Disappearing Computers Everywhere – Living in a World of Smart Everyday Objects[1]

Jürgen Bohn, Vlad Coroamă, Marc Langheinrich, Friedemann Mattern, Michael Rohs
Institute for Pervasive Computing, ETH Zurich, Switzerland

Summary

Still in its infancy, the research area of ubiquitous computing involves integrating tiny microelectronic processors and sensors into everyday objects in order to make them "smart." Smart things can detect their environment, therefore helping users to cope with their tasks in new, intuitive ways. Although many visionary concepts have already been tested out as prototypes in early field trials, the repercussions of such extensive integration of computer technology into our everyday lives are difficult to predict. This article attempts to classify the social, economic, and ethical implications of this development.

1 Brave New World

The increasing miniaturization of computer technology will, in the foreseeable future, result in processors and tiny sensors being integrated into more and more everyday objects, leading to the disappearance of traditional PC input and output media such as keyboards, mice, and screens. Instead, we will communicate directly with our clothes, watches, pens, or furniture (and they will communicate with each other and with other people's objects).

More than 10 years ago, Mark Weiser, a researcher at the XEROX Palo Alto Research Center, foresaw this development, and described it in his influential article "The Computer for the 21st Century" [39]. Weiser coined the term "ubiquitous computing," referring to omnipresent computers that serve people in their everyday lives at home and work, functioning invisibly and unobtrusively in the background with the aim of supporting them in their work and activities, and to a large extent freeing them from tedious routine tasks.

Whereas his ideas sounded rather utopian at the time, today the large-scale use of tiny computerized devices in everyday life seems realistic. The dramatic progress in the miniaturization of computer

[1] An extended German version „Allgegenwart und Verschwinden des Computers – Leben in einer Welt smarter Alltagsdinge" will appear in: Ralf Grötker (Ed.): Privat! Kontrollierte Freiheit in einer vernetzten Welt, Heise-Verlag, 2003.

components and a continuous fall in prices due to new production techniques and technological developments are making possible a multitude of new uses, collectively described as "pervasive computing." Recent technological developments in wireless mobile communications and sensor technology as well as positioning systems and wireless identification systems measuring just a few millimeters [13] are already enabling researchers in development laboratories to realize Weiser's utopia by creating numerous prototypes [32].

The vision of a completely networked future filled with smart everyday objects offers a whole range of fascinating possibilities: It will be virtually impossible to lose things, because they will always know where they are, and will be able to transmit this information to their owner's mobile phone if necessary. With location sensors and communications modules sewn into clothing, children will no longer go astray, even in the busiest of crowds. These tiny communicating computers could also play a valuable role in protecting the environment, for example as ocean sensors the size of plankton that follow shoals of fish or record tectonic plate movements. Another fascinating possibility is that of virtually linking any sort of information to everyday objects, effectively attaching it to them, so that for example an oven could download its operating instructions from the Internet in seconds, printing them out on the home printer, for example.

Even if this all looks at first glance like a cult program for science fiction enthusiasts, it is likely that ubiquitous computing will bring long term consequences for our everyday lives and ethical values that are much more far-reaching than the Internet with all its discussions about spam e-mails, cyber crime, and child pornography ever will. With its orientation towards the public as well as the private, the personal as well as the commercial, ubiquitous computing looks set to accompany us throughout our whole lives, day in and day out. And if Mark Weiser's vision of "invisible computing" actually materializes, we won't even notice any of the underlying technology.

It is not only advocates of a logically consistent technology assessment who suspect that with these technical developments, which will be pushed through largely unnoticed by the general public and will extend quite rapidly into our everyday lives, standards could soon be set for the rest of our lives, with consequences that are not easy to predict.

2 Technology Trends

The driving force behind the continuing technological progress in the field of ubiquitous computing is the long-term trend in microelectronics[2]: Moore's Law [25], drawn up in the late 1960s by Gordon Moore, and which states that the power of microprocessors doubles about every 18 months, has held true with astonishing accuracy and consistency. A similarly high increase in cost-efficiency can be observed for some other technological parameters such as storage capacity and communications bandwidth. To put it another way, prices for microelectronic functionality with an equivalent amount of computing power are falling radically over time. This trend, which will continue for at least 15 years, means that computer processors and storage components will become much more powerful, smaller, and cheaper in the future, so that there will be an almost unlimited supply of them.

Even more important are the results of microsystem technology and nanotechnology. These could lead to tiny sensors, for example, which could record a wide variety of environmental parameters. One interesting development in this regard is radio sensors that can report their readings within a few meters distance without an explicit energy supply – such sensors obtain the necessary energy from the environment or directly from the measuring process itself.

Electronic labels (so-called "smart labels" or RFID tags) also operate without their own energy supply. Depending on their construction, these are less than a square millimeter in area and thinner than a

[2] This section is based on [23].

piece of paper. In some ways, this is a further development of the well-known anti-theft technology involving security gates in department stores. However, this is not just about the binary information “paid/ stolen”; within milliseconds, several hundred characters could be read and written “wirelessly” up to a distance of about two meters [8].

What is interesting about such remote-inquiry electronic markers is that they enable objects to be clearly identified and recognized, and therefore linked in real time to an associated data record held on the Internet or in a remote database. This ultimately means that specific data can be associated with any kind of object. If everyday objects can be uniquely identified from a distance and furnished with information, this opens up application possibilities that go far beyond the original purpose of automated warehousing or supermarkets without cashiers.

Significant advances have also been made in the field of wireless communications. Especially interesting are recent short-range communications technologies that require very little energy, making it possible to produce designs that are much smaller and cheaper than today’s mobile phones. Intensive research is also being carried out on improved options for indicating the position of mobile objects. As well as increased accuracy (currently around ten meters for the GPS system), the aim is also to make the devices smaller. Location determination modules will soon be about the size of a credit card.

If you summarize these technology trends and developments – tiny, cheap processors with integrated sensors and wireless communications capability, attaching information to everyday objects, the remote identification of objects, the precise localization of objects, flexible displays based on polymers, and electronic paper – it becomes clear that the technological basis for a strange new world has been created: everyday objects that are in some respects “smart,” and with which we can even communicate under certain circumstances.

For implementing such communication with things, imagine everyday objects such as furniture, packaged food, medication, clothing, or toys being equipped with an electronic label containing a specific Internet address as digital information. If you can then read this Internet address with a portable device just by pointing it at the object, this device can, independently and with no further assistance from the object in question, access and display the associated information from the Internet via the mobile phone network.

The user has the impression that the object itself has “transmitted” the information, although in fact it has been supplied by the display device via the Internet. The information could be, for example, operating instructions, or cooking instructions for a ready-to-serve meal, or the information leaflet for medication. The details of what is displayed may depend on the “context” – for example, whether the user is a good customer and paid a lot of money for the product, whether he is over 18 years of age, what language he speaks, or his current location, – but also maybe whether he has paid his taxes on time…

The foreseeable technological developments will therefore add an additional new quality to everyday objects – these might be able not only to communicate with people and other “smart” objects, but also to discover where they are, which other objects are in their vicinity, and what has happened to them in the past, for example. Objects and devices could thus behave in a context-sensitive manner and appear to be “smart,” without actually being “intelligent.”

3 Personal Privacy

The fascinating possibilities opened up to us by the recent technical impetus described above are enabling more and more realistic scenarios and trials to take place, even outside research laboratories; for example, in hospitals, family homes, schools, and kindergartens. But at the same time, more and more of the key issues start shifting away from purely technical problems towards questions of a predominantly social or even ethical nature: How are we to use those smart devices in our daily routine? When should they be turned on and off? What should they be allowed to see, feel, or hear? And whom should they tell about it?

Among such questions, privacy is probably the most prominent concern when it comes to judging the effects of a widespread deployment of ubiquitous computing. By virtue of its very definitions, ubiquitous computing has now the potential to create an invisible and comprehensive surveillance network covering an unprecedented share of our public and private life. The following sections try to add a differentiated view on the impact of ubiquitous computing on personal privacy by first examining *why* personal privacy is desirable, describing *when* we feel that it has been violated, and then assessing *how* ubiquitous computing affects all that.

3.1 Motivating Personal Privacy

Along with articles covering privacy aspects, a range of definitions for what actually constitutes privacy are given, the most prominent probably being judge Brandeis' "The right to be left alone" [38] and Alan Westin's "The claim of individuals... to determine for themselves when, how, and to what extent information about them is communicated to others" [42]. These definitions certainly help to illustrate that privacy not only has different goals in different contexts, but also that personal limits for privacy differ according to factors such as geography (e.g., whether we are at home or in a public park), informational access rights (e.g., anti-mask laws in certain states/countries prohibit hiding ones face in public), or expectations and manners (e.g., expecting people not to openly stare at you in public) [22]. Depending on any of these dimensions, individuals can both expect a reasonable level of protection from the prying eyes and ears of their fellow citizens, or be required to disclose certain parts of their own information when necessary by law or custom.

Privacy is often seen as a fundamental requirement for any modern democracy [30]. Only if people can freely choose according to their interests and believes, without fear of repression from their fellow citizens, the necessary plurality of ideas and attitudes can grow that prevent bringing the general public into line by charismatic leaders. Harvard law professor Lawrence Lessig [17] takes this requirement a step further and differentiates between a number of motivations for privacy protection in our present-day laws and norms:

Privacy as Empowerment. Seeing privacy mainly as informational privacy, its aim is to give people the power to control the dissemination and spread of information about themselves. A recent legal discussion surrounding this motivation revolves around the question whether personal information should be seen as a private property (which would entail the rights to sell all or parts of it as the owner sees fit) or as intellectual property (which would entitle the owner to certain inalienable rights, preventing him for example to sell the rights to his name to anybody).

Privacy as Utility. From the data subject's point of view, privacy can be seen as a utility providing more or less effective protection from nuisances such as unsolicited calls or emails. This view probably best follows Brandeis' "The right to be left alone" definition of privacy, where the focus is on reducing the amount of disturbance for the individual.

Privacy as Dignity. Dignity not only entails being free from unsubstantiated suspicions (for example when being the target of a wire tap, where the intrusion is usually not directly perceived as a disturbance), but rather focuses on the *equilibrium* of information available between two people: analogous to having a conversation with a fully dressed person while being naked oneself, any relationship where there is a considerable information imbalance will make it much more difficult for those with less information about the other to keep one's poise.

Privacy as Constraint of Power. Privacy laws and moral norms to that extend can also be seen as a tool for keeping checks and balances on a ruling elite's powers. By limiting information gathering of a certain type, crimes or moral norms pertaining to that type of information cannot be effectively enforced.

Depending on what kind of motivation one assumes for preserving privacy, ubiquitous computing can become the driving factor of changing the reach and impact of privacy protection as it exists today, and create substantially different social landscapes in the future. Depending on which new possibilities ubiquitous computing systems create in the new social landscape, the adjustment of social rules demanded above could be substantially hindered. This is because ubiquitous computing influences two important design parameters relating to privacy: the ability to monitor and the ability to search [17].

3.2 Ubiquitous Computing and Surveillance

Monitoring people and their actions and habits is a human trait as old as humanity itself. In the "good old days", such monitoring would constantly be done within small villages and settlements by our close social peers, who would immediately notice anything out of the ordinary and disseminate it in society. It was this close monitoring that often enough drove people into the big cities, where the sheer number of citizens and their constant mobility effectively put an end to the watchful eyes of the neighbors. Yet with the advent of automated information processing, machines took over the role of the watchers and began to store more and more of our daily routines, not only when they happened to be "out of the ordinary." With ubiquitous computing, monitoring capabilities can obviously be extended far beyond credit-card records, calling logs, and news postings. Not only will the *spatial* scope of such monitoring activities be significantly extended with ubiquitous computing but also their *temporal* coverage will vastly increase: starting from pre-natal-diagnostics data stored on the baby's hospital smart card, to activity feeds in kindergarten and schools, to workplace monitoring and senior citizen's health monitoring.

Such comprehensive monitoring (or: surveillance) techniques create new opportunities for what MIT professor emeritus Gary T. Marx calls *border crossings*: "Central to our acceptance or sense of outrage with respect to surveillance ... are the implications for crossing personal borders." [22]. He goes on to define four such border crossings that form the basis for perceived privacy violation:

Natural Borders. Physical limitations of observations, such as walls and doors, clothing, darkness, but also sealed letters, telephone calls. Even facial expressions can form a natural border against the true feelings of a person.

Social Borders. Expectations about confidentiality for members of certain social roles, such as family members, doctors, or lawyers. This also includes expectations that your colleagues will not read personal fax messages addressed to you, or material that you left lying around the photocopy machine.

Spatial or Temporal Borders. The usual expectations of people that parts of their life, both in time and social space, can remain separated from each other. This would include a wild adolescent time that should not interfere with today's life as a father of four, or different social groups, such as your work colleagues and friends in your favorite bar.

Borders due to Ephemeral or Transitory Effects. This describes what is best known as a "fleeting moment," a spontaneous utterance or action that we hope gets forgotten soon, or old pictures and letters that we put out in our trash. Seeing audio or video recordings of such events later, or observing someone sifting through our trash, will violate our expectations of being able to have information simply pass away unnoticed or forgotten.

Putting ubiquitous computing systems into place will most certainly allow far greater possibilities for such border crossings in our daily routines. Consider the popular vision of a wearable *memory amplifier* [24,28], allowing its wearer to constantly record events of her daily life in a lifetime multimedia diary. While at first sight such a technology promises great help for those of us who tend to forget a lot of small details it also has substantial consequences for our privacy borders stemming from *ephemeral and transitory effects*: Any statement I make during a private conversation could potentially be played back as a high-quality audio and video feed if my conversation partner would give others a peek into her multimedia diary. Even if this information would never get disclosed to others, just the thought of dealing with people who have a perfect memory (and thus would *never* forget anything) will probably have a sizable effect on our interpersonal relationships.

The problem of *spatial and temporal borders* on the other hand is well known from the area of consumer profiles. Profiles are often enough the focus of public concerns, but so far social and legal attitudes have been relatively relaxed about them. Consumer acceptance is also much higher than the often negative news coverage might indicate, mostly because their harm is often perceived as being small (such as unsolicited spam) compared to their advantages (e.g., monetary incentives in the form of discounts or rewards). However, there are well-known risks associated with profiles, and their widespread as the basis for a ubiquitous computing infrastructure will only intensify such problems. Besides the obvious risk of data spills [27], profiles also threaten universal equality, a concept central to many constitutions, basic laws, and human rights, where "all men are created equal." [37]. Even though a thoroughly customized future (using ubiquitous computing) where I only get the information that is relevant to my (very comprehensive) profile holds great promise, the fact that at the same time a large amount of information might be deliberately *withheld* from me because I am not considered a valued recipient of such information, constitutes a severe privacy violation for many people.

Applying ubiquitous computing technology in areas with primarily *social borders* – for example where a close social group interacts only among themselves, such as families [26,41] or co-workers – might seemingly alleviate some of the above concerns. Most participants share already close relationships and tend to know a great deal about each other, without needing a system to compile a profile of their communication partner. Such systems, however, also raise the ante as to what *type* of information they handle. While a communication whiteboard for families may facilitate social bonding between physically and temporally separated members, it also increases the risk for unwanted social border crossings by accidentally allowing Mum to read a message you left for your sister, or a visiting friend to appear in the house activity log even though you told grandma you would spend the weekend alone.

Natural borders, then, might be easiest to respect when designing ubiquitous computing systems. Here, the concept of surveillance is well known and usually fairly straightforward to spot, after all: If others are able to watch your actions behind closed doors, they are most certainly intruding on your privacy. Proponents of wearable computing systems often cite the fact that information could both be gathered and stored *locally* (i.e., on the users belt, or within her shirt) as a turnkey solution for privacy conscious technologists [29]. Border crossings, however, are not only about *who* does something, but *what* is happening. Even though a context-aware wearable system might keep its data to itself, its array of sensors nevertheless probe deep into our personal life, and the things it might find there might easily startle (and trouble!) us, once such systems would start anticipating our future actions and reactions. The feeling of having someone (or something) constantly looking over our shoulder and second guessing us would certainly constitute a natural border crossing for most of us. And the temptation of law enforcement subpoenaing such information not only to determine your physical data (were you at the crime scene?) but also your *intentions* (by assessing the data feed from our body sensors) would certainly motivate legislation that would make the deletion of such information a crime (just as recent laws against cybercrime [4] do this for computer log files).

3.3 The Power of Searches

All these examples serve to show that ubiquitous computing systems, even when installed for the greater good and with the best of intentions, will run a high chance of involuntarily threatening our personal borders that set apart private from public, simply because their monitoring capabilities will facilitate more of the border crossings described above. Whether or not such crossings ultimately occur, given the opportunities created, will to a large extend also depend on the type of *searching* capabilities that such ubiquitous computing systems might offer.

Search technology is traditionally not a particular focus of ubiquitous computing, mainly since its core methods are more likely to be developed in the fields of information retrieval or databases. However, what *will* become relevant in ubiquitous computing is how the chosen architectures will support such search techniques. Chances are high that such technology will be a basic building block of future ubiquitous computing systems, as most of the envisioned applications in the fields of *context-awareness* and *memory augmentation* require just these capabilities. An automated diary collecting 24/7 audio and video-feeds will not be of much use unless being combined with a powerful search and retrieval technology that lets us comb large amounts of data for very specific information. And the ability to combine different information sources, especially large, innocuous ones such as walking patterns or eating habits, is the backbone of any envisioned "smart" system, which must make best use of a large variety of different sensor input to come to decisions that make it appear as if it would *understand* what was happening around us.

Having thus both monitoring and search capabilities at the very core of their architecture, ubiquitous computing system will very likely provide their developers, owners and regulators with a significant tool to drive the future development of privacy concepts in society. Depending on the actual systems that receive large-scale deployment, some of the motivating aspects of privacy as discussed above might become more or less prominent, thus influencing corresponding legal and social norms.

For example, imagine law enforcement having a low-cost ability to search a large number of homes without effort in short time, for example by having all home automation manufacturers build in hooks into their software that would allow police to register certain behavioral patterns and let motion, audio and video sensors report in when they detect a suspicious match. The temptation to try one's luck in order to find a certain suspect might very well lure policymakers, judges and police into giving up today's relatively cumbersome privacy laws, marking privacy as it exists today as a simple residue of inefficient tools that can be abandoned in favor of national security. By motivating privacy instead as a simple *utility* with a bit of *dignity* thrown in, these searches could still be considered privacy-friendly as they would neither disturb those subject to such a search, nor would they report any personal actions that would not fit the registered suspicious behavior.

4 Ubiquitous Computing and the Economy

Although the initial hype surrounding e-commerce has now faded, information technology and the Internet have made lasting changes to the way in which companies do business. One indication of this is terms such as "real-time economy" and "now economy" [33] to describe companies' use of advanced IT systems to obtain extensive real-time information on the location and condition of their entities. This is making information on company resources more accurate and considerably reducing reaction times in unforeseen circumstances.

4.1 Extensive, Ubiquitous Information

Ubiquitous computing technology that offers comprehensive methods of monitoring and extracting information on real-world entities is a natural extension of this "just-in-time trend," and is transforming "new economies" into "now economies" [33] – information on the location and condition of goods, equipment, and manpower being available not only in real time, but also with up to now undreamt-of accuracy. Increased transparency can be a worthwhile investment due to improved inventory management alone. If a company doesn't know the location and condition of its stock, and how long it has been in the warehouse, significant costs are incurred – missed profits, outsized inventories, and the devaluation of goods depreciating in the warehouse are all possible consequences of information lack. The stocktaking required for business or legal reasons also typically requires a considerable amount of effort. Stocktaking is not only expensive; it is inherently error-prone as well.

The use of ubiquitous computing technology such as indoor localization and automatic identification can largely automate this, thereby reducing costs.

If several companies along a supply chain simultaneously use such inventory data in addition to real-time order information, they can achieve additional savings by significantly attenuating the so-called “bullwhip effect” [16]. This effect, often noticed in practice, describes the following phenomenon: although consumer demand for a product remains almost constant over time, small changes in this demand amplify along the supply chain and ultimately result in either excess production (and associated storage costs) or sudden interruptions to supply (and associated lost income). However, the more information transparency there is along the supply chain, the more these undesirable effects can be reduced [15]. Ubiquitous computing technology can therefore lead to a significant reduction in the bullwhip effect, by making comprehensive information available along the supply chain.

The constant monitoring of additional product parameters (such as ambient temperature or acceleration) by tiny wireless sensors represents a further step towards the “now economy.” The business processes made possible by such “smart” goods deliver high added value to customers and suppliers alike [9]. Equipped with communications capabilities, smart goods are able not only to monitor themselves, but also to communicate relevant parameters to the outside world.

An example therefore could be that of chemicals and foodstuffs whose temperature is monitored whilst in transit. If the goods become unusable due to excessive temperatures, they trigger an alarm, or automatically adjust their best-before date. Or they become active and attempt to take corrective action, for example, by controlling the temperature of their container: “As sensors improve and always-on connectivity becomes a reality, products will be able to do something about their condition” [7]. In this way, products acquire a sort of self-consciousness – they perceive their condition, analyze it, and attempt to change their situation if they are dissatisfied with it.

4.2 Shopping – Any Time, Any Place

“See a great sweater on someone walking by? Find out the brand and price, and place an order. Or maybe you'll be wearing the sweater and earning a commission every time someone near you sees and buys.” This vision [7] describes a future, maybe not that far off, in which the boundary between the real world and the world of data has become rather hazy. Most products will have a representation in the data world, to which there is virtually unlimited access via wireless communication technology. People will be able to shop on the move – on the streets, in buses, or whilst chilling out in their favorite bar at night.

The ultimate in shopping may be achieved when all the decision-making is removed from people, and things do this themselves – “humans out of the loop.” The management consultants Accenture have already coined a phrase for this – “silent commerce.” When we think of “autonomous purchasing objects,” it’s not just photocopiers responsible for ordering their own paper, but also, to the public’s amazement, Barbie dolls[3] that delight children (and their parents …) 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” [20].

Until objects are able to do the appropriate shopping themselves, marketing has to use appropriate mechanisms to ensure that humans do it instead. The art of tempting people to buy may well be taken to new extremes by ubiquitous computing technology. Smart products could subtly advertise themselves or use the technique of cross marketing to advertise their “friends.” So a smart refrigerator could, for example, recommend healthy eating tips and recipes for the foodstuffs it contained, and

[3] Apparently, the toy manufacturers Mattel, owners of the brand, were not at all happy about this and sent in the lawyers right away – Accenture’s Web site now refers only to “a doll”, with no mention of Barbie.

build up its consumers' trust by providing information on the origin and contents of these foodstuffs. It could also introduce co-branding measures by issuing reward points every time frozen goods of a particular brand that it recommended were stored in it. And why not pass on details of eating habits (maybe in exchange for extra reward points), thus enabling individual one-to-one marketing?

However, in the future we may not only be gently tempted to buy, and have the ability to shop just about anywhere at any time; we may also *have* to buy non-stop. If you listen to your favorite CD, the record company will debit you a couple of cents. And if you sit on your sofa at home, the dealer gets commission. Sounds absurd? Thanks to ubiquitous computing technology, it is possible that the pay-per-use business model is on the verge of an enormous boom. The digital rights management systems that have recently been in the news are a first step in this direction. These systems make it possible to give customers only limited access to the data they are purchasing – for example, you can only listen the CD you bought before noon, or only ten times in total. Everyday objects equipped with sensors and communications capabilities could add a new dimension to the pay-per-use business model. Almost any object is suitable for pay-per-use leasing rather than outright purchase.

Another business model made possible by ubiquitous computing could be that of highly dynamic, personalized insurance premiums, for example, for automobile insurance. Criteria such as the way the insured person drives, whether they let other people drive, their driving habits, the times of day at which the automobile is used and the areas in which it is parked could determine the premium. "Sporty" driving would not only increase your gasoline bills, but your insurance company would also note this with interest! Even if there were still theoretically the possibility of opting out, drivers who did not wish to pass their details online to their insurer would have to pay a considerably heftier premium, as the insurer's risk would be less easy to quantify. This would effectively limit freedom of choice, particularly for low earners.

4.3 Dynamic Control and the Economy

Economists could also benefit from this new technology. If the history of products is known (i.e. where they were produced, their transportation means and route), more precise and finer control will be possible. Goods could for example independently determine their ecotax rate using the means by which they were transported from their production location to the sales point (truck or railroad). Taxes could also vary depending on the length of the journey, in order to favor regional producers. Other product characteristics would also depend on the product production history. For example, milk could automatically be classed as biological if it came from a suitably accredited source.

Using ubiquitous computing technology and smart products, a wealth of data on real-world processes can be obtained, and processed in information systems. Analyzing data from different sources can have unexpected results that otherwise would not have been discovered. The Economist's "R factor" is a widely known example of this. Since 1992, the magazine has been analyzing articles from selected newspapers and counting how often the word "recession" appears. If it appears less frequently than in the past, this indicates that a boom can be expected; if it appears more frequently, this is interpreted as an indication of an impending recession. Using this method, The Economist was one of the first observers to predict the coming recession at the start of 2001 [5].

Such early indicators also seem to exist in the field of medicine. For quite some time, the spread of flu epidemics has been predicted using centralized sales statistics reported by pharmacies. Ubiquitous computing technology could significantly increase the quality of such extensive data mining – in theory, it could be possible to record in real time not only the sale of medication, but also its actual use. Smart household medicine cabinets or even drug packaging equipped with sensors would transmit this usage information anonymously. In this way, it would be possible to analyze and predict drug usage and requirements as well as the efficiency of health measures or guidelines, to a greater level of detail than ever before.

4.4 The Economy on Autopilot

Despite a whole range of economic advantages, there are also lots of dangers associated with the use of ubiquitous computing in the economy. Obviously the purchase of medication is not the sort of data you would want to pass on to the authorities. But it is also the increasing automation of economically relevant aspects and the exclusion of humans as decision-makers that is giving cause for concern. Under "normal" circumstances, automated control processes increase system stability – machines are certainly much better than humans if they have to devote their whole attention to a particularly boring task. But situations keep cropping up (such as tragic accidents with airplane autopilots) that have not been anticipated in the software and that could have disastrous consequences if they are not directly controlled by humans.

The same applies to the economy. For example, the stock market crash of 1987 was partly caused by newly implemented software [33]. This was designed in such a way that, when a certain pattern appeared in the daily fluctuations of share prices, further shares were released for sale. Since the majority of traders were using the same software, the appearance of this pattern caused a flood of sales, which triggered the crash.

To be as efficient and adaptable as possible, the economy has to be very lean. Under such conditions, which are often only possible thanks to ubiquitous computing technology, unforeseen events can, however, have grave consequences. In the case of supply chain management, for example, the reduction of the bullwhip effect permits a large reduction in storage capacity. However, if all the companies along the delivery chain drastically reduce their stocks, one small unexpected interruption in supply by the weakest member leads to the whole chain grinding to a halt.

In general terms, the automation and acceleration of the economy seems to increase not only the potential for possible savings, but also the associated risk of malfunctions in this type of complex and sensitive system. So it is important that the ubiquitous computing systems implemented are *reliable* and *socially acceptable*.

5 Social Challenges

Life without computers is unimaginable for us today – embedded processors monitor the condition of high-risk patients round the clock, they control central heating in buildings, air conditioning in tunnels, and they safely guide airplanes through take-off and landing.

Just as more and more objects and environments are being equipped with ubiquitous computing technology, the degree of our *dependence* on the correct, reliable functioning of this technology is also increasing. Today, we are still usually able to decide for ourselves on the use of new computer technology (e.g. by manually controlling our central heating or deciding to dispense with a mobile phone and its associated constant accessibility). But in a largely computerized future, it might not be possible to escape from this sort of technologically induced dependence, leading to a number of fundamental social challenges of future ubiquitous computing systems, which we discuss in the following.

5.1 Reliability

The vision of ubiquitous computing describes a system that works completely in the background, discreetly and unobtrusively helping us to carry out our tasks. Since our needs and circumstances can change over time, such a system must be able to adapt itself dynamically to the current situation. One crucial basic requirement of such a system is its *reliability* in the *broadest sense* of the word: Apart from being dependable from a technology-based point of view, a complex and highly dynamic system must remain manageable and controllable. This also requires the ability to be able to predict and to a certain extent to check that the system is behaving correctly.

Manageability. If a multitude of objects become in a certain sense “smart” thanks to embedded processors and wireless communication capabilities and thus start to lead their own lives, this also raises the questions of the adaptability and scalability of the ubiquitous computing services which they implement. Will these services and applications still be able to meet their original demands, even with a massive increase in the number of tiny interacting objects? And, above all, how will we be able to understand and control such a highly dynamic world?

Predictability and Diagnosability. Our lives today are already becoming characterized by a large number of technical infrastructures, such as the phone system, television, and electricity. Things that these ubiquitous infrastructures have in common are the fact that they are easy to use, even for people with no special qualifications, and the way in which they function is easy to predict. For example, if you lift the receiver in a phone booth, you expect to hear a dialing tone. If this doesn't happen, it is immediately evident that the phone is not working properly, or there is a fault. However, this type of *predictability* and intelligibility of system behavior can no longer be taken for granted in typical ubiquitous computing systems. The ideal of the invisible computer hidden away in the background carrying out its work is in direct conflict with this. In a world of ubiquitous computers, there will necessarily be a lot more potential serious faults and incidences of malfunction precisely because we are often unaware of the processes and activities running in the background. In certain situations, however, it is essential to know *what* has gone wrong and *when*. *Diagnosability* is therefore another fundamental demand placed on ubiquitous computing systems [6]. If a failure in equipment used round the clock to monitor a high-risk patient were not noticed within a reasonable time, for example, the patient would be denied life-saving medical care in the event of an emergency.

Dependability. Whilst the trend towards miniaturization offers the ability to equip objects and devices with ubiquitous computing technology, it also leads to a considerable reduction in the resources currently available, due to the dwindling physical space available. Whereas in traditional computer systems the failure of individual components can be compensated for by incorporating redundancy, this type of hardware redundancy is often not possible for tiny devices in a ubiquitous computing world due to the limited space, resources, and energy available. Added to this, users generally only possess a single instance of each type of device (PDA, intelligent watch, digital camera, smart key ring etc.) Despite this, it is extremely desirable for the technical dependability of the ubiquitous computing services on offer that a high degree of robustness and fault tolerance is achieved. This calls for alternative concepts and mechanisms in order to overcome service interruptions and device failures, such as an explicit *diversification* of system functions on different levels of abstraction, for example. Such a diversification can be achieved by providing fully independent ways to carry out the same task, preferably based on disjoint sets of system resources wherever feasible. A communications connection, for instance, can be diversified if the system provides different communications mechanisms in parallel, such as GSM, Bluetooth and wireless LAN.

5.2 Delegation of Control

In order to minimize the need for human intervention in complex, highly dynamic ubiquitous computing systems, new concepts for *delegating control* are necessary – automatic processes should take care of routine tasks in a dependable manner, but also provide mechanisms that account to humans for the work achieved, and support them in monitoring complex control flows. Clarification is needed in this context, particularly relating to the question of decision-making powers in dynamic systems that act largely in an autonomous manner. It is also questionable how far the accountability of automatically executed actions can be guaranteed, and who should take on the responsibility and liability for these.

Accountability. As we have already discussed, many new business models are conceivable with the help of ubiquitous computing technology, such as the short-term leasing of everyday objects. Just imagine leasing each seat we used throughout the day for precisely the time we sat on it. Instead of buying tickets for a concert or for public transport, we would automatically take out a short-term leasing contract for the theater seat or the streetcar, and immediately settle the costs incurred (dependent on the seat type, duration of hire and time of day) by micropayment. This type of short-term leasing could be extended to cover all sorts of other things, such as items of clothing or books, for which we would pay depending on the actual period of use, in other words, on a pay-per-use basis. Consequently, a large number of short-term contracts and micropayments would accumulate over time. Irrespective of technical feasibility, this prompts the question of how, in such a world, we could keep track of the resultant large number of short-term contracts and the countless micropayments, let alone retrospectively check the legitimacy of these transactions. Not only would it be extremely tedious and unrealistic to manually check thousands of transactions, micropayments, and microleases, but it is also questionable to what extent inappropriate financial demands could be identified and rejected, and to what extent legitimate payments could be unambiguously and indisputably allocated to the responsible party. Mechanisms would therefore be needed to help ensure the *accountability* of claims and services.

Responsibility and Liability. If information is attached to "electronically enhanced" objects, in other words physical objects effectively become media, this also raises the question of who can or should determine their content. If, for example, ready-to-serve meals contained an electronic label, could a consumer protection institute map this label's number using its own electronic directory onto information other than that which the producer intended (for example, to warn of allergies to the ingredients)? To put this in more general terms: if objects are equipped with information or a means of identification that enables a personal digital assistant, maybe located in a pair of spectacles, to explain the world ("Computer, what's that?"), can real-world objects then be interpreted by the manufacturer of the smart spectacles in any way he likes? Even if the question of accountability can be resolved, clarifying the *responsibility* and *liability* for ubiquitous computing systems will still be a challenge to keep lawyers, amongst others, scratching their heads for quite a while.

Decision-Making Powers. It is a declared aim of intelligent environments and "smart" objects in ubiquitous computing to improve people's quality of life. In order to do this, new methods and services are being provided that unobtrusively support people in their everyday lives, whilst at the same time shielding them from the complexities of a world full of technology. But this route treads a fine line between inspiration and frustration, between obliging helpfulness and pig-headed patronization, and also presents a challenge to researchers [31]. For example, when should an intelligent device obey human orders, and when should it follow its own "convictions?" Imagine that your vehicle prevented you from opening its doors because you had stopped in a no-parking zone. What if you were in an emergency situation, had stopped in the no-waiting area outside a hospital entrance because there were no parking spaces available, and your "smart" car prevented you from getting out? In such situations, some sort of manual emergency override mechanisms would seem appropriate, giving users full *decision-making powers* (and also responsibility) to make the appropriate decisions.

Maintaining the Balance of Power. There is also the question of the general balance of power in a world full of ubiquitous computers, from a bird's-eye point of view. Smart products will certainly be used to tie customers more closely to traders by recommending they purchase other goods produced by that same trader, for example. So if products provide information about themselves, this raises the question of who guarantees the objectivity and accuracy of the statements that are made. In a certain sense, objects are becoming media representing a particular "ideology" (e.g. that of the product's manufacturer, or the politically motivated opinion of a consumer protection organization). Who should control these new "media"? Let's take the case of a smart toy that finds its way into a child's room. Who decides what the smart talking doll tells the children? Could the children become ideologically polarized? There is also the risk that the doll could influence the education and the shaping of the children's opinions, without the parents being fully aware of this. And if the doll starts begging for new clothes from TV advertisements, this could stimulate the children's commercial appetite. If the manufacturer also uses the doll to obtain information on the children's play habits and their other toys, he is in a position to target advertising towards an individual person or household.

It is fascinating to consider to what extent our future living conditions could be controlled, both economically and ideologically, by the manufacturers and operators of smart products, and in what way a possible imbalance of power could be transformed into a *balance of power*.

5.3 Social Compatibility

Another fundamental challenge for ubiquitous computing systems is their social compatibility. If we, as humans, want to be capable of participating in highly dynamic systems, their parameters will have to be adjusted accordingly. System behavior relating to particular aspects should retain a certain inertia, allowing humans to adjust to changes. On the other hand, it should also be taken into account that a ubiquitous infrastructure from which, under certain circumstances, people cannot escape, should also meet the needs and requirements of as broad a section of society as possible.

Sustainability. People do not feel at ease in highly dynamic environments, and there is a lot of data and information in everyday life that remains valid for quite a long period of time, e.g. food prices in our favorite supermarket, or public transport prices. It is the *sustainability* of information that permits us to use acquired knowledge and prior experiences to cope with future situations and tasks. This raises the question of how far people can still cope in an over-reactive world of ubiquitous computers that has lost an element of inertia. In a highly dynamic world, the sustainability of knowledge risks being lost – an experience that was valid and useful one minute could become obsolete and unusable the next. A move towards highly dynamic systems could, therefore, have serious implications, such as the loss or the accelerated devaluation of long-term experiences, which could, in the long term, contribute to an increased uncertainty and lack of direction for people in society.

Fairness. As mentioned above, ubiquitous computing technology can contribute to the efficient one-to-one marketing and cross selling of products by use of personalized direct advertising. This would enable sellers to evaluate and categorize their customers much more precisely. One possible consequence of this could be that tailor-made offers will, in the future, increase traders' profits without benefiting customers. If manufacturers and traders are able to precisely evaluate the consumption behavior of their customers and, leading on from this, present individual customers with individual offers, these customers will quickly lose their overview of different price categories and special offers. At any rate, the right to equal treatment would be detrimentally affected, which also raises the question of the *fairness* of such ubiquitous computing systems.

David Lyon, Professor of Sociology at Queen's University in Canada, calls this process "social sorting" – "Categorizing persons and groups in ways that appear to be accurate and scientific, but which in many ways accentuate difference and reinforce existing inequalities" [19]. If customers get the impression that ubiquitous computing technology is being used to take them for a ride, they may feel a sense of impotence. In any case, this example raises an ethical problem. There is a need to clarify the extent to which the dependency of customers induced by ubiquitous computing technology should be exploited for economic purposes.

Universal Access. Today, new devices and equipment are often developed with a particular target group in mind from the design stage. This can result in people who are less technically knowledgeable being negatively disposed to such products right from the start, or even being unable to use them at all. For example, older people often have the problem of not being able to read small screens or use keypads because they are much too small and difficult to read [10]. But this gives ubiquitous computing the opportunity to include marginal and fringe groups in technological progress. Elderly and physically disabled people, in particular, could benefit from ubiquitous computing, for example with electronic "memory aids," reading aids and navigation systems [21].

The challenge of *universal access* to ubiquitous computing systems is desirable on moral and ethical grounds. The use of ubiquitous computing should be accessible to as many levels and groups in society as possible, and could help to integrate marginal groups (at least technologically). What is more, such an effort may also require that the needs of minority groups and marginal groups are already considered at the design stage, paving the way for a *universal design* [34].

5.4 Acceptance

In this section, we have used a variety of examples to illustrate a range of potential problematic consequences that ubiquitous computing may have on our society, and have derived from these a number of broad demands placed on ubiquitous computing systems. The justification of some of these demands may at first sight appear to be less obvious than traditional issues, such as the issue of privacy examined above. But they are no less important. These are questions of fundamental importance that may ultimately even have a decisive influence on the large-scale acceptance of ubiquitous computing technology and its ability to assert itself. If insufficient attention is given to the challenges posed by ubiquitous computing systems, there is a risk that the negative side effects will overshadow the envisaged benefits of ubiquitous computing.

This could finally lead to users losing their trust and not wanting anything to do with the merits of ubiquitous computing. As a result, this could also mean that the systems developed would either not be used by the general public at all, or that they would be implemented and operated against their will, thus aggravating existing *problems of acceptance*.

6 Criticisms of Ubiquitous Computing

Whereas the somewhat spectacular consequences of ubiquitous computing on the economy and society have scarcely featured in public debate, more mundane questions such as the possible effects of the associated technology on the environment have attracted attention.

The vision of lots of everyday objects and wearable “information appliances” wirelessly communicating with each other does in fact give cause for concern due to the health risks relating to electromagnetic radiation, which are still not fully understood. Because of limited resources and the short communications distances involved, as well as the fact that “changing batteries” in everyday objects would be unreasonable, the radiation in such cases will be orders of magnitude weaker than for today’s mobile phones.

The influence that large-scale use of ubiquitous computing technology would have on environmental issues such as raw material consumption, energy consumption, and disposal is difficult to predict, not least because changing lifestyles, more dynamic business cycles and other consumer habits resulting from the new technology will affect these parameters. For example, if all supermarket goods were equipped with smart labels in the future, billions of these tiny and individually quite harmless chips would end up in the household garbage. On the other hand, the remote identification capability provided by smart labels would enable information on products to be available throughout their entire lives, permitting the materials in waste products to be efficiently identified and separated.

Of course environmental impact plays an important role in assessing a technology that could permanently influence the lives of future generations. However, the far-reaching economic and social implications of ubiquitous computing addressed in the previous sections appear to be more serious. In this respect, it is no surprise that ubiquitous computing has sometimes been viewed very critically by the arts and social sciences as well as by the media.

The criticisms voiced in this respect can be divided into three broad categories:

- Criticisms relating to the *vision* and *aims* of ubiquitous computing, particularly with regard to its all-embracing nature for the objects and people affected, its spatial expansion, and its temporal permanence;

- Concerns about negative consequences and damaging side effects of the *promises* of ubiquitous computing, which transform the technology into a *threat*;
- Concerns regarding the nature of the changes in the relationship between man and the world that ubiquitous computing entails.

We will consider these aspects in more detail below, and attempt to identify some of the implications mentioned in previous sections in the explicit points of criticism.

6.1 Visions and Aims – A Totalitarian Technology?

Critics see ubiquitous computing as "an attempt at a violent technological penetration of everyday life" [3], as the "feverish dream of spooks and spies – to plant a 'bug' in every object" [35] or even as "a project that aims at totality and, of course, verges on the totalitarian" [2]. Why is it that ubiquitous computing attracts such intense criticism?

Far-Reaching Implications. One possible answer to this question has to do with the vision itself. Its explicitly declared aim is to make a revolutionary change to everyday life that will have a fundamental impact on *all* aspects of the existence of *every* person in our already mechanized society. The vision aims at pervading the everyday environment with information technology, through which "each person is continually interacting with hundreds of nearby wirelessly interconnected computers" [3]. Whereas in other areas of information technology changing everyday life in our society was not an explicit goal, but rather a resultant side effect, the vision of ubiquitous computing expressly proposes transforming society by fully computerizing it. According to Adamowsky [2], this transformation ultimately applies to all objects and living beings. She claims that for this reason, ubiquitous computing appears to be a research paradigm that aims at "totality" and "verges on the totalitarian." In the vision formulated by Mark Weiser, every object, place, and living being is in fact affected, leaving individuals with no choice of whether to take part or opt out.

A Vagueness of Vision. Many critics [2,3,18] argue that the proposed scenarios seem extremely vague, bearing in mind the enormous research effort required to implement them and the scope of the envisaged objective. The world is to be made "smart somehow or other," without this "somehow or other" being further specified. Although technological advances such as miniaturization, increasing computing power, and wireless connectivity open up the possibility of new applications, it is not yet clear how these possibilities are actually going to be put into practice.

"Everything will be connected to everything else," but "no one has any idea what all those connections will mean" [18]. There is a gap between technical feasibility and our ability to use it in a beneficial way, or even to suitably assess its potential. John Thackara describes this divergence between increasing technical feasibility and decreasing subjectively perceived benefit as the *innovation dilemma* – we may know *how* we can create incredible things, but we don't know *what* needs they are supposed to meet. He argues that we find it hard to think about that question and are "brilliant on means, but pretty hopeless when it comes to ends" [36].

In order to counter this criticism, it is important to develop a more concrete vision of ubiquitous computing centered on aims that seem attractive, credible, and realistic.

6.2 Promises and Threats

Although the social effects of ubiquitous computing are still not clear, various critics have tried to identify potential negative consequences and damaging side effects of the promises of ubiquitous computing, which could transform the technology into a threat.

The Risk of Monitoring and the Loss of Privacy. It is not surprising that the most immediate fear associated with ubiquitous computing is that its mechanisms will be misused to enable efficient, comprehensive, and universal surveillance, which could lead to a reduction in or complete loss of privacy (see also section 3). To quote Lucky [18]: “The old sayings that ‘the walls have ears’ and ‘if these walls could talk’ have become the disturbing reality. The world is filled with all-knowing, all-reporting things.” Industry is fully aware of the problem of such an image of ubiquitous computing technology. Whilst on the one hand the product that has been purchased can be transformed into a marketing tool by providing information on itself or similar products and collecting and automatically reporting usage information, it could, on the other hand, appear at the same time to be a monitoring tool. “A very cautious approach is needed [...] with this kind of monitoring otherwise newspaper headlines such as ‘Spy in the Kitchen’ would soon appear, killing the intelligent appliance before it takes off” [14].

False Promises. Winner [43] argues that ubiquitous computing raises false expectations when it promises to simplify our lives, help us save time, and relieve us of laborious tasks. For him, this is an assertion that has been constantly repeated throughout the twentieth century by the consumer goods industry. He quotes anthropological studies on employees in Silicon Valley showing that they lead an extremely busy, complex, carefully balanced, and exhausting existence in which the traditional borders between work and leisure time have disintegrated. He believes that adding “smart machines” everywhere in built environment in such a situation would not help to overcome the existing pattern of hurry, rush, stress, and separation from other people. In his opinion, using ubiquitous computing technology would not lead to more leisure time or a more relaxed lifestyle, but would simply permit people to carry out their activities more effectively. Stress levels would remain the same, it’s just that more could be done with the same effort, since activities could be better coordinated and would individually require less effort.

Loss of Control. When designing ubiquitous computing systems, one important task is to give users a feeling of control over their environment and a sense of the “loyalty” of the objects contained in this environment. Thanks to new technical possibilities (allied to appropriate legal conditions) it is conceivable that automobiles or other products, as components of a ubiquitous computing network, would no longer feel completely “loyal” to their users, and would instead enforce the guidelines of insurance companies, manufacturers, or the judiciary.

Networked everyday objects embedded in a ubiquitous computing system lose part of their autonomy and, with this, exhibit an increased dependence on the infrastructure. For users, this reduces the “object constancy” of the objects that surround them, as the example of electronic books made from smart paper shows: reading such a book may presuppose a regular connection to a server (license server, accounts server etc.). Because of this, it appears to be more error-prone and less autonomous than a “normal” book, which can always be read, whereas the electronic one can only be read if the infrastructure is functioning.

The Risk of a New Digital Divide. When talking of the digital divide, we are referring to the differing abilities of different sections of the population to take part in the information society, in particular to make effective use of the information and communications opportunities provided by the Internet. Whilst there is currently no agreement over whether the digital divide will widen or narrow in the future, we can safely assume that it will take on a new quality within the context of ubiquitous computing.

If things become “smart” and offer information on themselves and other objects, they also become new media, thus creating new information opportunities. Having more information opportunities would not necessarily mean more justice or freedom, because the potential dependencies and opportunities for manipulation would be so numerous they would overwhelm individuals.

In the case of smart products, manufacturers’ interests will doubtless play an important role in designing the “information aspect” for each of these products. Manufacturers who attach information to things and can use objects as information channels also simultaneously gain the ability to define the reality of the product user. Whether we can afford independent and “objective” information, or whether we are given the world view of a manufacturer by his products, without being fully aware of this, could depend on the size of our wallets. Cooperating objects as new media could give manufacturers a very precise picture of each household, forming the basis for customized offers and information. In future it will be even more difficult than it is now for individuals to assess the trustworthiness of information or its source. Information that was uncritical or sponsored by advertisers and therefore one-sided could be available free of charge, whilst independent, high-quality information would cost money. Since ubiquitous computing is not just about information itself, but is inherently linked with real-world objects, this could easily lead to the digital divide becoming a real rift in society.

6.3 Changes in the Relationship between Man and the World

Philosophical analyses of ubiquitous computing examine its effects on man's relationship to the world. Araya [3] thinks that ubiquitous computing would fundamentally change the environment in which we live. He believes that the physical environment would become like an extension of our own body, whilst ubiquitous computing would extend our nervous system by means of artificial sensors. The environment would become a "subservient artifact" [3]: "By this weaving of extensions of ourselves into the surroundings, significant parts of the environment lose important aspects of their otherness and the environment as a whole tends to become more and more a subservient 'artifact'. This artifact, which the world immediately surrounding us becomes, is almost entirely 'us' rather than 'other'. In this sense, the surrounding world has almost disappeared." In this context, Adamowsky raises the question of whether we are really ready to "live without an outside" [2]. In her opinion, the "outside" is going to disappear and we will live in "placements" – equivalents of particular aspects of the real world in the digital world, implemented in the form of models, simulations, and virtual counterparts. Our inability to handle the physical world in a flexible enough way will force us to replace it by these digital surrogates, leading to a transformation, dislocation, substitution, and the loss of fundamental properties relating to the world.

6.4 Implications of the Criticism

What is plain from the criticisms presented here is the need for public debate on the aims and ideas of ubiquitous computing. Until such a debate takes place, there is the danger that ubiquitous computing will be misinterpreted, and therefore may provoke somewhat irrational reservations and fears. One example of this is the fundamental paradigm of ubiquitous computing, namely that computers disappear from the user's consciousness and recede into the background. This is seen by some critics as an attempt to have ubiquitous computing infiltrate everyday life unnoticed by the masses, in order to circumvent any possible social resistance. For Araya [3], this view is supported by a quote from Mark Weiser which, taken in isolation, can be misunderstood: "The most profound revolutions are not the ones trumpeted by pundits, but those that sneak in when we are not looking" [40]. A wide debate about ubiquitous computing could be used as an opportunity to steer the development process in the right direction, namely to constructively use the enormous technical potential at our disposal in a way that would advance society.

7 Brave New World?

Using ubiquitous computing systems in the real world will, in many cases, have consequences that reach far beyond the obvious technical repercussions. Whether these consequences are to do with the protection of personal data, the implications for the macroeconomy, or social acceptance, developers of ubiquitous computing systems can profit greatly from a careful evaluation of the consequences of such technology within the framework of established concepts from the fields of sociology, economics, and jurisprudence.

Although predicting the future is often difficult, the above discussion allows us to guess at a few of the possible implications of wide-scale use of ubiquitous computing: social values and motives will change; personal borders will be violated by new surveillance and search technology; new business models will increase profits, possibly at the expense of safety margins; the balance of political and economic power will shift; economic development will accelerate and initiate long-term changes in our social values; and, not least, there is the danger that we will lose confidence in our environment, thus fundamentally changing our attitude to the world that surrounds us.

Bibliography

1 ABOWD, GREGORY D., BARRY BRUMITT and STEVEN SHAFER (Eds.): *Proceedings of Ubicomp 2001*, Atlanta GA, USA, September 2001. Springer-Verlag.

2 ADAMOWSKY, NATASCHA: *Kulturelle Relevanz. Ladenburger Diskurs „Ubiquitous Computing"*, February 2000. Available at: www.inf.ethz.ch/vs/events/slides/adamowldbg.pdf.

3 ARAYA, AGUSTIN A.: *Questioning Ubiquitous Computing*. In: Proceedings of the 1995 ACM 23rd Annual Conference on Computer Science. ACM Press, 1995. Available at: doi.acm.org/10.1145/259526.259560.

4 COUNCIL OF EUROPE: *Convention on Cybercrime*. Available at: conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm, November 2001.

5 *Rrrrrrrrecession?* The Economist, 361(8203), January 2001.

6 ESTRIN, DEBORAH, DAVID CULLER, KRIS PISTER and GAURAV SUKHATME: C*onnecting the Physical World with Pervasive Networks*. IEEE Pervasive Computing – Mobile and Ubiquitous Systems, 1(1):59-69, January 2002.

7 FERGUSON, GLOVER T.: *Have Your Objects Call My Objects*. Harvard Business Review, 80(6):138-144, June 2002.

8 FINKENZELLER, KLAUS: *RFID-Handbook*. John Wiley & Sons, 2nd ed., 2003.

9 FLEISCH, ELGAR: *Von der Vernetzung von Unternehmen zur Vernutzung von Dingen*. In: SCHÖGEL, MARCUS, TORSTEN TOMCZAK and CHRISTIAN BELZ (Eds.): Roadm@p to E-Business – Wie Unternehmen das Internet erfolgreich nutzen, pages 124-135. Thexis, St. Gallen, 2002.

10 GONÇALVES, DANIEL J.: *Ubiquitous Computing and AI Towards an Inclusive Society*. In: HELLER, RACHELLE [12], pages 37-40. See also: virtual.inesc.pt/wuauc01/.

11 GRUNWALD, ARMIN and STEPHAN SAUPE (Ed.): *Ethik in der Technikgestaltung – Praktische Relevanz und Legitimation*. Springer-Verlag, 1999.

12 HELLER, RACHELLE (Ed.): Proceedings of the 2001 EC/NSF Workshop on Universal Accessibility of Ubiquitous Computing: Providing for the Elderly, Alcácer do Sal, Portugal, May 2001. ACM Press. See also: virtual.inesc.pt/wuauc01/.

13 HITACHI, LTD.: *The mu-Chip*. Available at: www.hitachi.co.jp/Prod/mu-chip/.

14 IBM GLOBAL SERVICES: Transforming the appliance industry – Switching on revenue streams in services. White Paper, 2001.

15 JOSHI, YOGESH V.: Information Visibility and its Effect on Supply Chain Dynamics. Master's Thesis, MIT, June 2000.

16 LEE, HAU L., V. PADMANABHAN and SEUNGJIN WHANG: *The Bullwhip Effect in Supply Chains*. MIT Sloan Management Review, 38(3):93-102, spring 1997.

17 LESSIG, LAWRENCE: *Code and Other Laws of Cyberspace*. Basic Books, New York NY, 1999.

18 LUCKY, ROBERT: *Everything will be connected to everything else*. Connections. IEEE Spectrum, March 1999. Available at: www.argreenhouse.com/papers/rlucky/spectrum/connect.shtml.

19 LYON, DAVID: *Facing the Future: Seeking Ethics for Everyday Surveillance*. Ethics and Information Technology, 3(3):171-180, July 2001.

20 MAEDER, THOMAS: *What Barbie Wants, Barbie Gets*. Wired Magazine, 10(1), January 2002.

21 MAKRIS, PANTELIS: *Accessibility of Ubiquitous Computing: Providing for the Elderly*. 2001 EC/NSF Workshop on Universal Accessibility of Ubiquitous Computing: Providing for the Elderly, May 2001. Available at: virtual.inesc.pt/wuauc01/procs/pdfs/makris_final.pdf.

22 MARX, GARY T.: *Murky Conceptual Waters: The Public and the Private*. Ethics and Information Technology, 3(3):157-169, July 2001.

23 MATTERN, FRIEDEMANN: *Ubiquitous Computing: Scenarios for an informatized world.* In: ZERDICK, AXEL et al. [44].

24 MAYO, ROBERT N.: *The Factoids Project*. Available at: www.research.compaq.com/wrl/techreports/abstracts/ TN-60.html.

25 MOORE, GORDON E.: *Cramming more components onto integrated circuits*. Electronics, 38:114-117, April 1965.

26 NAGEL, KRISTINE S., CORY D. KIDD, THOMAS O'CONNELL, ANIND DAY and GREGORY D. ABOWD: *Family Intercom: Developing a Context-Aware Audio Communication System*. In: ABOWD, GREGORY D. et al. [1], pages 176-183.

27 O'HARROW JR, ROBERT: *Prozac Maker Reveals Patient E-Mail Addresses*. The Washington Post, July 2001.

28 RHODES, BRADLEY: *The Wearable Remembrance Agent: A System for Augmented Memory*. Personal Technologies Journal. Special Issue on Wearable Computing, 1:218-224, January 1997.

29 RHODES, BRADLEY, NELSON MINAR and JOSH WEAVER: *Wearable Computing Meets Ubiquitous Computing – Reaping the Best of Both Worlds*. In: Proceedings of the Third International Symposium on Wearable Computers (ISWC '99), pages 141-149, San Francisco CA, October 1999.

30 ROTENBERG, MARK: *Testimony and Statement for the Record*. Hearing on Privacy in the Commercial World before the Subcommittee on Commerce, Trade, and Consumer Protection, U.S. House of Representatives, March 2001. Available at: www.epic.org/privacy/testimony_0301.html.

31 SATYANARAYANAN, MAHADEV: *Pervasive Computing: Vision and Challenges*. IEEE Personal Communications, 8(4):10-17, August 2001.

32 SATYANARAYANAN, MAHADEV: *A Catalyst for Mobile and Ubiquitous Computing*. IEEE Pervasive Computing Magazine, 1(1):2-5, January 2002.

33 SIEGELE, LUDWIG: *How about now? A survey of the real-time economy*. The Economist, 362(8257):3-18, January 2002.

34 STEPHANIDIS, CONSTANTINE: *Towards Universal Access in the Information Society*. 2001 EC/NSF Workshop on Universal Accessibility of Ubiquitous Computing: Providing for the Elderly, May 2001. Available at: virtual.inesc.pt/wuauc01/procs/pdfs/stephanidis_final.pdf.

35 TALBOTT, STEVE: *The Trouble With Ubiquitous Technology Pushers, or: Why We'd Be Better Off without the MIT Media Lab.* NetFuture: Technology and Human Responsibility, January 2000. Available at: www.netfuture.org/2000/Jan0600_100.html#3.

36 THACKARA, JOHN: *The design challenge of pervasive computing*. Interactions, 8(3):46-52, May 2001. Available at: doi.acm.org/10.1145/369825.369832.

37 UNITED STATES OF AMERICA: *The Declaration of Independence and the Constitution of the United States.* August 1998.

38 WARREN, SAMUEL and LOUIS BRANDEIS: *The Right to Privacy*. Harvard Law Review, 4(1):193-220, December 1890.

39 WEISER, MARK: *The Computer for the 21st Century*. Scientific American, 265(3):94-104, September 1991.

40 WEISER, MARK: *Ubiquitous Computing*. IEEE Computer, 26(10):71-72, October 1993.

41 WESTERLUND, BO, SINNA LINDQUIST and YNGVE SUNDBLAD: *Cooperative Design of Communication Support for and with Families in Stockholm*, September 2001. Available at: interliving.kth.se/papers.html.

42 WESTIN, ALAN F.: *Privacy and Freedom*. Atheneum, New York NY, 1967.

43 WINNER, LANGDON: *The Voluntary Complexity Movement*. NetFuture: Technology and Human Responsibility, September 1999. Available at: www.netfuture.org/1999/Sep1499_94.html#3.

44 ZERDICK, AXEL, ARNOLD PICOT, KLAUS SCHRAPE, JEAN-CLAUDE BURGELMAN and ROGER SILVERSTONE (Eds.): E-Merging Media. Springer-Verlag, 2003.