the user to get on with more productive and useful tasks. Intelligent buildings displaying such properties are said to display ambient intelligence. Research to generate the technology to support this vision is now well under way and perhaps the most influential benchmark for this vision is a report entitled "Scenarios for Ambient Intelligence in 2010" produced by the European Community Information Society Technologies Advisory Group (ISTAG) in 2001 [Ducatel 01]. The ISTAG report envisions a pervasive computing world in which everyday environments such as intelligent buildings are built from numerous artefacts containing tiny, sometimes physically invisible, omni-present, and always-on computers with attached sensors and actuators, communicating and collaborating with each other to control and offer information relating to the environments we live in. Pervasive computing and informatisation will generate massive opportunities for the development of intelligent structures at every level of the urban landscape and that this in itself will give rise to the real need to solve the problems that we have flagged throughout this paper [Clarke 2007].

Clearly, whatever the particular technology employed, such systems require vast numbers of sensors and monitoring devices to acquire and interpret information on what the users are doing. Whilst this technology is advertised as offering benefits e.g. improved energy efficiency and quality of life for the building occupants, increased profitability for companies etc., the presence of sensors and networked intelligent agents gathering information about people is an issue that needs very serious consideration.

Story #1 – Human versus Machine Intelligence: *Norman felt that he was being watched, no matter where he went or what he did. Often he imagined that out of the corner of his eye he could see them moving, or their shadows looming, some sign anyway of their presence, the 24/7 watchers that observed his every move like some auditor in hell as his sins were logged. Norman was mad of course and in a new generation of ‘virtual asylums’; high-tech spaces in which his behaviour was monitored and controlled without the need for expensive staff. Because his activity was stereotypical, repetitive, obsessive and compulsive he was ideally suited to being monitored and serviced by embedded agents who could learn his patterns and provide for him as he required, signalling to his human guardians if he went beyond his ‘safe bounds’. One lesson that had become obvious to all those who worked on characterising human behaviour using agents was that fixed and repeatable patterns were what suited the technology best. The free and spontaneous flux of life where each activity was subtly different and unpredictable was intractable to the mechanised system. After years of research the embedded agent technology that derived rules from the patterns of behaviour of the occupants had proved conclusively that rigid, fixed and habitual behaviour patterns were what suited the learning mechanisms best. In fact the joke amongst the technical staff of the virtual asylum was – ‘you don’t have to be mad to be here, but it helps!!’*

We believe that a significant issue is privacy - an individual’s right to control the collection and use of personal information by third parties. The ongoing theme of this paper is the question who should exercise this control. Should it be the individual, government, commercial organizations or some combination of each? Related critical questions are how should that control be affected, what regulation of this technology is required and how should it be policed?

2.1 Intelligent Buildings - Domestic Environments

The home is one of the most important areas for the application of pervasive computing. Craig Mundie, chief technology officer of Microsoft, was reported in the Economist [Economist 05] as saying “We view the digital home as critically important the home is much more exciting than the workplace”. The home is the most private and personal space for individuals; most people are protective of their privacy, and technology that has sensors and records our ‘private lives’ is likely to meet with strong resistance unless there are overriding benefits.

In the home environment, intelligent buildings are more frequently called smart-homes or digital homes. A noteworthy example is the ‘Integer House’; a venture to encourage change in home building practices, particularly those that enable the creation of more environmentally friendly homes [Kell, 2005]. From its initial roots in Watford in 1996, where it built a single demonstration home on the Building Research Establishments site, more than one hundred organisations have participated as it grew to have sites in countries such as Ireland and China.



Technology View #2 *iDorm; a digital home testbed at Essex University where people can experience the use of intelligent agents that build a model of people's preferences based on their previous behaviour. The agents pre-emptively control the environment based on these learnt preferences.*

Smart homes have noble aims; they are said to be able to improve energy conservation, comfort, health, security, entertainment and communication. Control of these systems is generally accomplished by writing computer programs which include, for example, conditional statements such as “if the room is unoccupied, set the heating to minimum and turn lights to off” [Callaghan 04] More sophisticated systems are able to learn (self-program) based on monitoring a user's habits, replacing pre-programmed functions by dynamic adaptation to a person's actual behaviour. This can potentially increase the efficiency of the system by pre-empting user actions based on habitual patterns of behaviour. One argument for the adoption of such systems is that savings can be considerable, for instance, [Davidsson 98] estimates up to 40% of energy consumption in the home could be saved by the use of this technology. Advances in microelectronics and network technology are resulting in ever cheaper and more functional appliances being developed. Cheap and compact microelectronics means non-electronic artefacts e.g. shoes, cups, chairs, floors, beds, clothing fibres, paint pigments etc. are now potential targets of embedded-computers or stand-alone sensors. In addition, such systems can be implanted into our own bodies [Warwick 05].

Story #2 – Small Issues: *Mala felt as if she was being observed, which she was, but she knew about that as she had subscribed to a medical monitoring service with her local medical practitioner. As part of this new service, she had been put on a course of agentX “programmable” pills funded by her health care policy a few weeks ago. AgentX pills were the ultimate in silicon designer pills; they were in fact nano-scale agents that were injected into the body to repair problems (in her case to seek and destroy fatty deposits clogging her arteries). The much advertised advantage was that the agents provided feedback on what they found, and could either reprogram themselves, or be reprogrammed by specialists remotely. Avoiding an operation was something Mala liked. What she didn't know was that the agents also recorded other, wider, biological data from within her body primarily aimed at providing better analysis to improve the treatment she was receiving, together with helping the scientist improve their technique. This was all perfectly legal as the small print of the agreement, which Mala hadn't read, detailed such possibilities. Unfortunately for Mala this wasn't the end of it as during the period she was on the course of agentX pill, the agents recorded she ignored the strict regime the doctors had spelt out for her and she was thus required to pay for the treatment herself because of her flagrant abuse of the contract.*

Indeed, there is no technical or medical reason why, as domestic animals increasingly are, we could not be ‘chipped’ at birth with a unique identity that could be used throughout our lives. At this moment, it is not clear that the advantages of this sort of ‘tagging’ outweigh the potential disadvantages and, in any case, for many this is clearly also the stuff of nightmares and needs to be discussed widely.

The major advantage in networked environments is that appliances can collaborate to produce meta-functions (virtual appliances) formed by communities of co-ordinating devices (or services). One key question for individuals and society is how these systems are to be programmed and by whom? Fixed programming by a manufacturer, delivering limited functionality could be used, as in automation and similar systems. A more flexible approach is to employ intelligent agents to self-program the system autonomously with only implicit involvement from the user. Alternatively, people could be intimately and explicitly involved in the programming of collectives of devices, which they may also have defined themselves. These alternative approaches are hotly debated issues amongst some researchers with passionate views held on all sides and we now, briefly, discuss some of these issues.

When setting up and programming any computer system end-users are faced with a significant cognitive load as they seek to understand and configure the system appropriately. The underlying principle for the use of embedded intelligent agents is to transfer some of this cognitive loading from people into computers, freeing the user from the need to understand the technology. Such systems work by sensing the user as he goes about his everyday routine in the house, and learning from this behaviour so as to enable the ubiquitous system to perform in the manner the user seems to require [Mozer 98].

Whilst autonomous agents may appeal to many people, their acceptance is not universal. Some people distrust autonomous agents and prefer to exercise direct control over what is being learnt about them, when it is learnt and where that information is communicated. The alternative, a person-centred approach, is supported by the argument that it encourages people's creativity by allowing them to become designers of their own systems. People-centric approaches of this type are being developed to enable people to direct the operation of ubiquitous computers in a way that gives them full control, but avoid the need for them to have technical knowledge of the systems or programming. One recent example of explicit end-user control and programming is the UK DTI funded PHEN (Pervasive Home Environment Networking) research consortium's user interaction paradigm called Pervasive Interactive Programming (PiP) which puts the *user at the centre of the system programming experience* by exchanging autonomous learning for *explicit user-driven supervision* [Limb 05]. In this approach, a user defines a community of coordinating ubiquitous devices and the system learns usage rules and coordinating actions for groups of ubiquitous devices by using a "show me by example" approach. This enables people to create an electronic space built from a variety of network ready computer-based appliances such as TVs, DVD players, cookers, washing machines and mobile phones etc. However, the model goes further than simply connecting existing appliances as PiP uses the notion of decomposition of appliances into basic functionalities, which users can recombine, to form soft, or virtual, appliances. A key aspect of this new end-user empowerment is that lay-users have the power to associate together devices (and functions) in both familiar and novel arrangements to make highly personalised systems. A significant aspect of this paradigm is that it allows the coordination of numerous devices to provide new "meta appliances / applications" or virtual appliances so the lay-user can create novel meta functions that were not foreseen by individual appliance manufacturers. In short, lay-users become the designers of the potentially unique functionality of their own home systems. This work transfers the focus of design from the manufacturer to the end-user, a paradigm that aims to empower the lay-user, and challenges the nature of current appliances, all of which might contribute towards profound changes in social activity in the home and workplace [Chin 06].

2.2 Intelligent Buildings - Commercial Environments

Whilst the workplace has many features in common with the home such as heating, lighting, communication and computing systems, the variety and types of device are greatly different, as are the behaviours of the users. The typical worker is not the principal stakeholders of his environment in that he does not own the environment, nor is he master of his own time; rather he is often following a highly structured daily routine designed and supervised by other people. This managerial (and supervisory) style of life leads to the natural inclination for the stakeholders to utilise pervasive technology in a very different way to a domestic home. For instance, the manager or owner of a business may be more interested in the amount and quality of his employees work than their being allowed to design novel arrangements of appliances to entertain themselves. A manager might be interested in the employees' time keeping, or whether there is misuse of resources such as surfing the internet for private ends [Ball 01]. Similarly, he may be interested in employing technology to make working practices more efficient, or perhaps rewarding employees based on their ability to rapidly complete certain tasks. Such practices are already common as many employers monitor e-mail, telephone calls or breaks. Pervasive computing enhances the employers ability to monitor employees as it brings cheaper, more numerous and more varied sensors with more intelligent capabilities. For example, embedded agent techniques could be used to learn and characterise habitual patterns of behaviour thus allowing one employee to be compared to another, and to detect and flag "abnormal" behaviour by comparison to a template or ideal, whilst conventional networking technology gives the employer the ability to have a virtual presence with the employee, whenever he chooses.

Story #3 - Agents Encoding Human Behaviour: Li-Wong had been voted top CEO for the fifth year in succession. Investors queued up to buy shares in the many companies she ran as her companies were widely acknowledged as being the most productive operations in the world. The press had long debated how an engineer with little previous business experience, had been able to take over companies in which employees were not particularly productive, and through a process of matching pay to employees performance increased productivity dramatically, well above that of their competitors. In response to press questions about how Li-Wong achieved such high productivity levels she simply replied; "I invest in my workforce by giving them the most advanced intelligent buildings available that tend to their every need, they repay me with record levels of productivity". Tucked away in her executive office Li-Wong read reports of how other employers had tried to emulate her achievements by investing in high-tech buildings but had failed to achieve comparable levels of success. She couldn't help smiling to herself as she mused; "they all think I invest in the technology to make my employees more comfortable, of course that is a bonus, but the key to my success is that agents capture and analyse my employee behaviours, which gives me invaluable information on who to reward!"

Whilst it can be argued that an employer is acting within his rights by using this technology to make the supervision of his staff more efficient and less costly, it clearly has the potential to appear as extremely threatening to employees as few people like to have someone standing over their shoulder as they work. In addition, in some jobs initiative and independence, encouraging responsiveness and flexibility, are valuable human characteristics, which such close monitoring might undermine. It would seem that for employees to accept such monitoring then the technology has to appear not just beneficial to the manager, but also to the employee, and not be used as a tool to enforce a rigid working ethic but rather to support and reward employee creativity or make their job less of a chore in other ways. Some legislative regimes employ the principle of 'reciprocity' in which, what

the manager can see, is made available to the employees and even the management may be subject to monitoring. Lyons' makes an interesting point that technology that seeks to enforce working practices according to well-defined rules, is equivalent to the "work-to-rule" weapon that employees have traditionally used against employers. Thus, he argues it would seem counter productive for employers to turn this "weapon" on themselves [Lyons 02],

3.0 Social Implications

3.1 Introduction

Although scientists and engineers direct their effort at making this technology 'helpful and enabling', the fact that this technology senses and communicates behaviour clearly mean it could be used to develop and sustain a surveillance society. Without careful planning and regulation to control the systems and software of the pervasive computing environments of the future we could be creating a modern equivalent of Bentham's Panopticon [Panopticon] with some variety of "Big Brother" [Orwell 49] being able to monitor our every move and find out about all of our personal preferences. Over the years much has been written about such dangers [Lace 05] [Lyon 03] [Rule 73] [Burnham 83] [Marx 85] [Gandy 89 & 93] [McGrath 04] [Regan 05]. [Raab 05]. It would seem that we are caught in the paradox that in order to be useful the system has to know, but once it knows others can know too i.e., there is a direct threat to our privacy. However, the developmental trajectory of these systems is towards greater and greater distribution and local autonomy of both knowledge and activity – so technically the model is a highly distributed form of control. These systems are intrinsically anti-hierarchical in their design and operation and as such, they might well present greater and greater difficulties for any centralised monitoring and control. They might thus provide a metaphor or guiding model for a political reality in which control is more widely distributed.

Story #4 - The Value of Privacy: Ama, Bubba and Collo live in a gated community on the island of Java. This purpose built complex for wealthy participants in the knowledge culture provides them with all of the comforts of a wealthy lifestyle and none of the drawbacks. The independent state of Java has a number of such communities and each offers highly secure environments in several senses. Java's citizens have benefited greatly from the development of these super-wired communities so the level of local resentment is at a minimum and Java has negotiated a completely surveillance free relationship to the rest of the 'noosphere' – the virtual world that is the dominant economic feature of the global economy. Amma works on developing augmented and virtual reality training programmes for space shuttle staff taking holidaymakers to the space hotels that are an increasing feature of the travel industry. Bubba trades in ontology futures, the building blocks of the wired world while Collo gets the very best of education via online mixed reality systems and can play freely and safely with the other kids in Java-7's spacious, secure and superbly appointed grounds.

3.2 Citizenship and Pervasive Computing

Knowledge is power, and the level of distribution or centralisation of those exercising control over pervasive systems may be key to the development of political systems (and vice-versa). Thus, for example, the sort of technology that has so far been described opens up the possibility of the plebiscite as a major form within the democratic process. This puts

the education and development of responsible individuals at a premium. This opens up the possibility that the preferences of the population as a whole could become more visible to the population as a whole, with this technology acting as a form of real-time market research. For example, managing a home is in many ways analogous to the process of government. There are finite resources with much competition for them. Opinions and information needs to be gathered, deliberated on, policies formed and actions taken (c.f. a micro government). These “micro-government” choices, if gathered from enough homes and communicated to government, could provide important input to deliberation and policy formation. Thus, government rather than confining itself to indirect implicit data based upon, market research of one sort or another could use the power of pervasive computing to enable the population to give implicit feedback to government directly based on their routine as they go about their normal daily routines. Whilst there are benefits to the citizen and government there are clearly risks which put the education of the population at a premium

Story #5 - The Politics of Information: Nicole lived on the beautiful island of Cazeco, just off the Australian coast. She owned the latest Eco-Home which, boasted the use of exceptional insulation, energy minimising intelligent networked agents and renewable-energy generators on the roof. Nicole had numerous choices of when and how to use energy. The weather conditions, when and how appliances were used, hugely influenced her energy costs. Surplus electricity could be returned to the grid (or drawn from it when there was a shortage). Nicole admired greatly the Cazeco government whose enlightened environmental policy had funded the installation of the networked eco-technology in all homes. This policy had, proved so popular that since installing the equipment some 20 years earlier, the government had never lost power, being re-elected on 5 successive occasions. Asked about the secret of his record breaking re-election success, the president of Cazeco said that the secret was simply “listening to the people” (however, he couldn’t suppress a smile as he thought to himself “technology enabled listening, of course; what a wise government investment in technology that was!”)

3.3 Privacy and Security

In general, strong security measures are necessary because in a society where computer hacking and spam are such a widespread nuisance and danger to the continued development of such systems there is a need to be able to guarantee levels of privacy and security for this technology to be accepted and effective. One major security problem since all these systems will be dependent upon electrical power of some sort is the failsafe setting for the systems should there be a widespread power outage. Another issue is that agents, like people, can suffer from problems such as instability and require mechanisms to lock some functions to break or avoid deadlock and looping [Zamudio 07]. Clearly, the desired failsafe would be the return to whatever normal mechanical operation was in place before the pervasive computing system was installed. Otherwise, people could become trapped in their own homes and unable to get out. However, this also goes to illustrate that in the future the importance of infrastructural provision of power will be at a premium and reinforces the notion of the interconnectedness of all these systems. Technology is not just limited to systems we can physically see, but also those physically so small they are invisible to the human eye - nano technology. Whilst there are persuasive arguments in favour of direct human control of ubiquitous computing technology, there clearly are areas of it, such as this, where it is both necessary and beneficial to deploy autonomous agents. This leads to the

hybrid notion of “adjustable autonomy”, where individuals are able to tailor the balance of human versus agent control to suit their particular situation.

The opportunities for commercial and governmental interests to underwrite security would also potentially open up these systems to data mining for these vested interests so there is little doubt that security will be a number one priority if privacy is to be achieved, and the technology is to be accepted by society [Danna 02].

3.4 Consumers – A Growing Reaction

Whilst the issues surrounding the deployment of ubiquitous networked computing technology in our homes and offices are not widely debated, there are useful indicators of usage governments are likely to want to make of data. For instance car number plate data and mobile phone records are routinely stored and made available to government agencies, such as the police [McCue 06]. Internet search engine companies have been asked to hand over data on individuals search patterns [Mohammed 06]. Loyalty cards for large stores can be seen as a threat to privacy by some people resulting in the start of a campaigns to increase public awareness and encourage debate in the form of websites such as “Consumers Against Supermarket Privacy Invasion and Numbering” [CASPIAN 07]. Somewhat closer to the technology discussed in this paper are Radio Frequency Identification Tags (RFID); small electronic packages that can be added to products and people to transmit information on location. From a business perspective, they provide a more efficient method of providing bar-code data, already on products but in the mind of some consumers they represent a threat to our privacy and liberty, driving them to set up organisations, such as “NoTags” to raise public awareness of these issues [NoTags 07]. Such fears are well articulated by NoTags founder, Chris McDermott, who is quoted on their website as saying *“Do we really want a world where you can be identified from the clothes you wear, or tracked because there is a tiny chip inserted into your credit card or bank note? Can we trust the people holding this information to act properly and responsibly? The time is right for a serious debate to begin in the UK about how far we are prepared to let this technology invade our lives.”* There are similar movements in other parts of the world such as “RFID 1984” [Spychips 07] and Privacy International, a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations [PI 07]. Care environments are one of the better accepted areas where tags can be useful, for example, as a means of alerting carers to situations where people with memory problems may wander off and get lost [VeriChip 07]; but even here there are cautionary voices [Beresford 05]. All these growing movements serve to illustrate that the public not only consider the benefits of new technology, but have understandable concerns about their privacy and liberty. A key to ensuring the proper needs of society (both from an individual and government perspective) is understanding and participation. False fears can grow with ignorance, whilst ignorance can allow misuse; thus educating society and encouraging the participation of people at all levels is a key to the successful commercial deployment of pervasive computing, particularly in private areas such as our homes.

4.0 Regulation of Intelligent Buildings and Environments

If we are to live in intelligent buildings and environments, then questions like “who has control?”, “what is the extent of their control?”, “who has access to sensory data from our home and what use are they making of it?” are paramount. In short, how are people going to

be protected from the potential ravages of commercial or governmental powers based upon the exploitation of this technology? Whatever the 'official' answers to these questions, how can lay-people be sure that any assurances they are given on access and use of data gathered in the home is being complied with, and that there is no misuse by government, multi-nationals, commercial or subversive organisations, individuals or perverts?

Undoubtedly, the highly specialised and technical nature of ubiquitous computing makes it hard for individuals to understand the entirety of the vulnerabilities they face, and makes it difficult for them to have confidence in any technical tools that are supposed to protect their privacy. Whilst government legislation and self-regulating computers might go part of the way to providing assurance to an individual, the ultimate assurance to any individual relies upon their understanding of the issues, and the provision of tools they can understand, use and trust to protect themselves.

***Story #6 – A Question of Balance:** In Europe the take up of ambient intelligence was much slower than in the developing world. There was a built-in inertia in terms of the existing investment in technology, which the developing countries did not have. They had no need to consider the cost of replacing a technology they had already invested heavily in since they were leaping from a mainly pre-industrial to an advanced industrial technical civilisation within a generation. Furthermore, the complex legal and cultural traditions of Europe, developed over millennia, were proving to be an impediment to the development of ambient intelligence technology and the European Court of Human Rights was bogged down in a backlog of sensitive cases on the issue of privacy. Old-fashioned ideas about privacy and ownership and 'civilised' values were acting as a brake on the full development of some new technologies within Europe. By the end of the first quarter of the 21st century, the really dynamic economies were all in Africa and Asia. With their massive built-in markets, they had no need for 'the West' and without the encumbrance of a deeply established technical infrastructure, they were free to take up the intelligent environment vision enthusiastically. Not being burdened by the 'advanced' notions of individuality that were also symptomatic of 'the West' these cultures had less internal opposition to, and paranoia about, a technology that asked little but gave much. It was the community, not the individual that was the fundamental unit within these cultures.*

In our view, there is much work to be done in educating the population on the issues relating to intelligent-building and smart environment technology and even more work to be done to provide trustworthy and transparent tools for the user. We suggest that the scientists who are busy developing this new technology should put some effort into developing such tools, as without trust by the general public, the full market potential of such technologies will not be realised. Thus, it is in the best interest of companies seeking to build these market places to address these concerns by funding work on all aspects of the issues that give rise to public concern about the dangers of pervasive computing and intelligent buildings.

4.1 Beyond Asimov's Laws

One way that individuals might be given more trust in ubiquitous computing technology, and more specifically autonomous agents, would be if they had explicit built-in rules which reflected the individuals values and needs. Isaac Asimov explicitly addressed this problem in his "I Robot" series [Asimov 68] where he proposed a set of three rules designed to protect humans from the robotic technology they created. These rules can be summarized as "1) Protect Humans, 2) Obey Humans and 3) Protect Yourself". Although not without flaws

these have since become widely accepted within mainstream science as providing a well-founded moral framework for a society of robots and humans [Clark 93]. What should the equivalent laws for ubiquitous computing be, given that this involves a more intimate relationship between the individual and machine world? Would Asimov's Laws of Robotics suffice for ubiquitous computing controlled environments and vehicles?

We have argued that ubiquitous computing controlled buildings (Intelligent-Buildings) can be regarded as robots we live inside [Callaghan 00]. From this, one may draw a parallel between a robot and a system of ubiquitous computing devices. The particular nature of ubiquitous computing supported buildings is that they are often expensive and multi-occupant dwellings. This raises moral issues such as the rights of individuals as opposed to a society of occupants or indeed an owner. For instance, should an individual member of a shared urban dwelling be allowed to take an action such as reducing the temperature below freezing point, which may have some benefit to him, but severely damages the building or puts a company and all its human dependents out of business? Clearly the relationship between a person, a dependent community of people, an intelligent building or a robot is of a different order, the former being *self-reflexive* rather than hierarchical or separable in simple terms. This raises many difficult issues that are not explicitly addressed by Asimov's Laws of Robotics.

Asimov's Laws refer to an ideal world where machines have the ability to interpret and execute such rules or laws. However, this is clearly impossible as present - machines (or pervasive computing devices) are simply not advanced enough. For instance, they cannot adequately mediate differences of opinion amongst occupants, or make judgments on flimsy evidence part-human, part physical science. Such judgments are difficult enough for us and would necessitate highly advanced knowledge and artificial intelligence techniques not currently available and as a last resort recourse to the law. However, whilst engineers do not have sufficiently sophisticated technology to fully implement Asimov's Laws, each time they build an agent they implicitly implement a set of rules that determine its operation and these can be explicitly compared with these Laws.

The ubiquitous computing systems we are developing at Essex University are rule-based systems [Callaghan 04], [Hagras 04]. We are also looking at how these systems can detect the emotional state of the user and include that in the decision making process (e.g. react differently, depending on the occupant's mood) which further complicate the boundaries between people and machines [Leon 07]. In all these systems, there are rules implicit in the design that are the equivalent of Asimov's laws. Looking at our current work in this light we can derive the following set of Essex based intelligent building technology rules:

1. *Do not violate any safety constraints set by law or the manufacturer*
2. *Do not violate any privacy constraints set by user of the environment or community (providing safety constraints are not violated)*
3. *Accept instructions (including configuration and training) immediately from the stakeholders of the environment) (providing safety and privacy constraints are not violated)*
4. *Preserve the pervasive community (providing all the above are not been violated)*

The first rule is aimed at ensuring user safety is paramount. Rule two aims at ensuring that access to the system is safeguarded to adhere rigidly to the user's wishes. The third rule aims at allowing the user to particularise the ubiquitous environment to satisfy his individual need. Commonly this is undertaken in a teaching or learning mode. The forth rule aims at

making the ubiquitous system as robust and reliable as possible. For example if a member device fails, the community of devices immediately seeks to find a replacement device, and thereby maintain the operation of the overall system. Far from regarding these as ideal long term laws, we see them as a short term pragmatic approach to allow us to build ubiquitous computing environments from today's technologies whilst we are awaiting the arrival of more advanced processes and better established 'laws' based in widespread use.

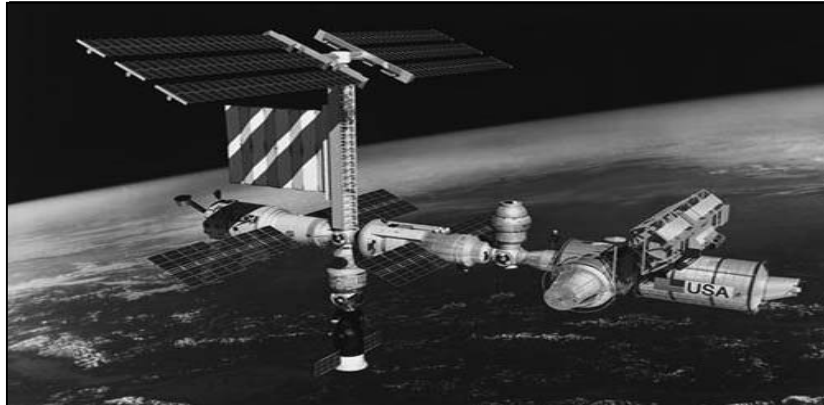
5.0 Government Regulation

What then are the issues for today's society and lawmakers to consider? Clearly, unless society takes a hand in framing such laws it will be left to small vested interest groups and commercial companies to construct rules to their own ends. Thus, at a minimum, such issues should be widely known and debated within society. Such a discussion would be interesting as investors may argue that any fundamental rules for machines should reflect the need to protect them (as investors, as companies etc) whilst individuals and various social political groups would surely make very different arguments. In this respect reports from the European Parliament Technology Assessment unit [EPTA 2006] and the UK Information Commissioner's Office [ICO 2006] are particularly useful as they seek to promote debate on how society should balance the convenience that new technology affords with the need to preserve privacy.

It is possible in the future, that much of the Health and Safety legislation will be actively embodied within the bounds of allowable operations of building control systems rather than sitting in a statute books gathering dust. If there is no regulation then there are immense dangers that various groups with their own agendas will misuse the technology. Companies might seek to gather information on people's behaviours to enhance their products, or to sell the data to third parties to mitigate the costs of their services (and increase their profits), and government agencies might gather evidence of fraudulent tax or disability claims etc. It is also possible that extremist organisations, or governments, could use the technology to develop terrorism or create a police state. The opportunities for misuse of this technology are almost endless. Experiences with the internet and mobile phones have revealed that there are additional problems. The distributed and international nature of the services and providers means it is difficult to frame laws that work as the violators may be operating out of other countries or using network connections where there are different laws, which makes it almost impossible to enforce local laws. In this respect, as with climate change, international organisations such as the UN would seem better placed to frame and oversee such legislation. The development of global institutions run under the auspices of the UN may turn out to be the only alternative to the potential chaos of individual states and corporations finding loopholes in national laws. Internationally agreed standards and compliance with such standards will however be a fundamental aspect of the successful development of this technology.

6.0 Future Intelligent Buildings

As we move into the longer-term future, we will become even more dependent on technologically supported environments. For example, if humankind ventures outwards, towards habitation of other planets, people will need to live in permanent space stations, planetary colonies or in spacecraft engaged on inter-planetary journeys. In these, the social and other constraints are simplified as the absolute dependency upon each other and the local environment is highlighted.



Technology View #3 *The International space station is the forerunner of mankind's ambition to inhabit deep space*

We are all of course dependent, to some degree or another, upon others in our daily lives and many of us experience the pleasures and support of working within relatively close functional communities, many of which overlap e.g. family and work communities. With the space colony, in some form or another, we will be moving into an experimental community of an entirely different order of magnitude in that it will need to be reliably autonomous and self-governing at all the levels of critical safety, although individuals will probably still retain a strong desire to personalise aspects of their habitat. Functional authority rather than rigid hierarchy, a sense of community that is both practical and durable, a means of resolving conflict and reaching agreement without schism and so on are going to be of the highest priority in off-earth urban habitat. This interdependence and local autonomy are qualities that will be shared by both the social and the technological organisation of the community. The need to be able to see things for what they are and not transfer deep pathologies into space with us means that the selection of personnel and their continual support within the communal practice of the vessel, colony or space station will need to be addressed. Although, currently, space habitation is managed by clear lines of hierarchical control, for the longer term the metaphor of a community of distributed co-operating ubiquitous devices and agents, without any obvious hierarchy is precisely the sort of model that these new and demanding circumstances might require. Space is an interesting example where inhabitants of an urban planetary habitat might realise that mutual dependence, tolerance and respect is much more likely to engender a robust and flexible community separated, as they will be from immediate help from Earth and dependent upon their own communal resources for survival [Clarke 00]. It is certainly true that the exploration of space will require us to look at ourselves and the ways in which we can work together in groups to achieve our common aims. We will be required to do this in a way that has rarely been asked of us before and with a range of tools and theories as to the social nature of human beings that are still being developed. This might enable us not just go to other planets and found new colonies but in a genuine sense, to found new societies.

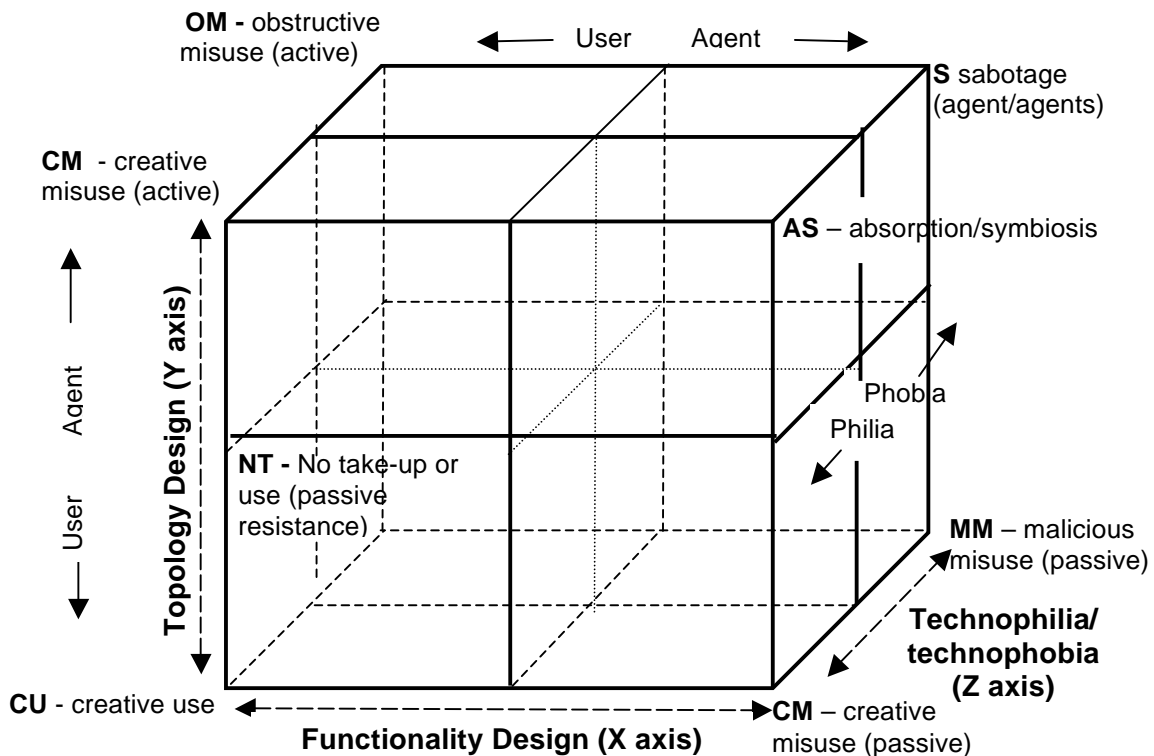
Story #7 - : The Final Frontier: *Xavier works as a porter in the first of the orbiting hotels – the Space Hilton. He works for three weeks on with relatively short periods off during any one day – if you aren't on holiday space can be very boring. He then has a weeks 'shore' leave when he comes back to his hometown of San Diego. Here he lives in one of the greatest conurbations of predominantly Hispanic peoples known to man - Los Angeles Mayor. Since the rich started to withdraw from normal urban life these areas have become even more dangerous than they used to be fuelled as they are by drugs and local rivalries in a megalopolis of over 200 million people – a loose confederation of thousands of gangs and small time crooks who have some purchase in their own areas but little power or influence outside of that. Hi-tech surveillance of these communities is at a minimum though they are savagely policed by a heavily armed militia style police with hi-tech equipment. Attempts to have all citizens tagged earlier on in the century failed so only people like Xavier who work in prestigious areas of great delicacy are visible to the constant sweep of the detectors over the dark and threatening city/state. Xavier doesn't*

7.0 A Socio-Technical Framework for Intelligent Building Research

In an attempt to find a way of approaching the problem of human interaction with pervasive computing technology for intelligent buildings and environments, there is a need to find a way of categorising the main technology and social drivers.

At Essex we have a multi-disciplinary socio-technical research centre, the Digital Lifestyles Centre, that is involved in developing and evaluating technologies that span a range of approaches from the exclusive use of intelligent autonomous agents, to user-controlled approaches. There are at least two dimensions to each of these systems, one concerning the functionality of the system and the way it is derived e.g. programs, rules derived from user behaviour etc., the other concerning the topology of the system, its components and the way they are networked together. Now in both cases there are examples controlled by intelligent agents, or determined by a user, or some combination of each. We used these two characteristics as the axes of an initial system to characterise our research in its widest sense and found an interesting spread across this space where the functionality is represented by the X-axis and varies between being totally controlled by a user to being totally controlled by an agent, and where the topology of the systems is represented by the Y-axis and varies from being totally defined by the user to being totally determined by an intelligent agent. Therefore at one extreme you would have a system where a user determines both the functionality and the topology explicitly and at the other extreme you would have a system whose functionality and topology were totally controlled by intelligent agents. This forms the basis of our figure 1. When it comes to human responses to these different systems, we have chosen a relatively simple measure, which we commonly observe in the behaviour of people as they approach these systems. This dimension we have called technophilia/technophobia which forms the Z-axis of figure 1. We are particularly interested in how these intelligent environment systems might stimulate or constrain human creativity and the consequences that might flow from this. Technophobia may, for example, arise from a fear of loss of privacy and control. We have represented these possibilities in a three dimensional graph, see figure 1, that we offer as a preliminary framework to spur discussions and help orient research concerning the ways that people and pervasive computing technology might interact in the digital home and workplace environments. The X-Y plane shows the possibilities for control (functionality) and configuration (topology) from automatic to manual. The Z-Y plane shows user reaction (phobia versus philia) to these different possibilities. The eight vertices represent potentially significant but extreme positions within the space defined by the cube concerning the relations of people and

Ubiquitous Computing. A general assumption underpinning this model is the view that the less understanding of, and control over, their environment that people have the more resistant or fearful they will be of it and vice versa. In this model, the vertices reflect extreme possibilities with all other combinations of response occupying the space between. The model is not normative but depicts a conceptual space of possibilities drawn from experiences with our technological work, which we have produced to generate and promote discussion between social scientists and technologists about this difficult area.



Technophilia – all forms of play to some degree
Technophobia – all forms of rejection to some degree.

The technophile/phobe continuum is dynamic, i.e. changing with time AND with different technologies

Figure 1 – A Socio-Technical Framework for Intelligent Building Research

In the following table we characterise the extremes which this model allows us to capture:

Vertice Property	Description
OM - obstructive misuse	The agent sets the topology but the user is able to programme the functionality. The technophobic person's response is to use the technology against itself, to find ways of disrupting or obstructing the system
S - sabotage	Agents are autonomously setting the topology and functionality. The technophobic person has no power at all to intervene in the working of the systems and so resorts to sabotage.
NT - No take-up or use	The user is empowered to set the topology and functionality; The technophobic person wants nothing to do with the technology.
MM – malicious misuse	Agents are autonomously setting the functionality but the user has control over the topology; The technophobic person will use the area they have control over to interrupt or interfere with the overall functioning of the system.
CU - creative use	The user is able to set both the topology and functionality; The technophile person enthusiastically uses the system to enhance their lives and what they perceive to be the attractiveness and interest of their environment.
AS – absorption	Agents set the topology and functionality;

/symbiosis	The technophile person loves the technology so much that they become immersed in it totally.
CM - creative misuse (two instances)	Agents set either the topology or functionality (but not both); The technophile person can intervene at the level of topology or functionality (depending upon the system) and uses whatever aspects they can to generate the functionality/topology they want.

Table 1 – Description of the Socio-Technical Framework Model

8.0 Concluding Discussion

In this paper we have discussed how embedded intelligent agents might contribute to future directions of intelligent buildings and smart environments together with raising social consequences of their use. Currently there is an increasing level of debate on ethical issues such as privacy in ICT, particularly with respect to technologies such as identity and loyalty cards, data mining, internet search engines and RFID tags. As computer scientists actively researching the technologies involved, we have sought to extend this discussion into the area of intelligent buildings and smart environments. We have described how intelligence can be created using embedded-agents and how the main research on intelligent-agents can be categorised as belonging to two underlying approaches; implicit programming (intelligent autonomous agents) and explicit programming (end-user programming). We have shown how these possibilities can be represented using a 2D space bounded by the degree to which intelligent agents or people are in control of both the functionality (X-axis) and the topology (Y-axis) of these systems. By introducing another axis (Z-axis) to indicate the degree to which the person involved is comfortable with this technology and the part they play in it (technophilia/technophobia) we have developed a framework for categorising and visualising these issues using a three dimensional diagram of possibilities where the vertices represent particular extremes. Based on our experience we speculate that combinations of these approaches engender a variety of emotional responses that will be important factors in the success or failure of these technologies. Whilst the focus and success of our own research is firmly in the technological developments, we have found ourselves dealing with questions that concern the ethics of specific aspects of Intelligent Buildings and smart environments together with its potential for being turned from a beneficial technology for both the individual and society into its opposite. Clearly this is a complex matter that is dependent on individual attitudes, governments and cultures, but also upon the level of understanding and agreement of the issues involved at all levels of society. As technology advances, it opens up new and exciting possibilities for intelligent buildings whilst simultaneously raising ethical dilemmas which need to be confronted if intelligent buildings are to reach their full potential. These issues are also critical for all those pursuing ambient intelligence projects which entail the widespread deployment of intelligent agents

Acknowledgements:

We are grateful to our colleagues from Chimera (<http://www.essex.ac.uk/chimera/>) who acted as a “sounding board” for the socio-technical framework presented in section 7.0, in particular Michael Gardner, Chris Fowler, Debbie DiDuca, Joy Van Helvert and Anna Haywood

References

- [Asimov 68] Asimov I, “*I Robot*” Panther Books, September 1968
- [Ball 01] Ball, K. ‘*Situating workplace surveillance: ethics and computer based performance monitoring*’, *Ethics and Information Technology*, 3(3): p211-223, 2001.
- [Barbaro 06] Barbaro, A. and Zeller, T. ‘*A face is exposed for AOL*’, *New York Times*, 9 August 2006
- [Beresford 05] Beresford P “*Gadgets Don’t Care*”, *Community Care*, 18-24 August 2005
- [Bruno 02] Bruno L “*The mobile home of the 21st century*” *Red Herring*, 30 October 2002.

- [Burnham 83]** Burnham D *“The Rise of the Computer State”*, Vintage Books, New York, 1983
- [Callaghan 04]** Callaghan V, Clarke G, Colley M, Hagrais H Chin JSY, Doctor F *“Inhabited Intelligent Environments”*, BT Technology Journal , Vol.22, No.3 . Klywer Academic Publishers, Dordrecht, Netherlands, July 2004
- [Callaghan 00]** Callaghan V, Clarke G, Colley M, Hagrais H *“A Soft-Computing DAI Architecture for Intelligent Buildings”* Journal of Studies in Fuzziness and Soft Computing on Soft Computing Agents, Physica-Verlag-Springer, November 2000
- [Callaghan 06]** Callaghan V, Chin J, Zamudio V, Clarke G, Shahi A, Gardner M, *“Domestic Pervasive Information Systems: End-user Programming of Digital Homes”* Chapter 7 in Book Pervasive Information Systems published as part of Advances in Management Information Systems research monographs, ME Sharp Inc , New York, August 06
- [CASPIAN 07]** *“CASPIAN - Consumers Against Supermarket Privacy Invasion and Numbering”* [Cited February 2007 - Available from <http://www.nocards.org/>]
- [Chin 03]** Chin J, Callaghan V, *“Embedded-Internet Devices: A Means Of Realizing The Pervasive Computing Vision”*, IADIS International Conference, Algarve, Portugal, 5-8 November 2003.
- [Chin 06]** Chin, J.S.Y., Callaghan,Vic, Clarke,G., *‘An End User Tool for Customising Personal Spaces in Ubiquitous Environments’*, IEEE the 3rd International Conference on Ubiquitous Intelligence and Computing (UIC-06), 2006
- [Clark 93]** Clark, R. *“Asimov's Laws of Robotics”*, *IEEE Computer*, Dec 1993, p.53
- [Clarke 90]** Clarke, A.C. *“2001: a Space Odyssey”*, *Orbit*, 1990
- [Clarke 07]** Clarke G, Callaghan V *“Ubiquitous Computing, Informatisation, Urban Structures and Density”*, Built Environment, Volume 33, no 2 edited by Michael Cohen and Margarita Gutman, 2007
- [Clarke 00]** Clarke G, Callaghan V, Pounds-Cornish A *“Intelligent Habitats and The Future: The Interaction of People, Agents and Environmental Artefacts”*, 4S/EASST Conference on Technoscience, Citizenship and Culture in the 21st Century, Vienna, 26-28th September 2000
- [Danna 02]** Danna A, Gandy O. *‘All that glitters is not gold: Digging beneath the surface of data-mining’* Journal of Business Ethics, 40: 373-386, 2002
- [Davidsson 98]** Davidsson P *“Energy Saving and Value Added Services: Controlling Intelligent Buildings Using A Multi-Agent System Approach”* in *DA/DSM Europe DistribuTECH*, PennWell, 1998
- [DTI 07]**, The Next Wave Technologies and Markets programme”. [Cited February 2007] Available from <http://www.nextwave.org.uk/>
- [Ducatel 01]** K. Ducatel, M. Bogdanowicz, F. Scapolo, J. Leijten, J-C. Burgelman *“Scenarios for Ambient Intelligent in 2010”*. EU Information Systems Technology Advisory Group (ISTAG), IPTS-Seville, February 2001 (Available from www.cordis.lu/ist/istag.htm)
- [Economist 05]** *“The digital home; Science fiction?”*, The Economist, Thursday September 15th 2005
- [EPTA 06]** *“ICT and Privacy in Europe: Experiences from technology assessment of ICT and Privacy in seven different European countries”*, European Technology Assessment Unit, Final report October 16 2006
- [Gerstner 99]** Gerstner L, *“Presentation to Joint Economic Committee's first National Summit”* 1999
- [Gandy 89]** Gandy O *‘The surveillance society: information technology and bureaucratic social control’* *Journal of Communication*, 39:3, 1989
- [Gandy 93]** Gandy O *“The Panoptic Sort: A Political Economy of Personal Information”*, Boulder CO: Westview Press, 1993
- [Grayling 05]** Grayling A C, *“In Freedom’s Name: The Case Against Identity Cards”*, London: Liberty. 2005
- [Hagrais 04]** Hagrais H, Callaghan V, Colley M, Clarke G, Pounds-Cornish A, Duman H, *“Creating an Ambient-Intelligence Environment Using Embedded Agents”* IEEE Intelligent Systems, Vol. 19, Issue 6, pp. 12-20, November/December 2004
- [Hogan 03]** Hogan J *‘Smart software linked to CCTV can spot dubious behaviour’*, *New Scientist*, 11 July, 2003
- [Horan 05]** Horan B *“Use of Capability Descriptions in a Wireless Transducer Network,”* Sun Microsystems Research Labs, Report Number: TR-2005-131, Feb 1, 2005
- [ICO 06]** *“A Report on the Surveillance Society”*, UK Surveillance Studies Network, Information Commissioner’s Office (ICO) September 2006

- [**ITU 05**] *“The Internet of Things”*, International Telecommunications Union, 7th edition, ITU Publications, Geneva, 21 September 2005, ISBN 92-61-11291-9
- [**Kell 05**] Kell A. (2005) *The Global Development of Intelligent and Green Buildings*. Presentation to the Intelligent and Green Buildings Conference, Beijing. Available at <http://www.ibexcellence.org/resources.html>.
- [**Lace 05**] Lace S *“The Glass Consumer”*, Bristol UK: Policy Press, 2005
- [**Leon 07**] Leon E, Clarke G, Callaghan V, Sepulveda F, "A user-independent real-time emotion recognition system for software agents in domestic environments", *Engineering Applications of Artificial Intelligence*, Volume 20, Issue 3, Pages 337-345, 2007
- [**Limb 98**] Limb R, Armitage S, Chin J, Bull P, Kalawsky R, "User interaction in a shared information space – a pervasive environment for the home", *Perspectives in Pervasive Computing*, IEE, Savoy Place, London, 25th October 2005
- [**Lyon 03**] Lyon D *“Surveillance after September 11”*, Cambridge UK: Polity Press, 45-48, 2003
- [**Lyon 03**] Lyon D (ed.) *“Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination”*, London and New York: Routledge, 2003.
- [**Lyons 02**] Lyons M, *“Pervasive Computing: Control and Freedom in Cyberspace”*, 2002.
- [**Marx 85**] Marx G T *‘The surveillance society: the threat of 1984-style techniques’* *The Futurist*, June: 21-26; 1985
- [**McCue 06**] McCue A *“Police to store number plate camera data for two years”*, Silicon.com, Wednesday 18 January 2006
- [**McGrath 04**] McGrath J. *“Loving Big Brother”*, Routledge; London, 2004
- [**Mohammed 06**] Mohammed A *“Google Refuses Demand for Search Information”*, Washington Post (p A01), Friday, Jan 20, Metcalfe R, 12-14 March 2001 *“Keynote Presentation”*, ACM1 Conference, San Jose Convention Centre, California.
- [**Mozer 98**] Mozer MC, *“The Neural Network House: An Environment That Adapts To It’s Inhabitants”*. In *Proceedings of American Association for Artificial Intelligence Spring Symposium on Intelligent Environments*, pp. 110-114, AAAI Press, 1998
- [**Orwell 49**] Orwell G *“Nineteen Eighty-four”* Penguin Books, September 1949
- [**Raab 05**] Raab C, Bellamy C *‘Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part I’*. *Public Administration* 83 (1): 111-133, 2005
- [**Regan 05**] Regan P. *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill: University of North Carolina Press, 2005
- [**RFID 1984**] *“Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID”* [Cited February 2007] Available from <http://www.spychips.com/>
- [**Rule 73**] Rule J *“Private Lives, Public Surveillance”*, London: Allen Lane. . (1973) 2006
- [**VeriChip 07**] *“The total solution for wander prevention”*, [Cited February 2007] Available from <http://www.verichipcorp.com/content/solutions/roamalert>
- [**Warwick 00**] Warwick K, *“Cybernetic Organisms: Our Future?”*, *Proceedings IEEE*, Vol.87, No. 2, 387-387, February 1999
- [**Warwick 05**] Warwick, K, Gasson M N, Hutt B D, Goodhew I: *“An Attempt to Extend Human Sensory Capabilities by Means of Implant Technology”*, IEEE SMC, IEEE International Conference on Systems, Man and Cybernetics, Waikoloa, Hawaii, pp.1663-68, 10-12 October, 2005
- [**Zamudio 07**] Zamudio, V., Callaghan,V., *“Preventing Instability in Rule-Based Multi-agent Systems; A Challenge to the Ambient Intelligence Vision”*, First International Conference on New Technologies, Mobility and Security, Telecom Paris, France, (2007)