Risk Assessment and Management in Pervasive Computing:

Operational, Legal, Ethical, and Financial Perspectives

Varuna Godara
University of Western Sydney, Australia

Information Science REFERENCE

INFORMATION SCIENCE REFERENCE

Hershey · New York

Director of Editorial Content: Kristin Klinger
Director of Production: Jennifer Neidig
Managing Editor: Jamie Snavely
Assistant Managing Editor: Carole Coulson
Assistant Development Editor: Heather Probst
Typesetter: Chris Hrobak
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

and in the United Kingdom by
Information Science Reference (an imprint of IGI Global)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanbookstore.com

Library of Congress Cataloging-in-Publication Data

Risk assessment and management in pervasive computing : operational, legal, ethical, and financial perspectives / Varuna Godara, editor.

p. cm.

Includes bibliographical references and index.

Summary: "This book provides extensive information about pervasive computing, its implications from operational, legal and ethical perspective so that current and future pervasive service providers can make responsible decisions about where, when and how to use this technology"--Provided by publisher.

ISBN 978-1-60566-220-6 (hardcover) -- ISBN 978-1-60566-221-3 (ebook)

1. Ubiquitous computing--Handbooks, manuals, etc. 2. Mobile computing--Handbooks, manuals, etc. I. Godara, Varuna.

QA76.5915.R57 2008

004.165--dc22

2008023193

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter XIV
Ethical Issues and Pervasive Computing

Penny Duquenoy
Middlesex University, London, UK

Oliver K. Burmeister
Charles Sturt University, Wagga Wagga, Australia

ABSTRACT

There is a growing concern both publicly and professionally surrounding the implementation of Information and Communication Technologies (ICT) and their social and ethical impact. As these technologies become increasingly pervasive and less visible to the user, there is a greater need for professionals to address the concerns in order to regain public trust and maximise the benefits that these technologies can bring. This chapter explores the ethical aspects of the world of pervasive computing and shows the need for an ethical perspective when considering the design and implementation of complex, integrated, multiple systems. We present the background to ethics and technology to give the foundation for our discussion, and refer to current research and ethical principles to provide the argument for ethical consideration. Finally, codes of professional conduct provide the standards, and endorsement, for professional responsibility.

INTRODUCTION

It has become increasingly clear that Information and Communication Technologies (ICT) raise ethical issues. The volume of research presented at conferences dedicated to computer ethics[1], the numerous academic texts on computer ethics produced to aid in the education of computer science

undergraduates, and the formation of ethics groups within professional bodies[2] (internationally and nationally) give an indication of the amount of concern within the profession on this subject. In the research context the European Commission has several projects from the 6th Framework tackling these issues[3] and has increased the visibility of ethics and ICT in its 7th Framework Programme.

With the emergence of these technologies over the last 10 years or so their ethical impact has often only become evident following implementation, for example many people now have concerns regarding privacy as a result of massive data collection, and extended monitoring capabilities. However, as ICT increasingly pervades almost every aspect of daily life (hence the term 'pervasive computing') supporting not only industry but also the citizen population, the aspects of ethical impact have had a significant effect on public perception and uptake. As we have just noted, public discussions have largely centred on the issue of privacy in terms of individual private space, and personal data. As a consequence we have seen a greater emphasis on addressing this issue resulting in substantial developments to offer protection through security technologies and efforts to encourage public trust by involving the users in the management of their privacy (for example, privacy policies and customisation of their Internet settings).

It is recognised that public confidence is key to the successful implementation of new technologies in the public sphere, not least by professional bodies who have demonstrated their commitment for public welfare in their codes of ethics for some years[4]. More recently, we have seen increased attention to the incorporation of ethical considerations in technical development by research funding agencies and the United Nations[5]. Quite apart from the strategic benefits of public acceptance in respect of continued economic growth, professionals have an ethical imperative to consider the benefits and harms to society and individuals within society when planning the next technological development.

Pervasive computing is not so much a new technological development (as, for example, the mobile phone) but a term that describes the concept of computer technologies becoming embedded within the social infrastructure in such a way that their use becomes commonplace and often invisible – the use of computer technology in cars is a good example. Other terms that are used to describe this concept are 'ubiquitous computing' and 'ambient intelligence'. A recently published book resulting from one European Project that was charged with looking at forthcoming security issues announces (Wright et. al., 2008): "In the near future, every manufactured product – our clothes, money, appliances, the paint on our walls, the carpets on our floors, our cars – will be embedded with intelligence, networks of tiny sensors and actuators, which some have termed "smart dust" or an "Internet of Things". The world of ambient intelligence (AmI) is not far off. We already have surveillance systems, biometrics, personal communicators, machine learning and more. Ambient intelligence will provide personalised services − and know more about us − on a scale dwarfing anything hitherto available."

As we move forward to utilise this technology to support our lifestyles in a variety of different ways that include communication and information exchange between devices and between humans and the devices, it is important that designers, developers and most importantly those funding development are confident that their products will be accepted in the marketplace – that is, that the public is ready to 'adopt'. The testing and evaluation that has historically taken place in the development process for individual devices does not go far enough to ensure public acceptance of the convergence of many technologies and devices that enable interactions beyond the simple functionality and usability testing within a lab. Thus, one cannot engage in extensive studies of users. Instead, following the concept of the heuristic evaluation used in the field of Human Computer Interaction (HCI), expert evaluation of proposed

technologies is needed. We need to forecast the possible ways the technology might affect users, using scenarios to explain the context of application, and extrapolating from existing and proposed pervasive technologies. These are the methods we use in this chapter to explore the issues.

The aim this chapter is to show why the consideration of ethics in the development and deployment of these technologies is important in any risk analysis of future technologies, and the sorts of issues that have arisen and are likely to be a cause for concern in the future. To illustrate the reasons for concern we will explain the difficulties posed to ethical understanding by changing technological contexts, and present our discussion in a framework that can be adopted by others: understanding of context and technical characteristics, gaining ethical guidance from existing ethical principles, and reference to professional codes of conduct. Examples will be used throughout to explain contexts and illustrate ethical issues.

Although we will be drawing on examples to highlight ethical issues, our intention is not to devalue the contribution of computer technologies to public and private life, but to indicate the areas where ethical reflection should take place. Technology brings many positive benefits, and in many cases the choices and trade-offs between benefit and harm are not easy to make. For example, the use of technologies for monitoring the health of seniors to assist in independent living is a wholly worthy ambition. On the other hand, monitoring people is often seen as an invasion of privacy, the data collected may be misinterpreted, or used in a way that is not in the best interests of the person being monitored. Determining the 'good' based on a set of values is at the crux of ethics but how one determines those values and 'good for whom' is not straightforward.

To set the context of this chapter we begin the following section with a brief overview of ethics and give some examples of the benefits and harms that are apparent in the technologies in use today (expanding on the example of monitoring given above). We then give some detail on the characteristics of computer technology as it has evolved to show how the changes affect ethical values and why we need to consider ethics in its development and use. Having given a picture of ethics, technology, and the changing shape of our social sphere, we show how reference to ethical principles and professional codes of conduct can help in assessing impact and guide professional behaviour.

A BRIEF ETHICS OVERVIEW

This chapter looks at ethical issues in pervasive computing, so it is important to understand what is here meant by the term ethics. There are many good texts available on ethics, so beyond a brief explanation here, readers interested in ethics as an area of further reading are encouraged to see the suggested reading list at the end of this chapter.

Ethics is about directing people to consider the values of life. It addresses issues such as finding out which values are more important than others are. Ethics, traditionally associated with moral philosophy, concerns concepts such as personal integrity. Ethical theories are concerned with explaining human morality and providing people with guidance on how to conduct life. Philosophers who have contributed to the development of modern ethical thinking include Plato, Aristotle, Immanuel Kant and John Stuart Mill. There is no single approach to ethics. Kant for example founded his theory on a logical argument beginning from a premise of human rationality leading to universal rules. From this position, he could argue that certain actions could not be morally justified because it would not be logical for all to act in the same way – for example stealing, lying and breaking promises. For Kant, the 'will' (intention) was the driving force behind ethical action summarised by his categorical imperative[6]. This theory however allows no flexibility

according to contingent circumstances. A more recent, and popular, approach is to think in terms of consequences of actions – if the consequences bring good (whatever that may be deemed to be) then the action can be morally justified. Competing and at times complementary ethical theories include consequentialism, relativism, deontology, utility, and many others. Each takes a different philosophic stance. Few people are purists, instead we tend toward a little of one or another, our views can change over time, and we are all influenced by culture, religion and our peers. It is for this reason that many of the world's professional ICT societies stipulate that members should adhere to the professional ethical code of that society, thus ensuring that a common (normative) ethical standard applies to all ICT workers in that country.

Often debates in ethics arise when the stakeholders involved come at whatever the issue is, from differing philosophical viewpoints. A brief example showing Kant's 'intention' view versus a consequentialist view will illustrate this point. Say I have a friend in hospital and I bring her flowers to cheer her up. However, it turns out that she had an allergic reaction to the flowers and it prolonged her hospital stay by 2 days. (Assume I did not know she was allergic to these flowers.) According to an intention view, I acted ethically. However, the consequences of my action suggest I acted unethically (as the consequence did not bring good). There are flaws in these two theories (as is the case for most theories) on the one hand Kant's view is absolute and does not allow for flexibility, whereas the consequentialist view allows us to take into account the circumstances of a situation, but falls down because consequences cannot be accurately predicted (as our example has shown).

Putting ethics in the context of pervasive computing, what might be some of the issues? Examples are given below of positive (good) and negative (harm) issues, as well as others that might be deemed neutral or debatable.

Positive issues include such things as social responsibility toward disadvantaged members of our society. For instance, in medical technology pervasive computing is making many encouraging strides forward in helping monitor patients. Western governments around the world are faced with lower infant mortality and greater longevity, meaning that over time a smaller work force supports a larger ageing population. Given this prognosis, governments are looking for ways to decrease aged dependency on institutional care, by encouraging seniors to live at home longer. Pervasive technologies are already helping in this area, by monitoring seniors in their homes. The technology can monitor if medication was taken, and if a senior is in trouble. For the latter, a senior may experience a fall in their living room. Technology embedded in an intelligent armchair can monitor the senior rising from the chair, while smart flooring, integrated with other monitoring technology in the home, can register the fall. The result can be a report to nursing staff, who can then make an immediate house call. Other equipment can monitor if a senior has been too long in the toilet or in their bedroom, and send out a call for assistance.

Negative issues arise often in the context of positive issues that are abused. Other technologies can be invasive raising privacy and other ethical concerns. Returning to the monitoring of seniors above, there are pervasive technologies proposed for ingestion, to monitor internal organs – useful for patients receiving medical treatment, as well as for high performance athletes training for their events. An abuse of such technology could be when it is being used to monitor a senior, and a hereditary disease is discovered, as a result of which the children and grand-children of that senior find their health insurance premiums inflated significantly, or refused altogether.

Neutral or debatable ethical issues arise in situations where there are conflicting ethical principles, cultural distinctions, or legal matters that blur interpretation of events. At times, this also

involves the area of ethics known as professional ethics. It may be legal in some countries not to take the concerns of visually impaired customers into account, but when one has a professional obligation to the users of the technology one is producing, then a debate can arise whether or not to spend the extra time and money to cater to that category of user. In some countries, the professional society for ICT will have stipulations about professional conduct in such matters, and in other countries, there are no such professional obligations. One example of a debatable issue is the use of monitoring technology in motor vehicles. There have already been cases where new technologies in cars monitor driving habits, similar to the black box flight recorder in airplanes. In the case of an accident, crash investigators and insurance companies can find out the speed the vehicle was travelling and other vital data. While useful for resolving accident issues, it might also result in insurance cover being refused, because the data shows no seatbelt was worn at the time, or that the car was driven too quickly. This is a debatable issue in that some might argue that third parties such as insurance companies should be denied access to private data, while others argue that this is necessary to avoid false claims on insurance, which drive up insurance premiums for other insurance customers. Such debates often involve many stakeholders, with conflicting viewpoints. There is seldom a right or wrong approach, but a professional judgment can be made by an analysis of stakeholders set against ethical priorities and the extent of benefits and harms.

ETHICAL CONSIDERATIONS AND TECHNOLOGIES

It might be argued by some that with the experience of technological development gained so far we are now more informed on these issues, and are in a position to pre-empt many of situations that have caused some of the problems. However, the emergence of pervasive technology that will in many cases become invisible to the user raises a number of challenges in (a) the ability of those engaged in the development to predict the ethical impact of the convergence of the various technologies (such as mobile, wireless, radio frequency identification (RFID) chips, nano technologies etc.), and (b) the awareness of the user to what is happening and their inclusion in managing their "ethical risk" without the familiar interface (e.g. monitor, mobile phone etc.).

Thus, there is a need for an exploration of ethical aspects in this new context where risk may be increased through the diminishing visibility of the device and its function and the lack of public familiarity with the medium of information communication. Our short example of computers in cars shows the invisibility problem – we are used to computer aided diagnostic capabilities in cars and assume that the diagnoses will be correct, but are users aware of driver monitoring and its implications? For public confidence to be maintained, ICT professionals need to be seen to follow ethical guidelines in the use of these new technologies. The boundaries of public and private space are disappearing, and it is becoming urgent to assess the future use of embedded technologies. Where their use is intended for children or the elderly, or people who have impairments, it is particularly important to make sure they have been carefully thought through.

The realisation that the particular characteristics of computer technologies raise ethical concerns is not new, or particularly recent. As long ago as 1960 Norbert Wiener warned of the dangers implicit in machines that "acted" faster than we could react, and that had a complexity beyond our understanding (Wiener, 1960) and some years later, following the interest in artificial intelligence Joseph Weizenbaum was concerned about their context of application (Weizenbaum, 1976). However, it was in 1985 that the current field studying ethical issues and computers began in earnest and has largely been inspired by James

Moor's observations on why computers raise the issues they do. In his article Moor explains that computers raise ethical issues because of their social impact (increasing use in society), their logical malleability (they can be shaped to perform a number of operations), and their 'invisibility factor' (potential for invisible abuse, invisible programming and invisible complex calculations)[7]. All of the above reasons for concern are still relevant, but it is worth noting that invisibility is promoted as one of the key benefits of the new pervasive computing environment. However, this characteristic also has the potential for unwanted ethical consequences.

The technological environment described by terms such as 'pervasive' or 'ubiquitous' computing is one where computer technology becomes embedded in a variety of everyday objects with the aim of making life easier. A similar concept is described by the term 'ambient intelligence' (adopted by the European Union particularly in its Framework 6 research programme) which describes an environment where "people are surrounded by intelligent intuitive interfaces that are embedded in all kinds of objects and an environment that is capable of recognising and responding to the presence of different individuals in a seamless, unobtrusive and often invisible way." (Ducatel et. al., 2001, Preface.)

Whilst the vision of pervasive and ubiquitous computing is worthy and has highly desirable aims that are well worth pursuing, the concerns expressed above still apply. Moreover, the situation has scaled-up considerably since the days of Wiener, Weizenbaum and Moor. The influence of computer technology has spread, the capabilities of the technology have increased, and not only will the operations of the technology be invisible the devices in which the technology is embedded will merge into the background. So, while some might argue that things are no different because 'invisible is invisible' and that if complexity already gives cause for concern 'more' complexity does not exacerbate the situation, we would argue that the pervasive environment is different – the vision demands 'difference'. The social impact will increase (again, part of the vision in supporting lifestyles in new ways) and the users of the technology are unlikely to be familiar with the operations behind the technology – this can be seen as a benefit that reduces the inconvenience of traditional interfaces, but can also be detrimental to the user who is likely to be a 'novice' user and therefore unaware of the capabilities of the technical devices, and the potential for misuse. This makes them vulnerable to exploitation by, for example, the use of marketing, tracking, and monitoring technologies, as well as to more familiar threats such as fraud. All of the above give good reasons to ensure ethical considerations are at the forefront of discussions.

The Challenges of a New Technological Context

Many of the issues surrounding the use of ICT have been the subject of debate and discussion for many years (cf. Westin, 1967, on privacy). With each technological development we have seen an expansion in opportunities for the exchange of information between an ever increasing audience, some legitimate and others not. Along with these developments has been a catch-up game between regulators attempting to control the flow of information and those pursuing the 'freedom' offered by a global Internet.

As new technologies and uses of the technologies have changed and developed academic debates around ethics and technology have progressed from discussions around what the impacts are to how the ethical context may have changed[8]. There was a great deal of confusion in understanding the new digital environment, in appreciating the difference between an analogue and digital representation of the world, and difficulties in finding terms to capture a concept that was totally new – for example 'Cyberspace'[9].

What all of this interest and the resulting

discussions serve to demonstrate, is that diverse communities were operating in unfamiliar contexts – the technical community clearly had an understanding of the operational aspects but did not fully anticipate the effects of viruses or the opportunities for hacking. The new users were unaware of the underlying technical operations and were thus unprepared for viruses, and other less damaging but exploitative programs such as cookies[10]. Similarly, apparently inappropriate and unsociable behaviour was becoming evident within the new virtual communities and, because of the novel environment, was cause for investigation and discussion (cf. Turkle, 1995).

Today, having gone through this conceptual change and learning curve, we are in a better position to assess future impacts based on a more informed understanding of the technologies involved, their interactions and those of the users. We know, for instance, the limitations of security techniques, the capabilities of measuring, tracking, and monitoring actions, the changes in work and social practices that occur from introducing ICTs and that lack of access to these technologies results in social disadvantage (Moss, 2002; Buchanan, 1999).

The problem of security is already a significant issue. Security has an impact on privacy (of personal information and profiling of users) as well as other, usually financial, considerations. Privacy is arguably one of the most hotly debated topics today. The characteristics of computer technology – collecting, managing, interrogating and analysing large amounts of data – have resulted in applications that enable easy monitoring and tracking of activities, not just in using the Internet, but also in other activities (e.g. the use of CCTV cameras to monitor driving, the use of travel permits to track personal travel on public transport (the Oyster card in London, UK), 'loyalty' cards to gather information on buying habits), telephone calls, and the use of RFID tags to track people serving penalties for low-level criminal convictions.

The impact on social relationships has perhaps seen the biggest changes, utilising mobile technologies to send messages, photos, music, video, as well as the capability of constant communication from almost anywhere in the world through the written and spoken word. At the same time, this medium of communication has been misused to record unsuspecting people at inappropriate times, and in the worst cases to set up street fights to provide video material on the Internet. Being constantly available for work is another change that mobile computing has fostered, many employees find they are answering emails and their mobile phones for work during unsociable hours and even during their holiday period. In the same way, marketing companies use all of these means of communication (traditional telephone, mobile telephone, and email) to exploit sales, so invading the personal space of the buying public.

Whilst the above are cause for concern, this does not seem to put people off from taking part in the 'information society'. Therefore, the aspect of choice is seen as crucial, and for many the choice to take part is not an option. Accessibility to ICT is problematic for a number of individuals because of cost, the interface design, training in how to use it, and the availability of adequate access (technical infrastructure, service provision, government policy). There is also a problem from those not wishing to take part, or not realising what taking part means. A recent case reported in the UK was the issue of an RFID enabled card (issued by a bank) to enable small payments (transactions under £10) without the need for a PIN number or signature. The customer of the bank did not want this card, and disposed of it. However, when attempting to use his traditional bankcard to withdraw money from a cash machine, his attempt failed. "After calling [the bank] helpline, [the customer] was told that the (unsolicited) issue of the 'contactless' card had automatically cancelled his original card, something not mentioned in the paperwork that came with the old card" (Leyden, 2008). In this

case, the customer had no understanding of the implications of accepting, or using the new card and resolving the issue took time, phone calls, and caused frustration.

These issues are discussed in the following section where we look at key ethical principles, following an outline of the characteristics of pervasive technologies.

PERVASIVE TECHNOLOGIES

As we noted in our introduction the new vision is for smaller and less intrusive ICTs that are supportive in all aspects of daily life – travel, work, entertainment, education, and healthcare. To achieve this will need a continuing integration of technologies, and full exploitation of wireless and nano-technologies, and robotics. We are told that the infrastructure to support this vision "will consist of a myriad of wireless sensors working in collaboration …"[11] leading to 'the Internet of Things'[12] and concepts such as 'smart dust'[13] and 'smart matter'. The collaboration of sensors expressed in the previous sentence naturally implies the integration of compatible technologies with artificial agents, and the sensors themselves of course have to be embedded in physical infrastructures. As there are a 'myriad' of them, it can be assumed they will be embedded in a variety of places – household artefacts, building materials (for 'smart homes'), cars[14], fabrics (including clothing[15]) and in some cases the human body (Mordini, 2008).

Utilising these supportive technologies and integrating them within lifestyles has founded the research domain of pervasive and ubiquitous computing, and in Europe, the domain based on the concept of Ambient Intelligence. The document elaborating the concept of Ambient Intelligence (AmI) and which has informed research in Europe was produced by the Information Society Technical Advisory Group (ISTAG) to describe scenarios for the future based on technical developments at that time (Ducatel, et al, 2001). The aim of that exercise was to assess the feasibility of a technologically supportive environment from a technological and socio-economic perspective, and incorporating the feasibility of user uptake. This document has since provided the foundation for further scenarios and ethical and social assessments of such an environment (cf. Antona et. al., 2007; Friedewald, et. al., 2007; Duquenoy and Masurkar, 2003 and most recently Wright et al., 2008). One key application area that is seen to benefit from the utilisation of pervasive technology is that of supporting the elderly and infirm.

eHealth and the Aged

Pervasive technology is important in many areas of eHealth. It is one of the areas perceived to reap great benefits from pervasive and ubiquitous technologies, in particular the support of the elderly and chronically ill. Providing healthcare for an increasing elderly and infirm population is one of the key challenges for the future. Populations are increasing, people are living longer, and social changes have resulted in diminished home care provided by family members or neighbours. The cost to the state of providing good care is high, and if technology can enable people to live in their own homes for longer this benefits both the person and the state. ICT and in particular the technologies coming under the umbrella of ideas such as pervasive computing are seen as a way the challenge can be addressed (Duquenoy and Whitehouse, 2006). These technologies will lead to "innovative, context aware, smart services with natural and comfortable interfaces for older people with the goal to extend the time, in which they can live independently and autonomously in their homes"[16]. The context of home care has spawned research into supportive applications such as: drugs monitoring devices, health monitoring in homecare, assistive listening devices (using smart acoustic sensor arrays) and the extraction of data from distributed vision sensors[17]. Naturally, given

the vulnerability of the user group and their likely lack of competence with technology (as compared to the younger population) it is vital that potential ethical issues are considered and addressed by all professionals engaged in their design and implementation. In line with this Swift (2007) particularly notes that in the context of 'agency' – whereby the technology makes decisions, not the user – the systems has been designed with certain values that may be at odds with the user values, for example system values may be "increased competency, effectiveness, proficiency, productivity, complexity …". These are not necessarily values that are important to seniors; a recent study showed that values important to seniors include respect, equality, fairness, and trust (Burmeister, 2008).

Understanding and recognising ethical issues is not always easy. The following section uses a selection of core values to assess ethical impact in relation to the domain characterised by pervasive computing.

ETHICAL VALUES AND PERVASIVE TECHNOLOGIES

We have noted above some of the issues that have arisen from the application and implementation of ICT, not only as the subject of investigation by researchers but also from media reports of harms and the resulting debates amongst professionals, government and others. In this section we cover some core values that appear to be challenged by the pervasive technology context: privacy, equality; cultural diversity; and informed consent.

Privacy

We have said that privacy was surfacing as an issue as far back as 1967 and is now arguably the most hotly debated issue as far as ICT is concerned. Many of the debates are founded on breaches, or anticipated breaches, of privacy resulting from the use of the latest technologies.

Privacy is a human right, according to the United Nations: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks". (United Nations, Article 12 of the Universal Declaration of Human Rights).

In Europe this is supported by the European Convention on Human Rights (summarised below):

Respect for private and family life: Everyone has the right to respect for his or her private and family life, home and communications (Article 7). Protection of personal data: Everyone has the right to the protection of personal data concerning him or her (Charter of Fundamental Rights of the European Union (2000/C 364/01)).

The increasing capability of today's technologies to capture information, from names and addresses to DNA stretches concepts of privacy, and forces questions regarding aspects of ourselves (such as our DNA) that can be classed as 'personal data'. In a report published by the Information Commissioner's Office (the office responsible for overseeing data protection in the UK) the Information Commissioner asks: "What is the right balance between public protection and private life? How long, for example, should phone and internet traffic records be retained for access by police and intelligence services fighting against terrorism? Whose DNA should be held, and for how long, to help solve more crimes? What safeguards are needed for commercial internet-based tracking services which leave no hiding place?"

Earlier in the same report, the Information Commissioner recognises the impact of technology on privacy: "Never before has the threat of intrusion to people's privacy been such a risk. It is no wonder that the public now ranks protecting personal information as the third most important social concern. As technology develops within a globalised 24/7 culture, the power exists to build comprehensive insights into daily lives. As Inter-

net shopping, smart card technology and joined-up e-government initiatives reduce costs, respond to customers' demands and improve public services, more and more information is accumulated about us. According to one estimate, information about the average working adult is stored on some 700 databases." (Information Commissioner's Office Annual Report Summary 2005 – 2006)

In the environment of pervasive and ubiquitous computing, it is difficult at present to see how individuals might manage their privacy. On the one hand, the technology aims to be less intrusive, and on the other, we are arguing that users should know how its use might affect them. Paradoxically, the benefit of less intrusive devices for the user, in terms of visibility and disruption, leads to the likelihood of greater intrusiveness from third parties potentially to the users' disadvantage. David Wright points out that currently when users are online (and using the usual interface of monitor and keyboard) they may on occasions be aware of the need to make a deliberate choice regarding levels of privacy, but in the case of environments based on the concept of ambient intelligence "Such will not necessarily (or even likely) be the case in the instance of ambient intelligence. Indeed, an individual may not even be aware that he is in a space embedded with ambient intelligence" (Wright, 2005, p.49)[18]. We should not forget that the impact in such environments is not merely confined to adults who have full cognitive function – the environments will of course include babies and children, the elderly, and infirm. In some of these instances decisions regarding privacy permissions and limitations may fall to third parties (carers). There will be difficult choices to make as many of the benefits promoted for pervasive technologies, particularly in the home and to support the elderly, can only be achieved by monitoring individuals (in this case the aged person living independently). Details of personal movements, health information and medication required are just two frequently cited properties. Profiling is essential in such situations to achieve the aims of noticing unusual behaviours, or medical crises. The question to be considered then is: what are the personal boundaries, and what are the trade-offs? Will these users, that is, the aged, have any choice as to whether they accept these technologies? We will return to the matter of choice in respect of informed consent at the end of this section.

Equal Access

The home care setting raises other issues based on the principle of equality – in this context it relates to the opportunity for equal access to, and participation in, ICT. Again, equality is a fundamental human right, as characterised by the United Nations: (Article 7) All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to *equal protection against any discrimination* in violation of this Declaration and against any incitement to such discrimination. Also Article 21: Everyone has the *right of equal access to public service* in his country. (Authors' italics) (United Nations, Universal Declaration of Human Rights)

These rights are supported by the European Union in their Charter of Fundamental Human Rights: (Article 21) Non-discrimination: Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.

Taking the above into account, it is important therefore to ensure that all users have the same opportunities to utilise and manage ICT. In the same way that the future vision of ubiquitous and pervasive technologies is presented as enabling a good life, a similar forecast surrounded the growth of the Internet and the global communication applications that emerged from it. Buchanan (1999) comments: "We are repeatedly told the world is shrinking, boundaries are closing, peoples

becoming one - a result of the information age and its technologies. This growing intimacy, however, does not equate with equitable access and dissemination of information. The information age is a time of mythology, a time for fantasies of wealth, power, and ownership. The ethics of information services in this time, however, are very real, and don't necessarily correspond to these fantasies". This has a familiar ring. In their analysis of the ISTAG scenarios mentioned earlier Antona et. al. criticise the scenarios for taking the easy operability as a 'truth'. That is, the assumption that all the systems would work seamlessly together, be generally available, and that the ICT devices within the environment could be operated by the citizen. In fact, none of the scenarios discuss situations where individuals may want to access systems differently, that is, "individuals who cannot see, hear, speak, manipulate objects, move around or have difficulties with memory, concentration or problem solving" (Antona et. al., 2007; p.157). Actions need to be taken to ensure equal access – whether it is access to the infrastructure or accessible interfaces – and despite great developments to date in both respects there are still serious deficiencies whereby the poor, the uneducated, the computer illiterate, older people and disabled are denied opportunities for access. They note, for example, that extending the development of language translation to include sign language is not brought up for discussion, as well as a number of other technologies that would be helpful.

However, all that taken into account, they accept that the types of technologies that are employed and currently available to achieve the seamless and unobtrusive interaction envisaged can be a plus factor for people with different impairments. They quote for example the use of voice synthesis and recognition, input prediction (as currently used for text in mobile phones), vibrating materials used as alert systems, GPS (Global Positioning Systems) for tracking people who get lost or to help with navigation, smart tags identifying items in the house (that could be read from voice output mechanisms), and the replacement of traditional input devices by virtual representations, and other novel interfaces such as systems that are able to lip-read, and gesture recognition interfaces for sign language recognition. In the spirit of the vision of developing technologies, they interestingly use the concept of avatars (as intelligent agents) to provide help to this group of users. One such idea is an 'e-guide dog' for people who cannot see. They conclude that "if the new technology is developed and deployed taking on board the needs, requirements and preferences of all potential users, i.e., all the citizens of the emerging Information Society, and if ethical problems are taken into account, the emerging situation could be an opportunity for favouring socio-economic integration." (Ibid., 185)

Cultural, Religious and Linguistic Diversity

If we are to subscribe to the notion of equality, we should also recognise diversity. Although these two terms appear to be opposite, they both reflect the same notion of equal rights regarding the freedom of autonomous human agents. Equality means to respect cultural differences, religious beliefs and the right of all individuals to communicate in their own language. This message is conveyed in the European Union charter quoted above as: The Union shall respect cultural, religious and linguistic diversity (Article 22). If, as posited by Kant, ethical principles rest on universalisation it cannot be considered ethical for one group of people to deny others the rights that are expected by some. The issue of accessibility discussed above holds true especially in the case of language. The ability to access technology today, and maximise the benefits, relies heavily on literacy. As the computer interface changes and in some cases becomes invisible, this requirement may diminish and this would favour those who might currently be excluded. However these difficulties are man-

aged, interfaces and interactions must take into account cultural and religious diversity, both to meet ethical standards and to ensure user uptake. The first World Summit of the Information Society (WSIS) held in Geneva in 2003 resulted in the Geneva Declaration of Principles which upheld not only the right to access the Information Society, but also the right of individuals to participate in the discussion forum of the Internet in their own language. These rights are endorsed by UNESCO in their Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace adopted in 2003 (Poullet, 2007). In principle the pervasive and ubiquitous computing notion lends itself to accommodating diversity – as we have said above, interfaces will change or disappear, and may be replaced by touch screens (using symbols perhaps) or relevant language choices determined by intelligent agents. However, for this to happen design choices must be made and current experience with accessibility issues indicate that these design choices are forsaken in favour of reducing costs and capitalising on a mass-market standardisation.

Informed Consent

The right to participate in the Information Society, whether it is delivered via the Internet or other new developments and technological devices, must be founded on a principle of informed consent. To look at it another way, the alternative of 'uninformed coercion' does not meet the ethical basis of 'free choice'. The whole notion of ethics relies on individuals having the freedom to determine their actions. This is demonstrated in law where people are held responsible and accountable for their actions, and groups that are not are considered unable to make a fully informed decision, that is, children or people suffering from mental disorders. To be able to choose between actions one needs sufficient information and an understanding of the likely consequences of their choice. (Note our previous example of the RFID enabled bank payment card.) Where technology 'disappears' into the background, and when users have little knowledge of how their actions and choices are translated and mediated by technology, it is difficult to see how 'informed' the consenting user is (Duquenoy and Whitehouse, 2006). Where choices regarding participation are restricted, for example if services are supplied via technology as a matter of course, or where there are no alternatives, how meaningful is consent? Ratto (2007) notes: "One important ethical question that faces ubiquitous computing in general is not just what kinds of subjects do these infrastructures construct and maintain, but also what possibilities are left for individuals and non-normative social groups to resist these enfoldings and characterizations in order to allow for difference"? This notion of informed consent becomes particularly challenging when the user population consists of children and the elderly or infirm. In research ethics terms these groups are considered vulnerable and warranting particular care when conducting research with human subjects (Rivera et. al., 2001).

This issue becomes extremely relevant as we move toward the sharing of medical information and the use of electronic patient records. In this case, both groups of young people and the elderly and infirm become participants, are unlikely to have a choice, and have a reliance on third parties to mediate. In a recent report from the British Computer Society (BCS HIFSP, 2006) on health informatics the authors noted the following:

- There are major issues about the sharing of electronic patient data that need to be resolved whatever the shape of future informatics in the NHS. These must not be hijacked by technical issues, and *informed patient consent* should be paramount. (Section 1.12)
- If patients do not feel comfortable with the confidentiality of their data, they will not al-

> low significant information to be recorded or will withhold it, so *informed patient consent* is paramount. In either case, their care will suffer as a result. (Section 3.5) (Authors' italics)

Informed consent, which implies free choice, asserts moral autonomy and a sense of control over ones life and activities. The concept of user control becomes significant in the pervasive computing environment. Earlier in this section, under the topic of privacy, we discussed the use of ambient intelligent systems, profiling, and monitoring elderly people in the home. Wright notes the need for individual control of the technologies in order to meet the requirements of the principle of autonomy: "It should be possible for persons to control and make choices concerning the functioning of ambient intelligence, e.g. concerning their own profiles or the system's operation. This is an implication of the moral principle of autonomy." (Wright, 2005; p.194).

GUIDING THE PROFESSIONAL: CODES OF CONDUCT

As discussed above, there are many varying approaches to ethics. There are difference ethical theories, as well as cultural and religious views that influence ethical positions. With so many competing positions, it seems there is no sure means of ensuring public trust in product development, because the ethics of designers can vary dramatically. Add to this that few ICT professionals have training in philosophical ethics and it becomes difficult to see how designers are meant to give adequate consideration to ethics. What is needed for emergent technologies in ICT, such as pervasive computing technologies, is a normative approach to ethical decision making within design.

Normative Ethics that Guide the ICT Professional

One can see from the discussion on positive, negative and neutral issues, and the detailed examples on privacy, that ethical considerations are important for ensuring public trust of newly introduced technologies.

In the USA, the UK and in Australia, there are clear guidelines for what it means to be a professional. For instance, the Australian Council of Professions (ACP) accredits professional societies for law, engineering, medicine and many other areas, including the Australian Computer Society. The professional ICT societies in the UK, USA and Australia share a common understanding of what it means to be a professional. Among these principles are that a professional provides a service to society, and that professionalism implies ethical behaviour. Put in terms used earlier in this chapter, public trust (implying duty of care) and awareness of ethical considerations are important aspects of an ICT professional's work.

For accreditation as a professional society, the ACP insists on a publicly available code of ethics that all members of that professional society are required to adhere to. As stated earlier, there are many ethical theories and divergent religious, cultural and other influences on a person's ethics. A professional ethic, that is, an ethic based on the code of one's professional society, is seen as a normative approach, in that it ensures a certain standard that the ICT professional is committed to, irrespective of his or her own religious, cultural or other convictions. Therefore, when considering appropriate ethical responses to emergent pervasive technologies, the predominant consideration should be what one's professional society stipulates. Even this approach is not guaranteed to solve all situations. Some ICT societies do not have a code of ethics, and some countries have multiple ICT societies, each with their own (albeit similar) codes of ethics. Add to this that ICT development can span multiple countries, and the complexities

increase. While there is no single universal code of ethics, there are common aspects. Professionals working with ICT can be involved in different application areas, and there are often specific codes or guidelines relevant to these different areas. One of the most widely accepted codes of ethics for developers is the Software Engineering code, developed by the Association for Computing Machinery (ACM) society. We recommend that if developers do not have a code in their own country to follow, that they use the ACM code. There are fields of professional work that may warrant a more focussed approach to situations in the field, for example the British Computer Society has produced a handbook of Ethics for health informatics professionals that details rules of ethical conduct for health informatics professionals (Kluge, 2003).

Codes have many uses. Those most important to the current discussion include the fact that codes can identify both current and future problem areas. In addition, codes help the professional to identify and think through potential ethical issues and how to resolve them before actual problems arise. There is also the concern to protect oneself from litigation. While adherence to one's professional code does not guarantee immunity from litigation, codes lend support and justification for the actions of individuals faced with problems that are addressed by the code; they are a means of substantiating that one has followed best practice during development of the technology.

The Chair of the ACM ethics committee, Donald Gotterbarn, strongly advocates the use of a professional ethic. Professional ethics in his view is about the values that should guide a professional. These are not personal values necessarily, but the values agreed to by the ICT society in that country. They are an authoritative standard, based upon accepted norms, and can be seen as normative ethics.

Given the many different ICT societies and their different codes, professional responses can vary from one country to another. The following examples serve to illustrate this. In considering examples, we need to consider pervasive computing from the viewpoint of the user (as in the privacy example below, where the user is the person using the ICT to monitor seniors), as well as from the designers viewpoint (as in the example of cultural diversity below).

Privacy

In systems administration work there is a conflict of interest that can arise, that one can easily envisage arising with pervasive computing. A systems' administrator can be called upon to investigate problems with the computer of a corporate executive, and in the process discover non-work related material on the computer. This could be pirate software, pornography or something else. As an ICT professional, the systems administrator has a reporting obligation, yet the conflict arises in that this involves a colleague, who may consider the contents of their computer a matter of privacy.

Similarly, as we have illustrated above, monitoring seniors in their homes is an increasingly common use of various and integrated pervasive technologies. If in the process of such monitoring instances of elder abuse are discovered (where a carer, often a relative, beats the senior, refuses to change their (bed) clothes for long periods, doesn't feed them very often, etc), what is the professional response?

It may be argued that this falls outside the responsibility of the ICT professional, in that the user monitoring the senior may be a medical practitioner, not an ICT professional. However, the Systems Administrator Guild [SAGE (Aust.)], sees the related example above, as clearly within the purview of professional responsibility. It is not an invasion of the executive's privacy, but rather a professional obligation to report the offence. We will assume that the user in this case is an ICT professional; it could for instance be a systems engineer working with medical practitioners to maintain the technology involved in monitoring seniors in their homes.

Equal Access

Again, we can build on knowledge from other areas of ICT. In many nations, there is legislation about equality of access for people with disabilities. One can readily envisage a situation in which pervasive technology designers need to make design considerations about whether and how to implement systems for equality of access. Wearable technology is one example of pervasive technology that we refer to above. If one wears intelligent earrings, that whisper the name of the person you are speaking to into your ear, are designers obliged to cater to people who are deaf?

Arguably, this is more a matter of legal, rather than professional obligation. For instance, in Australia accessibility considerations (with some exceptions) apply to government rather than private developments. So there would be no legal requirement for alternative designs in this instance, however in the UK this might not be the case[19].

Cultural, Religious and Linguistic Diversity

Imagine a major event, such as a major sporting event. Organisers may want ambient (intelligent) systems that monitor prospective users to automatically changing the language display. During the testing phase the developers could be confronted with the problem of the console changing language frequently as people of different nationalities approached the area. (This would be technically possible by exploiting the country identifier and language preference choices coded in the chip of each person's identity card.) Instead, they decide that they will utilise the intelligent support users have via their mobile phones, incorporating a language translation device for users to hear their preferred language. However, whilst this meets multicultural needs, they have to make text subtitles available on the console for hearing impaired users. They could also investigate an option for designated language specific areas within the stadium area. (Although this may necessitate national grouping which could cause other problems – in these days of heightened perceptions regarding terrorist threats a policy of having certain cultural groups together could be beneficial for intelligence and law enforcement purposes, but may be viewed negatively by civil liberties groups.)

Implementations like this might be considered in Europe, but less so in a country such as Australia. In Australia, citizenship, study and most work places require at least a minimum level of proficiency with English, so designers could safely assume that English is the only language to design for, despite the significant multi-cultural diversity that exists in the country. However, such assumptions of English proficiency are less appropriate, if the event were staged in Europe or elsewhere, and in such cases the accessibility principles noted above would apply.

Informed Consent

Pervasive technology is complex, not only in itself, but also by virtue of the fact that it is integrated with many other technologies, all of which together achieve an intended purpose. Monitoring seniors can involve multiple technologies, manufactured by different companies, and many will be embedded into appliances, walls, floors, etc. This makes it difficult to test individual pervasive technologies with users. Further, there is the issue of 'cognitive overload'. If a senior volunteers to test a new pervasive technology, how much should they be told? HCI informed consent procedures require that users by fully informed, so they can comprehend what is being asked of them and make an informed decision about participating in user testing. Think of your elderly mother, grandfather, or neighbour. In many instances memory loss to some extent is common, not necessarily in the form of dementia, but simply a function of ageing. Fully informing

such a user about all the integrated technology is likely to overwhelm them, to a point where they may refuse to participate.

However, it might be possible to set up a test situation where a carer or family member is present, so that the impact of new technologies could be assessed and feedback given.

Informed consent as such is not specifically addressed in either the Australian code or the BCS code, although both do guide professional decision making with regard to social implications, such as considering the risks to individuals affected by one's work (ACS) and not misrepresenting or withholding information (BCS).

Normative Responses

Each of the examples above will be handled differently by professionals from different countries. However, the codes of ethics in most western countries, while different, have many similarities. Readers are encouraged to consider their own professional society's code, in considering an appropriate response. Generalising, based on the codes of the British (BCS), Australian (ACS) and two major societies of the USA (ACM and IEEE), the following responses could be considered for ICT professionals from western countries.

In Australia, the code of ethics is divided into 6 ideals (values), that are then each elaborated into 4-6 statements aimed to show how the individual professional should respond (as opposed to what a corporate response ought to be, for which there is a separate code). The first ideal 'priorities' addresses the privacy case above, and to a lesser extent also that of cultural diversity and informed consent. That priority states, "I must place the interests of the community above those of personal or sectional interests." (ACS, 2008) The specific clauses of the code show that while the professional is obligated to secure the information gathered through monitoring and protect the identity of those monitored, they have a wider (more important) obligation to put the interests of the person being abused first. Similarly, the two main codes in the USA stipulate that public interest must override interests of clients and employers.

In the UK, the BCS Code of Conduct has as its first category "The Public Interest". This category would cover the privacy example particularly in the case where any local law is broken (e.g. in the case of pirate software) the professional has a duty to abide by that law and, under the BCS Code of Conduct have "regard to the legitimate rights of third parties".[20] In the example of equal access the professional requirement, according to the BCS Code of Conduct (Principle 4) is that: You shall conduct your professional activities without discrimination against clients or colleagues. An additional note on that document offers some clarification "Grounds of discrimination include, but are not limited to race, colour, ethnic origin, gender, sexual orientation, age and disability". This principle would also cover, to some extent, the issue of cultural, religious and linguistic diversity.

The issue of informed consent is a well-known normative principle in research ethics, but due to the different nature of research – i.e. the difference between research participants and consumers – the notion of informed consent does not specifically find its way in to the codes of ethics of professional bodies. This is not necessarily unreasonable, given that most research conducted by members of a professional body would be done through recognised research channels where informed consent is a requirement. However, the principles of informed consent, that users or consumers should have some understanding of what they are 'buying-into' or being asked to use in their lives, should be considered by professional bodies. Technical developments are moving fast, and the outcomes of their use are sometimes surprising and unwelcome, so the question could be asked: are consumers becoming research participants?

CONCLUSION

Pervasive computing is the combination of emergent technologies and professionals introducing it need to heed the lessons from earlier introductions of emergent technologies. Though the ethical issue of privacy has been recognised and to a certain extent accommodated in design considerations today, new concerns arise with the invisibility of pervasive technologies. For example, the paradox that less intrusion, in terms of 'noticeability' and 'disruption', leads to the likelihood of greater privacy intrusiveness.

The ethical challenge of pervasive computing comes from the combination of different technologies and exchange mechanisms, the invisibility of the system and its capacity for data-handling, reactive technologies (context aware and reacting to user preferences), information about the processes undertaken in real-time, (user) knowledge of what is happening and value of different types of data (for instance, medical data may be considered more sensitive and in need of more careful guardianship), and user authentication/validation. To gain public trust and acceptance, users must be aware of the operation of pervasive technology (even if in the background) and have some choice to disengage. This poses a challenge for many in the ICT profession, such as for HCI professionals - how to put the technology in the background, and at the same time offer some sort of interface to users so that they can interact.

There is a need to consider the whole technology system, in context, and including diverse users. We should also not forget the reality of integration with legacy systems and any ethical challenges such a situation might pose, for example reduced security of private information. New technological developments are always situated within an existing technological context and are just part of a continuum of change. When significant conceptual changes occur (such as we saw with the Internet, and we will see with pervasive computing), developers and users need to be aware of the implications of the new technology infrastructure on ethical and social impacts. Considering human values, such as the ones, we have discussed in this chapter, which are set out in legislation, and research ethics, and following professional guidelines, will become vital to gaining the confidence of users and increasing public acceptance.

FUTURE RESEARCH DIRECTIONS

The key challenge to integrating ethics within the design processes is to differentiate between the positive and negative affects of the technologies, and the uses to which they can be put. For example, profiling helps in the customisation of technology to individual needs, but can also affect privacy (as reported by the UK Information Commissioner (2005-2006)). We have noted the tension between personal boundaries and the trade-offs to be made in monitoring seniors. Research is needed in this complex area regarding the specified intended purpose of a technology, ascertaining and fixing the boundaries of purpose (i.e. de-limiting function creep), and evaluating personal boundaries and acceptable trade-offs.

We highlighted the importance of user knowledge and understanding (implied in informed consent) and the difficulties of achieving this posed by increasingly invisible technology. This will be a research challenge for the HCI community.

In maximising the benefits of pervasive technologies, there will be a greater reliance on intelligent artificial agents collaborating to exchange information, negotiate user preferences (for example privacy preferences) and find information. A greater understanding of these interactions – their scope, how decisions are made, how to ensure authentication of third-party intelligent agents – is needed in order to be able to fully consider any ethical impact.

Tools for ethical assessment that include foresight methods, frameworks, and ontologies, will

be needed to accommodate the changing technological scene, and processes developed that aid communicative practices between technologists and social/ethical specialists so that technological aspirations and ethical considerations can be more effectively integrated from conception to implementation.

Intelligent devices do not operate in isolation, but are embedded in a social context and have an impact on individuals as users. Therefore, as they are introduced into the various environments and cultures within which they will be used, consideration must be given to policies and regulation, and to the rights of individuals to retain some control over their use. Process and best practice methods for multi-stakeholder consultation across all disciplines will be needed to ensure maximum coverage of potential issues. If these artefacts are to bring benefits and not harm to citizens and commerce a consideration of potential ethical impact must be included in the vision.

REFERENCES

ACS. (2008). *Code of ethics*. Australian Computer Society. Retrieved March 10, 2008, from http://www.acs.org.au/index.cfm?action=show&conID=coe.

Antona, M., Burzagli, L., Emiliani, P.L., & Stephanidis, C. (2007). Ambient Intelligence and implications for people with disabilities. In *Towards an inclusive future: Impact and wider potential of information and communication technologies* (P.R.W. Roe, Ed.) COST219ter, 2007. ISBN: 92-898-0027. Full text from: http://www.tiresias.org/cost219ter/inclusive_future/index.htm accessed 27/11/2007

BCS HIPSP (2006). *The way forward for NHS health informatics: Where should NHS connecting for Health (NHS CFH) go from here?* A report on behalf of the British Computer Society (BCS) by the BCS Health Informatics Forum Strategic Panel, 15th December 2006.

Berleur, J., & Brunnstein, K. (1996) *Ethics of computing: Codes, spaces for discussion and law.* Chapman and Hall, Ltd. London, 1996.

Buchanan, E.A. (1999). An overview of information ethics issues in a world-wide context, *Ethics and Information Technology* 1, 193-201, 1999. Kluwer Academic Publishers. Netherlands.

Charter of Fundamental Rights of the European Union (2000/C 364/01). From: http://www.europarl.europa.eu/charter/pdf/text_en.pdf accessed 29/11/2007

Burmeister, O.K. (2008). *What 45,000 seniors value about online social interaction*. Proceedings of IFIP WG 9.5 2008 Conference on 'Massive Virtual Communities'. Lueneburg, Germany.

Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J., and Burgelman, J-C. (2001). *Scenarios for Ambient Intelligence in 2010.* Final Report, February 2001, IPTS Seville. From: ftp://ftp.cordis.europa.eu/pub/ist/docs/istagscenarios2010.pdf

Duquenoy, P., & Whitehouse, D. (2006) A 21st Century ethical debate: Pursuing perspectives on ambient intelligence. *The Information society: Emerging landscapes* (Chris Zielinski, Penny Duquenoy and Kai Kimppa, Eds.) Springer Science & Business Media, Series: IFIP vol. 195, 2006, ISBN: 0-387-30527-0.

Duquenoy, P., & Masurkar, V. (2003) Surrounded by intelligence … *Risks and challenges in the network society*, (Duquenoy, P**.**, Holvast, J., Fischer-Heubner, S., & Zuccato, A. Eds.) Proceedings of the Second IFIP 9.2, 9.6/11.7 Summer School, Karlstad, Sweden, August 2003.

Floridi, L. (1999). Information ethics: On the philosophical foundation of computer ethics. In Lucas Introna, Deborah Johnson and Helen Nissenbaum (eds.) *Ethics and Information Technology*, *1*(1), 1999, 37-56.

Gert, B. (1999). Common morality and computing. In Lucas Introna, Deborah Johnson and Helen Nissenbaum (Eds.), *Ethics and Information Technology, 1*(1), 1999, 57-64.

Gorniak-Kocikowska, K. (1996). The computer revolution and the problem of global ethics. *Science and Engineering Ethics*, *2*(2), 177-190.

Information Commissioner's Office Annual Report Summary 2005 – 2006. Published July 2006. From:http://www.ico.gov.uk/upload/documents/library/corporate/practical_application/annual_report_summary_2006.pdf

Friedewald, M., Vildjiounaite, E., Punie, Y., Wright D. (2007). Privacy, identity and security in ambient intelligence: A scenario analysis. *Telematics and Informatics, 24* (2007) 15-29. Elsevier.

Kluge, E.H. (2003) *A handbook of ethics for health informatics professionals*, The British Computer Society Health Informatics Committee, The British Computer Society, 2003.

Ladd, J. (1997). Ethics and the Computer World: A New Challenge for Philosophers, *Computers and Society*, September 1997, 8-13.

Leydon, J. (2008) Bank turns London man into RFID enabled guinea pig. *The Register* (27 January 2008). From: http://www.theregister.co.uk/2008/01/27/paywave/

Johnson, D.G. (2001). Sorting Out the Uniqueness of Computer-Ethical Issues, *Computer Ethics* (3rd Edition) Prentice Hall, 2001.

Moor, J.H., (1995). What is computer ethics? *Metaphilosophy*, *16*(4)

Mordini, E. (2008) Biometrics, human body and medicine: A controversial history in duquenoy, P., George, C., Kimppa K., (Eds.) (in press) *Ethical, legal and social issues in medical informatics*, Idea Group Inc.

Moss, J. (2002) Power and the digital divide, *Ethics and Information Technology* 4, 259-165, 2002. Kluwer Academic Publishers. Netherlands.

Poullet, Y. (2007). Internet governance: Some thoughts after the two WISIS. The information society: Innovation, legitimacy, ethics and democracy. Philippe Goujon, Sylvain Lavelle, Penny Duquenoy, Kai Kimppa, & Veronique Laurent (Eds.). IFIP International Federation for Information Processing (233), 2007. (Boston: Springer). 201-224

Ratto, M. (2007). Ethics of seamless infrastructures: Resources and future directions. *International Review of Information Ethics*, 8. (12/2007) 20-26.

Rivera, R., Borasky, D., Rice, R., Carayon, F. (2001). *Research ethics trainingcCurriculum*. Family Health International, 2001. From: http://www.fhi.org/training/en/Retc/intro.htm

Sampson-Wild, G., and Burmeister, O. K., 2001. The continuing evolution of best practice principles in designing for Web accessibility, proceedings of OZCHI2001 *Usability and usefulness for knowledge economics*, Nov, 122-127.

Swift, A. (2007) Locating 'Agency' Within Ubiquitous Computing Systems. *International Review of Information Ethics*, 8. (12/2007) 36-41.

Turkle, S., (1995) *Life on the screen: Identity in the Aage of the Internet*. New York: Simon and Schuster, 1995.

United Nations: Universal Declaration of Human Rights (1948). From: http://www.un.org/Overview/rights.html

Westin, A.F., *Privacy and freedom*. London: The Bodley Head, 1967.

Weizenbaum, J. (1976) *Computer power and human reason.* W.H. Freeman and Company, San Fransisco (1993 edition).

Wiener, N. (1960) Some moral and technical consequences of automation. *Science*, 131, 1355-8.

Wright, D., Gutwirth, S., Friedewald, M., Vildjiounaite, E., Punie, Y. (Eds.) (2008) *Safeguards in a world ofaAmbient intelligence*, Springer 2008.

Wright, D., 2005, The dark side of ambient intelligence, *Info*, 7(6), October, 33-51.

ADDITIONAL READING

Bynum, T.W. & Rogerson, S. (Eds) (2004) *Computer Ethics and Professional Responsibility*. Malden, MA: Blackwell.

Duquenoy P. (2005). Ethics of Computing. *Perspectives and Policies on ICT in Society*, Springer & SBS Media.

Kemppainen, E., Abascal, J., Allen, R., Delaitre, S., Giovannini, C., and Soede, M. (2007) Ethical and legislative issues with regard to Ambient Intelligence in *Towards an Inclusive Future: Impact and wider potential of information and communication technologies* (Patrick R.W. Roe, Ed.) COST219ter, 2007. ISBN: 92-898-0027. Full text available at: http://www.tiresias.org/cost219ter/inclusive_future/index.htm accessed 27/11/2007

McDermid, D.C. (Ed.) (2008) *Ethics in ICT – An Australian Perspective.* Perth: Pearson.

Rundle, M., Conley, C. (2007) *Ethical Implications of Emerging Technologies: A Survey.*

UNESCO, Paris, 2007.

From: http://unesdoc.unesco.org/images/0014/001499/149992E.pdf

Phillips, D. & Wiegerling, K. (Guest Eds.) Ethical Challenges of Ubiquitous Computing. *International Review of Information Ethics.* Vol 8. (12/2007)

Quinn, M.J. (2006) *Ethics for the Information Age*. 2nd ed. Sydney, Australia: Pearson.

Weiser, M. & Brown, J.S. (1997). The coming age of calm technology. *Beyond Calculation: the Next Fifty Years of Computing.* Metcalfe, R. & Denning, P. (eds.). Springer-Verlag, New York, 75-85.

Winter, J.S., (2006). Public involvement in technology policy: focus on the pervasive computing environment. *SIGCAS Computers and Society*, Volume 36, No. 3, September 2006.

KEY TERMS

Heuristic Evaluation: This has a precise meaning in Human Computer Interaction (HCI). In this chapter we are using the term in a similar fashion to its use in HCI. As in HCI, we think ethical evaluation of emergent technologies ought to take place early in the development of the new technology. As in HCI, ethical experts can evaluate the technology and its impact on society. Also as in HCI, this should be 3-5 experts, not one.

Invisible: Related to the idea of 'pervasive', this term describes the concept that ICT is becoming embedded within the social infrastructure in such a way that their use becomes commonplace and often invisible. Other terms that are used to describe this concept are 'ubiquitous computing' and 'ambient intelligence'.

Normative Ethics: Ethics is about directing people to consider the values of life, including concepts such as personal integrity. There is no single approach to ethics, nor a single unifying theory of ethics. This creates problems for ICT design, because designers can have varying ethical viewpoints that influence their design choices. For reasons such as this professional ICT societies stipulate that members should adhere to their professional ethical code, so that the public can trust that design choices were made against a norm, namely the ethical code agreed to by members of that professional society.

Pervasive: The idea that ICT increasingly pervades almost every aspect of daily life.

ENDNOTES

1 ETHICOMP (a conference series which began in 1995) and CEPE (Computer Ethics and Philosophical Enquiry).

2 For example, the International Federation of Computer Processing (IFIP), the British Computer Society (BCS) and the Australian Computer Society (ACS) amongst others.

3 See for example: SWAMI (Safeguards in a World of Ambient Intelligence) http://swami.jrc.es/pages/index.htm, ETHICBOTS (Emerging Technoethics of Human Interaction with Communication, Bionic and Robotic Systems) http://ethicbots.na.infn.it/index.php, MIAUCE (Multimodal interactions Analysis and exploration of Users within a controlled environment) http://www.miauce.org/

4 Starting with the Association of Computing Machinery (ACM) and Institution of Electrical and Electronics Engineers (IEEE) in the United States and followed by professional ICT societies elsewhere, for example the Australian Computer Society, the British Computer Society, amongst others. See Berleur & Brunnstein (1996) for a comprehensive overview of the Codes of Conduct for national computer societies at 1996.

5 For instance, the European Commission inclusion of attention to ethical impact, calls by national funding agencies for research into public perception, and the inclusion of a multi-stakeholder approach from the World Summit on the Information Society (WSIS) (See Action Line C10 of the Geneva Action Plan of the World Summit on the Information Society – regarding the ethical dimension of the information society: http://www.itu.int/wsis/docs/geneva/official/poa.html)

6 Kant worked through a number of versions of the categorical imperative, but the following summarises the position: "Act only on that maxim which you can at the same time will to be a universal law". Kant, I. Grounding for the Metaphysics of Morals, translated by James W. Ellington. Hackett Publishing Company, 1981. Indianapolis. P.421.

7 For a more detailed overview of these three authors and their continuing relevance to computing cf. Duquenoy, 2005.

8 The investigation of ethics as applied to information technology resulted in specific journals. The first, in 1999, was Ethics and Information Technology, published by Kluwer Academic Press, followed by Information, Communication and Ethics in Society (ICES) published by Troubadour press (from 2007 became the Journal of Information, Communication and Ethics in Society, published by Emerald Insight).

9 Discussions of whether the ethical issues raised by computer technology were novel in the sense that a new moral approach was required (cf. Ladd, 1997), whether the issues were the same but presented in a different guise (necessitating a conceptual change) (cf. Johnson 2001), or whether a new ethical theory more relevant to the online world was needed (cf. Gorniak-Kocikowska,1996; Gert, 1999; Floridi, 1999) were the focus of debate with the emergence of the new online 'cyberspace' community.

10 Cookies are text files stored on a users' computer by companies as a result of visiting their web site. Their beneficial use is to store the user details so that when return visits are made the website recognises the user which saves them re-entering their details. However, some contain more information about the user than is necessary and are used for extensive marketing purposes. Users' are often not aware of their presence and use.

[11] Extract from Workshop programmes: Ami-07 European Conference on Ambient Intelligence, Nov 7-10, 2007, Darmstadt, Germany. http://www.ami-07.org/wseu.html accessed 23/11/07.

[12] The 'Internet of things' denotes the use of RFID chips (Radio Frequency Identification) embedded in a myriad of physical objects, enabling the linking of physical objects with the Internet (or similar networked environments).

[13] The term and concept of smart dust was coined by Kristofer Pister, University of California, US. See http://www.dustnetworks.com/ accessed 26/11/2007.

[14] See for example the EU project PReVENT http://www.prevent-ip.org/ accessed 28/12/07.

[15] According to a report (April 1 2006, Science Dailey) quoting Tom Martin, a computer engineer at Virginia Polytechnic Institute and State University "E-textiles are a way for us to build wearable computers that look like normal clothing to build pervasive computing devices that fit in seamlessly with the environment." http://www.sciencedaily.com accessed 27/11/2007

[16] Extract from Workshop description involving the SOPRANO EU-IST Project, beginning January 2007. Ami-07 European Conference on Ambient Intelligence, Nov 7-10, 2007, Darmstadt, Germany. http://www.ami-07.org/wseu.html accessed 23/11/07.

[17] MINAmI EU project: http://www.fp6-minami.org/uploads/media/minami_brochure.pdf accessed 23/11/07

[18] In his discussion on privacy Wright also includes issues relevant for privacy management such as identity management (authentication) and security to engender trust and encourage user confidence.

[19] The Human Rights Act (1988) requires that people should not be discriminated against on "Any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status" (disability being equivalent to 'other status') and the Disability Discrimination Act (1995) requires 'reasonable' measures to be taken to allow access to: employment; to goods, facilities and services; education. In the example of the earrings above, it could be argued that a service is being provided, and some alternative option should be made available – the legal argument would hinge on what is 'reasonable'.

[20] The BCS Code of Conduct Principle 2: You shall have regard to the legitimate rights of third parties, and Principle 3: You shall ensure that within your professional field/s you have knowledge and understanding of relevant legislation, regulations and standards, and that you comply with such requirements.