Ethics and Information Technology (2005) 7:157–166
DOI 10.1007/s10676-006-0005-3

Freedom and privacy in Ambient Intelligence

Philip Brey
Department of Philosophy, School of Behavioral Sciences, University of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands
E-mail: p.a.e.brey@utwente.nl

Abstract. This paper analyzes ethical aspects of the new paradigm of Ambient Intelligence, which is a combination of Ubiquitous Computing and Intelligent User Interfaces (IUI's). After an introduction to the approach, two key ethical dimensions will be analyzed: freedom and privacy. It is argued that Ambient Intelligence, though often designed to enhance freedom and control, has the potential to limit freedom and autonomy as well. Ambient Intelligence also harbors great privacy risks, and these are explored as well.

Key words: Ambient Intelligence, autonomy, freedom, Intelligent User Interfaces, invisible computers, privacy, smart objects, Ubiquitous Computing

The promise of Ambient Intelligence

Envision the following scenario:

> A young mother is on her way home, driving together with her 8-month old daughter who is sleeping in her child seat on the passenger side of the car. The infant is protected by an intelligent system called SBE 2 against airbag deployment, which could be fatal in the case of an accident. SBE 2 detects when there is a child seat on the passenger seat instead of a person and automatically disables the airbag (...) Arriving home, a surveillance camera recognizes the young mother, automatically disables the alarm, unlocks the front door as she approaches it and turns on the lights to a level of brightness that the home control system has learned she likes. After dropping off her daughter, the young mother gets ready for grocery shopping. The intelligent refrigerator has studied the family's food consumption over time and knows their preferences as well as what has been consumed since the last time she went shopping. This information has been recorded by an internal tracking system and wireless communication with the intelligent kitchen cabinets. Based on this information, the refrigerator automatically composes a shopping list, retrieves quotations for the items on the list from five different supermarkets in the neighborhood through an Internet link, sends an order to the one with the lowest offer and directs the young mother there. When arriving at the supermarket, the shopping cart has already been filled with the items on her shopping list. Spontaneously, she decides to add three more items to her cart and walks to the check-out. Instead of putting the goods on a belt, the entire cart gets checked out simply by running it past an RFID transponder that detects all items in the cart at once and sends that information to the cash register for processing. (Source: Raisinghani et al. 2004).

This scenario illustrates the vision of Ambient Intelligence. Ambient Intelligence is a new paradigm in information technology that envisions a future society in which people will live and work in environments that recognize and respond to them in intelligent ways (Aarts et al. 2001; Aarts and Marzano 2003; Riva et al. 2005; Weber et al. 2005). This future is made possible through the integration of microprocessors into everyday objects like furniture, clothes, kitchen equipment and toys, that are provided with intelligent and intuitive interfaces and that can communicate with each other through a wireless network. The technology is in the background, almost invisible to the user, and interfaces are highly natural, responding to inputs like voice and gestures. People are surrounded with possibly hundreds of intelligent, networked computers that are aware of their presence, personality and needs, and perform actions or provide information based on perceived needs. The ambient intelligence vision conceives of a world in which humans are empowered and everyday life is improved through such "smart surroundings," resulting in added convenience, time and cost savings, increased safety and security, and more entertainment. Ambient

Intelligence, or AmI in short, has been heralded by some as the next step in the information technology revolution, and a major building block in the construction of an advanced information society.

The vision of Ambient Intelligence is now shared by research centers around the world, and has won major financial backing from the European Union. It was originally proposed by Philips Research in 1999. Philips Co. is one of the world's biggest electronics companies, and the largest one in Europe. The AmI vision has been further developed in Philips Research's collaboration with the Massachusetts Institute of Technology (MIT), in particular in MIT's Oxygen project. Philips' vision was adopted by the Information Society Technologies Advisory Group (ISTAG) in 1999. ISTAG is the key advisory body to the European Commission for its information technology research policy.

As a result of ISTAG's endorsement, the vision of Ambient Intelligence was adopted in 2001 as the leading theme for EU-funded research on information technology for the years 2002–2006, within the Information Society Technology division of the EU's Sixth Framework Programme for Research and Technological Development. This means that 3.7 billion euros were made available for research in this area. The Ambient Intelligence vision has been endorsed by major industrial players besides Philips like Nokia and Siemens, and by major research centers like Fraunhofer, IMEC and INRIA.

Clearly, the AmI vision now has a lot of industrial and political support, most strongly in Europe, but also in other places in the world. Moreover, the AmI vision may well become reality in the not too distant future; most technologies it requires are in place or under active development, and the ISTAG group predicts that many applications can be on the market by 2010 (ISTAG 2001).

Technology

Ambient Intelligence is an approach that combines two major technologies: *Ubiquitous Computing* and *Intelligent User Interfaces*. Some have called Ambient Intelligence a more human-centered version of Ubiquitous Computing, if not a successor to this approach. Ubiquitous Computing, also called *Pervasive Computing*, is an influential approach in information technology that aims to integrate computation into the environment and to move interaction with information technology away from a single workstation. In Ubiquitous Computing, computers do not appear as distinct objects, but are embedded into everyday working and living environments in an invisible and unobtrusive way. They make information, media and network access constantly and transparently available. This move away from single workstations may involve pen-based technology, hand-held or portable devices, wearable computers, large-scale interactive screens, wireless networking infrastructure, and voice or vision technology.

To the Ubiquitous Computing approach, Ambient Intelligence adds the technology of Intelligent User Interfaces, which are also called "User Adaptive Interfaces" and "Social User Interfaces" (Maybury and Wahlster 1998; Alcañiz and Rey 2005). These interfaces, which are based on human–computer interaction research, go beyond traditional interfaces like the keyboard, mouse and monitor. They aim to make information technology easier to use by making interactions with it more intuitive, efficient, and secure. They are designed to allow the computer to know a lot more about users and the user environment than traditional interfaces can. Intelligent User Interfaces (IUI's) have two key features: profiling and context awareness. Profiling is the ability to personalize and automatically adapt to particular user behavior patterns. Context awareness is the ability to adapt to different situations. Profiling and context awareness depend on sensors to record aspects of the environment and of user behavior and intelligent algorithms to make inferences about situations and users. IUI's are capable of creating a perceptive and proactive computer environment, rather than a passive one that relies on active and comprehensive user input.

IUI's can be developed to detect a wide range of features of users and user environments. For example, they could detect moods and emotions of users, by detecting delight or stress via language, speech and gesture. They could detect activities of users (e.g., whether someone is idle or working), the physical or virtual location and availability of objects and persons, and the social organization of groups and the roles participants play in them (e.g. leader, major contributor). IUI's could acquire information about users and the environment through different modalities. Visual recognition includes the recognition of facial features, 3D gestures, movements, objects and locations. Sound recognition includes the recognition of voice, speech, melody, and background sounds. In, addition, IUI's may include tactile recognition (as in touch screens), scent, recognition, and other sensor technologies. In many cases, IUI's will allow for multimodal input, combining mixed and possibly ambiguous or imprecise input such as written text, spoken language, gestures and gaze.

The output of intelligent ambient devices will often be multimodal as well, including coordinated presentations that may combine text, speech, and

graphics, and may involve animated, life-like agents. IUI's can be developed to facilitate knowledge- or agent-based dialogue, in which the computer engages in extensive communication with a user, and displays flexibility by adapting to the situation, by being capable of handling errors and interruptions, and possibly by being capable of combining multimodal dialogue inputs (spoken, written, and gestural). Agent-based dialogue systems can be included in IUI's to monitor users and make assumptions about their intentions and the task they are trying to perform, and help them in their activities by making suggestions.

Some proponents of AmI conceive of it as depending on a third major technology next to Ubiquitous Computing and IUIs: Ubiquitous Communication. This is an approach that aims to ensure flexible and omnipresent communication possibilities between interlinked computer devices that can be stationed in various locations. Embedded computer devices should not only be able to recognize and communicate with users, but also to recognize other devices, and be able to communicate with them. Ideally, such communication should be completely wireless and ad hoc. Ubiquitous Communication is necessary in order to make Ubiquitous Computing, and thereby Ambient Intelligence, operate at its full potential. After all, if the environment is full of computers that cannot communicate with each other, only limited functionality results. Ubiquitous Computing is to be made possible through wireless network technology, including Wireless Local Area Network (W-LAN), Bluetooth, and Radio Frequency Identification (RFID) technology.

Applications

Major markets for Ambient Intelligence are thought to be found in the *home environment* and in *organizations*. Most attention so far has been directed to the home environment. Technology developers have been working on conceptions of the "Intelligent Home," the "Automated Home," or the "Home of the Near Future" (de Ruyter 2003). The Intelligent Home is filled with "smart" objects that anticipate and respond to user needs and are supposed to make home life easier and more fun. In the Intelligent Home we may find a DVD recorder that will automatically record the favorite programs of its inhabitants when they are not at home. It may have a heating system that will automatically switch off when no one is at home, and switch on when someone comes at home, and choose the desired temperature for a room based on inferences about its users and the situation at hand. It may have a security network with a front door security camera and possibly more cameras for the easy identification of visitors.

The Intelligent Home may also have an interface in the bathroom mirror that projects the morning or evening news and important messages. It may have one or more centralized intelligent interfaces, either stationary or mobile, with which a multiplicity of electrical home appliances may be monitored and controlled, like the oven, the washing machine, the dish washer, the television set and the stereo system. It may have one or more interactive video walls that may project information or movies, or background paintings. It may have an intelligent refrigerator that employs sensors and a memory of the grocery-buying pattern of the inhabitants to compose a shopping list that may even be automatically forwarded to the local supermarket if it has a delivery service. Ambient Intelligence in the home is thought to benefit home users by providing higher convenience, by saving time and money, by providing added security and safety, and by providing more entertainment.

For organizations, AmI applications are thought to provide benefits by bringing higher efficiency and effectiveness and enhanced security and safety. AmI may help to organize the office in a better way, by making it "smart," and by providing new ways to monitor and coordinate work. Healthcare is conceived of as a promising domain. Distributed health care support systems are envisioned that support diagnosis and treatment in diverse settings, including the home and on the road. Through such a system, patients may undergo medical treatment at home, thereby freeing hospital space. AmI may also help people with disabilities and the elderly acquire more control over their environment. Other areas in which AmI applications are thought to have promise include mobility and transportation (e.g. navigation systems), industry (industry automation systems), the public domain (local information delivery systems in public buildings and places), education, and shopping and commerce.

Shopping and commerce allow for some particularly interesting applications of AmI. In AmI-enabled stores, the store's network may connect with the shopper's personal network and may make recommendations to the shopper based on her personal profile or give background information on products. At home, AmI sensors may detect needed items based on inhabitants' buying habits and preferences and compose shopping lists or make recommendations. This information may even be combined with link to online or real-world shops that may list products on sale or may test for availability of products.

As a next step, embedded computers may do the shopping themselves, issuing online orders of needed

products. This has been called "silent commerce" by the business consultancy Accenture, and involves "autonomous purchasing objects" that have been authorized by users to do their own shopping (Accenture Technology Labs 2002). Invisible RFID-tags embedded in products would allow consumer devices to read out the unique identification number of an item or product and use this to acquire background information on the item. This could also take place outside stores. A consumer may see someone walking by with an appealing sweater, scan its tag for its identification number, and receive information on its brand and pricing, as well as links to online stores where it may be bought. The wearer may even earn a commission every time someone makes a purchase inspired by his sweater's identification number. Rented objects equipped with sensors and communications capabilities could be charged on a pay-per-use basis. For example, a sofa could count the number of persons that sit on it, the persons' weight and seating time, and create a monthly itemized billing statement. Insurance companies could introduce dynamic insurance rates that are based on actual behavior, and that allow for more fine-grained calculations of risks. For instance, a smart car could provide an insurer with detailed information of the driving style and habits of its owner, and the car insurance premium could be adjusted accordingly (Bohn et al. 2005).

Freedom, autonomy and control

One of the fundamental ethical questions regarding Ambient Intelligence is whether it is more likely to enhance human autonomy and freedom or diminish it. The philosophical ideal of autonomy, or self-governance, has been a core ideal of Western societies since the modern era. It has long been defended as fundamental to human flourishing and self-development (e.g., Dworkin 1988; Hill 1991). Individual autonomy is often defined as self-governance, that is, the ability to construct one's own goals and values, and to have the freedom to make one's own decisions and perform actions based on these decisions. Individual autonomy is often defended as important because such self-governance is required for self-realization, that is, it is a freedom one must have in order to create a life that is experienced by oneself as meaningful and fulfilling. As Dworkin has pointed out, moreover, individual autonomy may be a requirement for a conception of human beings as equals. If some human beings are not autonomous, they cannot give equal input into moral principles that are aimed to reflect individual preferences, and hence they cannot function as equals in moral life (1988, pp. 30–31).

The ideal of autonomy is strongly related to the ideal of freedom. As Isaiah Berlin has argued in a famous essay, freedom comes in two sorts, positive and negative (Berlin 1979). Negative freedom is the ability to act without obstruction or interference by others. Positive freedom is the ability to be one's own master, having one's own thoughts and making one's own decisions. Negative freedom means that no one stands in your way. Positive freedom means that no one tells you what to think. Both types of freedom involve control. Positive freedom involves control over the environment. Negative freedom involves self-control, or control over one's own thoughts and decisions. The issue that will now be investigated is what potential AmI has to enhance positive and negative freedom, and to take it away.

Proponents of Ambient Intelligence claim that it will help humans gain more control over the environments with which they interact because it will become more responsive to their needs and intentions. Paradoxically, however, this control is supposed to be gained through a delegation of control to machines. In other words, control is to be gained by giving it away. But is more control gained than lost in the process? According to David Tennenhouse, vice president of Intel Research, this is certainly the case. Tennenhouse is proponent of the approach of *Proactive Computing*, which is one of the computing paradigms on which AmI is founded (Tennenhouse 2000). Tennenhouse contrasts Proactive Computing with *Interactive Computing*, which has been the dominant approach since the 1960s. In this "human-centered" approach, individuals are to operate one-on-one with computers, inputting commands and waiting for responses. Computers are to be designed such that they support this mode of operation and faithfully obey the commands of their users.

This approach, Tennenhouse argues, does not work in an information technology landscape in which one's environment may contain hundreds of networked computing devices. In such a landscape, computers should not wait for human inputs in order to take an action or communicate with another device, but proactively anticipate the user's needs and take action on his or her behalf. It is only desirable that humans give up direct control in such a setting, Tennenhouse argues, because if humans were to stand in between a computer and its environment, they would only function as glorified input/output devices that perform tasks that the computer can perform for us. By being freed from the tedious task of interacting with a multiplicity of computing devices and making decisions for them, humans can freely

focus on higher-level tasks. Tennenhouse's argument is hence that humans can gain better control over important tasks by delegating unimportant tasks to embedded computers, as long as these devices are programmed to anticipate and respond to their needs.

Ways of gaining and losing control

Ambient Intelligence may hence help humans gain more control over the environments with which they interact, and it may take away control as well. Let us now consider more carefully how such gains or losses in control are realized. There are at least three distinct ways in which AmI may confer control to its users. First, AmI may make the human environment more controllable by making it more responsive to voluntary action. AmI may make it easier for humans to reach particular goals or outcomes in an environment in which they operate by requiring less cognitive or physical effort from users in their use of objects in the environment. For example, a stereo set that starts playing music with a finger snap or the exclamation of a word is obviously easier to control than one that requires the user to go to the set and push a number of buttons. Second, AmI's may enhance control by supplying humans with detailed and personalized information about their environment, that may enable them to interact with it more successfully. Third, AmI may be seen as conferring additional control by doing what people want without them having to engage in intentional behavior. That is, AmI has the promise of making the environment respond to human needs without any cognitive or physical effort at all, freeing people from tedious routine tasks.

Although there are hence obvious ways in which AmI seems to enhance human control over the environment, AmI has also been argued to have a serious potential to take away human control. This may also happen in several ways. First, smart objects may perform actions that do not correspond to the needs or intentions of its user. This may happen because the object makes incorrect inferences about the user, the user's actions, or the situation. Second, even if a smart object ultimately does what one wants, it may still be experienced as taking away control by telling us how to act, by assigning particular meanings to human behaviors that may be unintended, and by requiring negotiations and corrective actions in order to avoid the object's preferred course of action and implement one's own. This loss of control may not only be due to the additionally required effort, but also to the psychological pressure that results from going against the will of a smart object that is suppose to have a good understanding of one's needs and desires. As Milon Gupta has put it: "In a way, it is quite a relief to know that all things in your home, including your PC and your heating system, are dumb. They give you the feeling that you are always in control. This feeling is in danger, if fridges, toasters, lamps, and wall paint suddenly turn smart. The very advantage of Ambient Intelligence could become paradoxically reverted: Devices and applications, which have become physically unobtrusive, could turn out to be psychologically obtrusive." (Gupta 2002). People may even put valuable time and energy into understanding the workings of smart objects in order to try to "outsmart" them.

A third type of loss of control occurs when a user profile or knowledge base in a smart object does not just represent the needs of the user, but also the interests of third parties. This may happen, for example, when a smart object has either been designed to take certain commercial interests into account, or gives commercial firms access to the user profile or knowledge base. This may result in a smart object either recommending a purchase or making a silent purchase which is not based on the user's real needs but on needs that a commercial firm assigns to the user. In general, the networked character of smart objects makes it possible that some third party on an external network imposes its will on a user through the behavior of a smart object. A fourth and final type of loss of control may occur when smart objects are used by third parties for data collection and surveillance. Thus collected information about someone's preferences, behaviors, social interactions and experiences could be used by third parties to harm that person's interest and exercise control over him or her. This type of loss of control will be further discussed in the next section on privacy in Ambient Intelligence.

Design ideals and sobering reality

Advocates of Ambient Intelligence argue that well-designed AmI does not take away control but only enhances it. Such AmI would have to meet high criteria: It would always or nearly always have to be correct about the needs and intentions of users, it would have to perform actions that can easily be modified or corrected by users, and it would have to bar third parties from influencing the knowledge base or having access to private information. Is this ideal attainable? I will argue that this is not likely. Let us first consider the conviction that AmI can be designed that is nearly always correct in inferring the needs and intentions of users. This would seem to require an advanced form of Artificial Intelligence that currently, at least, does not exist. People themselves

often have difficulty finding out what they want or need, so it seems that computers would often have to be more knowledge of the needs of users than these users are themselves. Some proponents of AmI have argued that computers may indeed acquire a better understanding of people than people have themselves. Computers may collect so much data about persons for such an extended period of time, that they may draw conclusions about their preferences and needs that people are incapable of drawing themselves. Whether this is true remains to be seen. Critics of AI research have argued that computers lack a true understanding of situations and contexts and are incapable of reaching the level of understanding of situations that humans can attain (Searle 1980; Dreyfus 1992). Users may themselves have an important role in composing a pre-given profile of their preferences. However, users cannot themselves predict their preferences in every future situation, and preferences of people also change over time. It is therefore likely that smart objects that are supposed to guess people's preferences, needs or intentions will frequently get them wrong.

But let us suppose, for the sake of argument, that smart objects could be made that are so intelligent that they nearly always correctly predict the needs and intentions of users. Then a new problem appears. Such objects may well use such complex algorithms in arriving at their conclusions that their inferences can no longer be accounted for. A smart object may conclude on the basis of very complex algorithms that a user wants to listen to a 1920s jazz tune at a loud volume or wants to order 200 bottles of Chardonnay, but may no longer be able to explain to the user on what basis it has drawn its conclusion. Users may even start experiencing cognitive dissonance, when they believe they want one thing but a smart object tells them they want something else. Using smart objects requires a basic trust in their judgments, and if these judgments conflict with the user's own judgments or intuitions, then the user has to choose whether to rely on herself or on a piece of technology that may or may not know her better than she does herself.

So it seems that we have reached another paradox: the better smart objects become in guessing what we want, the less we may understand them and therefore trust them. Marvin Minsky has put the problem thus: "There's the old paradox of having a very smart slave. If you keep the slave from learning too much, you are limiting its usefulness. But, if you help it to become smarter than you are, then you may not be able to trust it not to make better plans for itself than it does for you." (Minsky 1994, p. 25). The risk is that smart objects will turn out to be either half-witted, resulting in frequent actions against the user's wishes, or are super smart, and attain a degree of autonomy that make them unaccountable for their actions and may result in users having to choose between distrusting the machine or distrusting themselves. In both cases, users end up losing control.

Let us next consider the question whether AmI can be expected to respect only the wishes of their users, and not those of third parties. In principle, I believe, AmI can be designed to focus exclusively on the needs of the user. But in practice, it is not likely for this to happen. First of all, it is likely that future AmI will strongly represent commercial interests, next to the user's interests. Current development of AmI is driven by the idea that it can support new business models, and that it can function as a new way for firms to get information about their customers, reach out to them and sell them goods and services. AmI offers great potential for commercial firms, promising them total market transparency and direct access to consumers. It offers them very direct ways to find out about their customers and to reach them with targeted advertising and sell them new goods and services on the spot. Even better, if smart objects become trusted agents, then firms need no longer just rely on their own arguments, but could rely on the authority of smart objects to convince users to make purchases. Smart objects could become intermediaries between businesses and consumers, using their intelligence to persuade customers to buy products after themselves having been "convinced" by a business. It would be vital for businesses, then, to get to know the personal information represented in smart objects. It would be even better for if they could play a role in determining the needs represented in smart objects. This would require that they could influence the algorithms by which smart objects draw their conclusions. Such influence could already be exerted at the design stage, when technology developers work commercial firms with to support such new business models, or it could be exerted over external networks through to which smart objects connect with businesses.

Smart objects are hence likely to become commercial agents that mix the user's interests with those of businesses that try to sell products. They may end up highlighting those needs of users that have commercial potential and offering commercial solutions to them, while downplaying other needs. Imagine a scenario, 10 years from now, in which you get up for work and your bathroom mirror tells you: "Good morning, George! Don't forget your dentist appointment today. And I must tell you that you really look tired today, as does your wife. You've been working too hard these past couple of months, I have noticed. I've looked into a solution for you to

relieve your stress, and a brief holiday would be the best choice. Based on your preferences, your work schedule and your available budget, I recommend an 8-day holiday to Hawaii next month. I have already checked with your company whether you can take time off, and their AI tells me that you can be missed for a while that month. Sun Travel can offer you this trip at a special price of $900 with a stay in the Hyatt Regency Waikiki, if you approve this trip in the coming ten minutes. I advise you to do this. Make yourself and Susan happy. Please press "yes"." Even more extreme are scenarios based on the concept of "silent commerce" discussed earlier, with smart objects making autonomous purchases. The inventor of this concept, Accenture, gives an example of a Barbie doll that delights children by ordering new clothes with their own pocket money: "Barbie detects the presence of clothing and compares it with her existing wardrobe – after all, how many tennis outfits does a doll need? The toy can buy straight from the manufacturer via the wireless connection... She can be constantly and anonymously shopping, even though the owner might not know it" (Maeder 2002, p. 6). Silent commerce makes corporate dreams come true.

The commercial interests of manufacturers and insurance companies could also easily find their way into smart objects. A smart object may, for example, refuse to engage in actions that may expose the manufacturer to a liability suit, or that is deemed too risky by an insurer, even if the user would want it to perform these actions. Interests of the state and the judiciary could also find their way into smart objects. The state may demand that smart objects cannot be used to violate laws or regulations, and such policies can easily be incorporated into smart objects. For example, a smart car may be designed to refuse to open the door for its driver if he or she has stopped in a no-parking zone. As Jürgen Bohn et al. (2005) argue, such enforced policies in smart objects could make them disloyal to their owners, and they could end up being perceived as patronizing and troublesome. At the very least, they argue, manual override mechanisms should be put in place that enable users to make their own decisions (p. 16).

In many AmI scenarios, also, it is assumed that smart objects have a single user, and that this user is also the owner. However, this may often not be the case. As discussed in the previous sections, many AmI applications are foreseen for organizations, and in this case, the organization (usually meaning the employer) will own the technology, not the users (or employees). The AmI is therefore more likely to operate on the basis of the perceived needs of the organization rather than the needs of the user, and may end up taking away control from the user as a result. In addition, many smart objects will not have a single user but multiple users. This will be the case for the family living room and other communal spaces, as well as collectively used public and private facilities and places like libraries, shops, and railway stations. When there is collective use, smart objects will have to assume some default value, or will have to determine the different needs of all users and then calculate or "negotiate" a compromise value. When, for example, users have different preferences regarding room temperature, a smart heating system will have to calculate some mean value that take all needs into account as well as possible.

In conclusion, AmI has a serious potential to enhance positive freedom through its ability to enhance control over the environment by making it more responsive to one's needs and intentions. However, it also has a strong potential to limit freedom, both in the positive and the negative sense. It has a potential to limit negative freedom because it could confront humans with smart objects that perform autonomous actions against their wishes. Such actions could either result from imperfections in the technology or from the representation in the technology of interests other than those of the user. AmI also has the potential to limit positive freedom, by pretending to know what our needs are and telling us what to believe and decide. When smart objects correctly infer our needs, and inform us of them, they may also enhance positive freedom, by improving our self-understanding and thereby helping us become more autonomous. But as argued, such inferences about our needs will often contain biases and imperfections, and present us with a false image of who we are and what we want, and in such cases they will diminish our autonomy if we trust their judgment. Even if they guess us correctly and we rely on their judgments, it could be argued that we lose positive freedom, because we defer judgment to another intelligent agent. Even if that agent is our obedient slave, if it has the ability to tell us what we want and what we should decide, it is still, in a way, our master.

Privacy

Of all ethical issues that could be raised in connection to Ambient Intelligence, the issue of privacy has by far received the most attention. Proponents and critics of AmI agree that it has a significant potential to violate personal privacy. As Bohn et al. write, "Intelligent fridges, pay-per-use scenarios, and dynamic insurance rates paint a future in which all of our moves, actions, and decisions are recorded by

tireless electronic devices, from the kitchen and living room of our homes to our weekend trips in our cars.'' (2005, p. 9) And Langheinrich observes: ''With a densely populated world of smart and intelligent but invisible communication and computation devices, no single part of our lives will per default be able to seclude itself from digitization. Everything we say, do, or even feel, could be digitized, stored, and retrieved anytime later.'' (2001, p. 280). Critics of AmI have condemned it for its alleged ability to create a Big Brother society in which every human activity is recorded and smart devices even try to probe people's thoughts. Proponents have admitted that privacy issues require the utmost attention in the design of AmI, and that a basic trust that it is protective of privacy is vital for its acceptance by the public. In this section, I will consider the privacy issues that are into play here.

Privacy-relevant features of AmI

Let us first consider whether AmI has any properties that make it different from other computer science domains with respect to privacy. Marc Langheinrich has asked this question in relation to Ubiquitous Computing and has argued that it has four special properties (Langheinrich 2001):

(1) *Ubiquity*. Ubiquitous computing is supposed to be everywhere, and computers will therefore be omnipresent and impact every part of our lives. Because of the pervasive role in our lives that Ubiquitous Computing is supposed to have, its privacy issues may affect us more deeply than those associated with other forms of information technology.
(2) *Invisibility*. In Ubiquitous Computing, computers are supposed to disappear from view. Consequently, its users will not always know they are present, and will not always know what they are doing. If what they are doing is collecting and disseminating personal data, users may often not know this.
(3) *Sensing*. Ubiquitous Computing makes use of sensors that perceive aspects of the environment. These sensors will be increasingly sophisticated, and may in the future allow high quality audio and video feeds from cameras and microphones smaller than buttons. They may also sense emotions, like stress fear and excitement.
(4) *Memory amplification*. Ubiquitous Computing may allow for future applications that ''continuously and unobtrusively record every action, utterance and movement of ourselves and our surroundings, feeding them into a sophisticated back-end system that uses video and speech processing to allow us browsing and searching through our past.'' (p. 279). Ubiquitous Computing has the unique potential to be used to create a rather complete record of someone's past, which has been called a *life-log*.

As argued in section 1 (The Promise of Ambient Intelligence), AmI adds to Ubiquitous Computing the technologies of IUI's and Ubiquitous Communication. These technologies add two properties that are important in relation to privacy:

(5) *Profiling*. Smart objects in AmI contain, construct and use unique profiles of users, including their unique characteristics, preferences, and behavioral patterns.
(6) *Connectedness*. Smart objects have to be able to communicate with other devices, whether local or remote. Ideally, they will be able to form wireless and ad hoc networks with other devices, over which data is exchanged. Unless special safeguards are put in place, personal information may move freely over networks in this kind of architecture.

As Bohn et al. emphasize, it is moreover likely that many AmI devices will have searching capabilities to comb databases for specific pieces of data, notably data of past events.

It should be obvious from this list that Ambient Intelligence is a technology that harbors great risks for privacy, perhaps more so than any other form of information technology. As Bohn et al. observe, ''By virtue of its very definitions, the vision of ambient intelligence has the potential to create an invisible and comprehensive surveillance network, covering an unprecedented share of our public and private life.'' (2005, 9–10). The privacy risks of AmI are so great because of the often highly sensitive types of personal information that are recorded and encoded, the scale on which this information is recorded, and the ease with which it could potentially be disseminated and made available to other parties. Smart devices may record a range of information that goes beyond those of other forms of information technology. They may detect and record actions, events, locations, objects, social interactions, speech an writing, emotions, and bodily states, and they may use these recordings to make inferences about needs, preferences and intentions. They will frequently record their data in a private setting, such as the home and the car, as well as private organizations. And they will often record their data in relation to unique persons, making it part of his or her personal profile or record. Often, for sure, such information will only be temporarily

stored, just so long as it is needed for the smart object to do its work. But the proper operation of many smart objects may require them to build up records, or construct memory databases, and then such information may be stored indefinitely.

Clearly, then, AmI has the potential to penetrate deeply into the personal lives of humans, collecting and disseminating a very wide range of personal data that represent individual behaviors, mental states, and social interactions in private settings with an incredible amount of precision. Like no other technology, AmI could obliterate any notion of personal privacy if left unchecked. Even more so, as Augustin Araya has argued, AmI may end up fundamentally changing one's relationship to the world in the process, by making the whole world into a surveillable object. In an early critique of Ubiquitous Computing, Araya claimed: "Ubiquitous Computing aims not only at satisfying the need for instantaneous access to information, but it also attempts to give instantaneous access to any "thing" including tools, books, and people, transforming them into *surveillable things*." (Araya 1995: 233). Araya has pointed out that such surveillance is not just undertaken by third parties but also by users themselves. Objects will not just be objects anymore, Araya has argued, but will be information structures that can be monitored, and the same will apply to people. AmI thus has the potential to introduce widespread and pervasive surveillance into society, on a much greates scale than seen before, and may in the process fundamentally alter our relationship with the world.

Privacy invasions in AmI

A better understanding of privacy issues in Ambient Intelligence requires that we understand the circumstances under which uses of, or actions by, AmI constitute an invasion or violation of personal privacy. One influential definition of privacy describes it as limited access to personal affairs (Schoeman 1984; Brey 2005). The right to privacy is then the right to control access to one's personal affairs. Invasions of privacy occur when third parties have access to personal information contained in smart objects without a person's knowledge or consent. The networked character of smart objects and the need of smart objects to exchange information with other smart objects or other persons would require a very robust regime of privacy management to avoid such unauthorized access. It may, indeed, be very difficult to devise the technology such that unauthorized access never occurs. Central ideas behind AmI are that computers are ubiquitous, invisible, and proactive. These ideas preclude a scenario in which users constantly have to choose whether or not they authorize smart objects to record data, and whether or not other agents may have access to such data. Such authorizations must therefore be built into the technology. But this means that users will lose control over the authorization process. They may, perhaps, set some privacy parameters on some important smart objects that they use, but in many cases, they will have to trust the preconfigured privacy settings of the technology they use.

Langheinrich has argued that even when humans have a choice to be subjected to privacy-invading smart technology, this choice may often only be theoretical, since choosing to protect one's privacy may come at a high price. Often, the choice may be to use a facility and give away one's privacy, or not to get to use the facility at all. He concludes: "With only one option available, getting consent comes dangerously close to blackmailing. Imagine that in order to enter a public building, you must agree to completely unacceptable practices. Certainly you could always walk away from such a deal, but can you really?" (2001, p. 282). In addition, as has often been observed in discussions of privacy, privacy has now become a tradeable commodity. Commercial firms offer consumer schemes in which consumers get to trade in personal data in exchange for discounts or free goods. Many consumers find this an acceptable practice. It could be argued that technically, such practices do not involve violations of privacy, since authorizations have taken place. Yet, such authorizations are often given on the basis of a very limited understanding of what personal information is collected and how it would or could be used. It is therefore often doubtful that such authorizations are based on informed consent.

In conclusion, AmI presents formidable privacy challenges, that require great efforts in technology development and social policy to meet them. Significant current effort in AmI research goes towards ensuring privacy and security of systems and solve problems of access, authorization and consent. Inherent design features of AmI seem to make total privacy difficult, however, and powerful parties exist (commercial firms, law enforcement) that would have a great interest in having access to its data.

Conclusion

I have argued that Ambient Intelligence represents a powerful new vision for the future information society, that could make human environments more directly controllable and more responsive to human needs. Yet, AmI could also undermine human free-

dom and autonomy by confronting humans with smart objects that perform unwanted actions and make humans dependent on machines for their judgments and decisions. More than other information technologies, AmI could also threaten privacy, making detailed records of one's behaviors, mental states, and social interactions available to others. Great efforts in technology development and social policy will be required to limit these threats to freedom and privacy.

References

E. Aarts and S. Marzano, *The New Everyday. Views on Ambient Intelligence*. 010 Publishers, Rotterdam, 2003.

E. Aarts, R. Harwig and M. Schuurmans. Ambient Intelligence. In P. Denning editor, *The Invisible Future: The Seamless Integration of Technology into Everyday Life*, pp. 235–250. McGraw-Hill, New York, 2001.

Accenture Technology Labs. Seize the Day. The Silent Commerce Imperative (2002). Available at http://www.accenture.com/silentcommerce.

M. Alcañiz and B. Rey. New Technologies for Ambient Intelligence. In Riva et al. (2005).

A. Araya. Questioning Ubiquitous Computing. In *Proceedings of the 1995 ACM 23rd Annual Conference on Computer Science*. ACM Press, 1995.

I. Berlin. Two Concepts of Liberty. In his *Four Essays on Liberty*, pp. 118–172. Oxford University Press, 1979.

J. Bohn, V. Coroama, M. Langheinrich, F. Mattern and M. Rohs. Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing. In W. Weber, J. Rabaey and E. Aarts editors, *Ambient Intelligence*, pp. 5–29. Springer, Berlin, Heidelberg, New York, Tokyo, 2005.

P. Brey. The Importance of Workplace Privacy. In S. Hansson and E. Palm editors, *The Ethics of Workplace Privacy*, pp. 97–118. Peter Lang, Brussels, 2005.

B. de Ruyter. *365 Days Ambient Intelligence in Homelab*. Philips Research. Neroc Publishers, Eindhoven, the Netherlands, 2003. Also at http://www.research.philips.com/technologies/misc/homelab/downloads/homelab_365.pdf.

H. Dreyfus, *What Computers Still Can't Do: A Critique of Artificial Reason*. MIT Press, Cambridge, 1992.

G. Dworkin, *The Theory and Practice of Autonomy*. Cambridge University Press, Cambridge, 1988.

M. Gupta. *Walls With Ears and Brains. The Unobtrusive Intrusion of Ambient Intelligence*. 2002. http://www.eurescom.de/message/messageDec2002/A_bit_beyond.asp.

T. Hill, *Autonomy and Self-Respect*. Cambridge University Press, Cambridge, 1991.

ISTAG. *Scenarios for Ambient Intelligence in 2010*. European Commission, Brussels, 2001. http://www.cordis.lu/ist/istag.html.

M. Langheinrich. Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. In *Lecture Notes In Computer Science; Vol. 2201 Archive. Proceedings of the 3rd international conference on Ubiquitous Computing, Atlanta, Georgia, USA*, pp. 273–291. Springer-Verlag, London, 2001.

T. Maeder. What Barbie Wants, Barbie Gets. *Wired Magazine*, 10(1), January 2002.

M. Maybury and W. Wahlster, *Readings in Intelligent User Interfaces*. Morgan Kaufmann, San Francisco, 1998.

M. Minsky. A Conversation with Marvin Minsky about Agents. *Communications of the ACM*, vol. 37, no. 7, July 1994.

M. Raisinghani, A. Benoit, J. Ding, M. Gomez, K. Gupta, V. Gusila, D. Power and O. Schmedding. Ambient Intelligence: Changing Forms of Human–Computer Interaction and their Social Implications. *Journal of Digital Information*, Vol. 5(4), Article No. 271, 2004.

G. Riva, F. Vatalaro, F. Davide and M. Alcañiz. *Ambient Intelligence. The Evolution of Technology, Communication and Cognition Towards the Future of Human–Computer Interaction. Vol. 6, Emerging Communication*. IOS Press, Amsterdam, 2005. Also online at http://www.vepsy.com/communication/volume6.html.

F. Schoeman, *Philosophical Dimensions of Privacy. An Anthology*. Cambridge University Press, Cambridge, 1984.

J. Searle. Minds, Brains and Programs. *Behavioral and Brain Sciences*, 3(3): 417–457, 1980.

D. Tennenhouse. Proactive Computing. *Communications of the ACM*, 43(5): 43–50, 2000.

W. Weber, J. Rabaey and E. Aarts, *Ambient Intelligence*. Springer, Berlin, Heidelberg, New York, Tokyo, 2005.