

Ethical Issues in Ubiquitous Computing—Three Technology Assessment Studies Revisited

Lorenz M. Hilty

Abstract This paper discusses ethical issues in ubiquitous (or pervasive) computing from the perspective of the general discourse on ethics in computing, which started in the 1970s, two decades before the “ubicom” vision emerged. The IFIP “Human Choice and Computers” (HCC) conferences are used as points of reference for the general computing ethics discourse, and three technology assessment projects related to the ubicom vision serve as a (nonrepresentative) sample of documents from the discussion of ethical issues in a ubicom world. Revisiting these studies from the general computing ethics point of view shows that the basic issues have persisted, but ubicom has added new aspects that were not anticipated in the earlier discourse.

Keywords Ubiquitous computing · Ethics · Autonomy · Responsibility · Sustainability · Justice

1 Introduction

The terms “ubiquitous computing” (or “ubicom” for short), “pervasive computing,” “ambient intelligence,” and “the Internet of Things” refer to technological visions that share one basic idea: to make computing resources available anytime and anywhere, freeing the user from the constraint of interacting with ICT devices

L.M. Hilty (✉)

Department of Informatics, University of Zürich, Zurich, Switzerland
e-mail: hilty@ifi.uzh.ch

L.M. Hilty

Technology and Society Laboratory, Empa, Swiss Federal Laboratories for Materials Science and Technology, St. Gallen, Switzerland

L.M. Hilty

Centre for Sustainable Communications (CESC), KTH Royal Institute of Technology, Stockholm, Sweden

© Springer International Publishing Switzerland 2015

K. Kinder-Kurlanda and C. Ehrwein Nihan (eds.), *Ubiquitous Computing in the Workplace*, Advances in Intelligent Systems and Computing 333,
DOI 10.1007/978-3-319-13452-9_4

explicitly via keyboards and screens. This is possible by invisibly embedding computational devices in everyday objects and equipping them with sensors that enable them to collect data without the user's active intervention or even awareness.

This vision has partly become a reality during the last two decades through the continued miniaturization of ICT devices, the use of positioning systems making devices aware of their location, and the growth of networks for wireless or mobile communication. Ubiquity of ICT can even be understood at a global scale today, given the success and impact of the mobile phone particularly in the poor and heavily populated regions of the globe. However, some aspects of the ubicomp vision have not been realized (yet)—for example, we are still using screens to interact with smartphones and many other ICT devices. Conversely, technologies have emerged that had not been anticipated in the ubicomp vision, such as the availability of drones carrying cameras and wireless communication devices that are even affordable for private users.

This essay aims to identify the main ethical issues emerging from the vision and practice of ubiquitous computing. If we assume that an “applied ethics of *ubiquitous* computing” is different from an “applied ethics of computing,” there must be ethical issues specifically connected to the ubicomp vision and practice. Hence, the precise question I am trying to answer in this essay is, “What are the *specific* ethical issues in ubiquitous computing, viewed against the background of the (general) ethics of computing?”

The method for answering this question consists of three steps:

1. Identifying the main ethical issues that have been discussed in ethics of computing since the discourse emerged in the 1970s. This will be done by taking the discourse documented in IFIP proceedings as a reference.
2. Identifying ethical issues emerging from the ubicomp discourse, which emerged around the year 2000. This will be done by evaluating three technology assessment studies related to ubiquitous computing.
3. Classifying these issues either as special cases of preexisting more general issues or as new issues which have not been discussed before.

The scope of this work will be limited by focusing on three technology assessment studies from which the ubicomp ethical issues are derived. The sequence of these three studies, selected from the studies published by the Swiss Centre for Technology Assessment (TA-SWISS), starts with possibly the first technology assessment study on ubiquitous computing ever conducted (the project started in 2002) and ends with one of the most recent ones (published in 2012). Taking this sequence as *pars pro toto* for the development of the discourse on implications of ubiquitous computing is obviously a limitation of the current analysis. However, any wider-ranging approach would go beyond the scope of this short essay.

2 Materials and Method

Historically, the discourse on ethics of computing has been initiated and constantly promoted at the international level by IFIP TC9, IFIP's Technical Committee on ICT and Society. IFIP, the International Federation for Information Processing, was founded in 1960 under the auspices of UNESCO as an umbrella organization of the national computer societies. IFIP TC9 has continuously inspired, monitored, and framed the development of the national ethics guidelines and codes of conduct for computer professionals in the national member societies [3].

The work of IFIP TC9 can therefore be used as a reference for the development of the ethical discourse in computing. Instead of digging into the historical details of the development of ethics codes and guidelines, the following analysis will rather take a "helicopter view" and look at the broader discourse documented in the proceedings of the "Human Choice and Computers (HCC)" conference series, IFIP TC9's main conference. The analysis will rely on a recent lexicometric discourse analysis of the HCC proceedings from 1974 to 2012 [2, 4–6, 8, 11, 25, 26, 28, 29] conducted by Lignovskaya [24]. By providing the wider context in which ethical issues in computing have emerged over four decades, the HCC proceedings are an invaluable source of understanding of today's ethical concerns in computing.

There is an important structural difference between the general computing discourse and the ubicomp discourse: While the former emerged in the 1970s when computers had already begun to change everyday reality (in particular in the workplace), the ubicomp discourse started *before* ubicomp became reality. Even today, essential aspects of ubicomp are far from common. Ethical issues of ubicomp are therefore, at least in part, associated with *prospective* applications of computing, not necessarily only with applications existing today.

The public discourse on potential positive and negative impacts of prospective technological applications is often initiated and driven by institutions of *Technology Assessment (TA)*. TA is the study and evaluation of new technologies that are relevant for society and have ethical implications. Probably, the first TA study on ubicomp (in that case called "pervasive computing") was commissioned in 2002 and published in 2003 by TA-SWISS. An English translation of the 354-page study was published jointly by TA-SWISS and the Scientific Technology Options Assessment (STOA) body at the European Parliament in 2005 [13]. Since then, TA-SWISS has commissioned and published two additional studies related to ubicomp, one broaching the issue of the increasing autonomy or emancipation of computers [9], published in 2008, and a recent study on technologies for locating, tracking, and tracing [18], published in 2012.

The reason for selecting these three studies is that they emerged in a uniform institutional context (TA-SWISS), spanning a decade from the first systematic approach to assessing the implications of ubicomp to the most recent study. A review of the entire body of TA studies related to ubicomp would certainly provide a more comprehensive picture, but also go beyond the scope of this essay. Besides this geographic and institutional bias, this paper may also have a personal bias because

the author has been involved in two of these studies. I hope that the reader will nevertheless benefit from the—partially subjective—perspective presented in this paper.

The materials used for this analysis are therefore:

1. As a reference for the general discourse on ethical issues in computing: The “HCC” proceedings published by IFIP in the period 1974–2012 [2, 4–6, 8, 11, 25, 26, 28, 29] and, as a secondary source, the discourse analysis conducted by Lignovskaya [24] on these proceedings.
2. As sources for identifying ethical issues in ubiquitous computing, the following are three TA-SWISS studies and related literature:
 - (a) TA 46e/2005: “The Precautionary Principle in the Information Society: Effects of Pervasive Computing on Health and Environment” [13] and the related articles [12, 16, 30, 31]¹;
 - (b) TA 51/2008: “Die Verselbständigung des Computers” (“The Emancipation of the Computer”), published in German [9]; this study covers an essential implication of the ubicomp vision, the increasing autonomy of computers;
 - (c) TA 57/2011: “Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern” (“Located and Identified. How Positioning Technologies Are Changing Our Lives”), published in German [18], and an international conference paper summarizing the study [19]; this study focuses on one essential aspect of ubiquitous computing, the increasing location awareness of objects.

Besides these main sources, additional literature will be used where appropriate to illustrate or support the argument. In particular the work of the “Ad Hoc Committee for Responsible Computing,” an international group that developed a “normative guide for people who design, develop, deploy, evaluate or use computing artifacts” [1] will be considered as an additional input on applied ethics of computing, as well as the report “Exploring the Business and Social Impacts of Pervasive Computing” [20], jointly edited by IBM Research, the reinsurance company Swiss Re, and TA-SWISS, on specific ubicomp issues.

I will first identify the invariants in the discourse documented in the HCC proceedings in order to reveal the ethical issues of computing that seem to persist over time (although with a change in focus). In the second step, I will analyze the three TA studies, identifying ethical issues emerging from the ubicomp discourse.

3 Results

The persistent themes in the discourse on ethics of computing as documented in the HCC proceedings from 1974 to 2012 can be subsumed under three umbrella themes:

¹ “Pervasive computing” is considered synonymous to “ubiquitous computing” in this context.

- Autonomy and self-determination
- Responsibility
- Distributive justice.

The definitions of the umbrella themes are provided in the following subsections. This classification is not intended as a conceptual framework, but as a pragmatic means of structuring the issues found in the discourse analysis. The umbrella themes overlap, and some ethical issues may therefore be subsumed under more than one of them.

One result of this study is that all major issues discussed in the three ubicomp studies can be matched with the preexisting ethical issues (as shown in Tables 1, 2, 3), however, with new aspects occurring at a more concrete level.

Table 1 Results for autonomy and self-determination

Ethical issues in computing	Ethical issues in ubiquitous computing
Working conditions: <ul style="list-style-type: none"> • effects of computerization on job satisfaction [4, 25, 26, 29] • participation [4] 	Working conditions: <ul style="list-style-type: none"> • surveillance of employees [18] • blurring boundaries between private and professional life [18]
Virtual and augmented reality: <ul style="list-style-type: none"> • avatars [5, 28] • virtual property [6] 	Virtual and augmented reality: <ul style="list-style-type: none"> • in remote diagnosis [13] • in surgery [13]
Privacy: <ul style="list-style-type: none"> • informational self-determination [11, 28, 29] • and biometrics [8] • in health care [5] • and social media [11] 	Privacy: <ul style="list-style-type: none"> • automatic identification [13, 18] • location privacy [18] • implications of transparency [9]
Technology paternalism: <ul style="list-style-type: none"> • security and biometrics [8, 11] • in e-health [5] 	Technology paternalism: <ul style="list-style-type: none"> • as a tendency in ubicomp [9] • by the use of active implants [13] • in dependency relationships [18]

Table 2 Results for responsibility

Ethical issues in computing	Ethical issues in ubiquitous computing
Legal and moral responsibility <ul style="list-style-type: none"> • for “computer decisions” [8, 25] • in e-health [5] • of the user of social media [11] 	Legal and moral responsibility <ul style="list-style-type: none"> • and autonomous computer systems [9] • the “dissipation” of responsibility [13]
Social responsibility <ul style="list-style-type: none"> • for the impacts of automation and globalization [26, 29] • of governments [29] • of computer professionals [2, 4–6, 8, 11, 25, 28, 29] 	Social responsibility <ul style="list-style-type: none"> • for the implications of transparency [9]

Table 3 Results for distributive justice

Ethical issues in computing	Ethical issues in ubiquitous computing
Digital divide <ul style="list-style-type: none"> • computer literacy [4, 8, 29] • technology transfer [4] • intellectual property, piracy [6] 	Digital divide <ul style="list-style-type: none"> • reducing the digital divide [13]
Sustainable development <ul style="list-style-type: none"> • and the information society [2, 5, 6, 8] • sustainable X [11] 	Sustainable development <ul style="list-style-type: none"> • dematerialization potential [13] • material dissipation [13] • creation of a critical infrastructure [18]

3.1 *Autonomy and Self-determination*

Autonomy, as a philosophical concept, is the capacity of individuals to make choices based on their own personal beliefs and values. If seen as an ethical value, autonomy is central to moral theories and frameworks. The principle of autonomy (i.e., the principle that all individuals presumed to have decision-making capacity are afforded the right to self-determination, i.e., the freedom to make decisions for themselves) lies at the heart of various legal freedoms and rights, including freedom of speech and the right to privacy (or informational self-determination).

In applied ethics, the principle of autonomy has great practical relevance in medicine. The respect for a patient's autonomy is one of the most fundamental principles of medical ethics. In the field of computing, respect for the user's autonomy is an important issue as well, although it is frequently not labeled as such (as shown in Table 1). The title of the IFIP TC9 conferences, "HCC," refers to human choice, therefore to autonomy or self-determination, as a basic concern in the context of computing.

The relevance of the concept and the principle of autonomy in the field of computing can be explained by the trend toward increasingly "autonomous" machines, from the classical automation of repetitive tasks in manufacturing to the invisible control of complex sociotechnical processes in a (hypothetical) ubicomp world.

Starting from this perspective, I reviewed the discourse analysis [24] conducted on all ten HCC volumes [2, 4–6, 8, 11, 25, 26, 28, 29] and identified the main ethical issues connected to the topic of autonomy or self-determination. While the discourse analysis had mainly involved quantitative lexicometric methods, yielding histograms of words and of so-called n-grams (such as "working conditions" or "wireless sensor and actor networks"), my interpretation inevitably necessitated some qualitative contextual knowledge and is therefore not completely free of subjective judgment.

The result of my interpretation based on the discourse analysis of the HCC series is shown in the *left* column of Table 1. The *right* column lists related ethical issues specific to ubicomp that are mentioned in the three TA reports [9, 13, 18], each of them matched with its counterpart on the left side. The four issues under the

“autonomy” umbrella—working conditions, virtual and augmented reality, privacy, and technology paternalism—are discussed in more detail in the following paragraphs.

Working conditions. Throughout the 1970s and 1980s, effects of computerization on employment, working conditions, and job satisfaction dominated the discourse at the HCC conferences [4, 25, 26, 29]. Participation of employees in management decisions became an issue, including the idea of participatory design processes for computer applications [4].

The issue of working conditions has returned in the ubicomp discourse, driven mainly by two aspects: the potential of ubicomp for close surveillance at the workplace and its tendency to blur the boundary between professional and private life [18]. The latter is also described in [20] as the “virtual merging of our social, family and working roles,” forcing “new flexible boundaries between the different spheres of work, home and leisure, leading for some to a sense of increased stress and for others to greater empowerment” (p. 40).

Overall, the changes in working conditions because of computing have been discussed as a threat to human self-determination since the early days of computing; the original focus that led to the demand for participation in the design of the systems used at the workplace in the 1980s seems, however, to have lost importance in the ubicomp age. Instead, surveillance issues and around-the-clock availability of the workforce have become the new focal points of discussion.

Virtual and augmented reality. Communicating through virtual realities (e.g., provided by a computer game or a virtual working environment), taking on a virtual human role represented by an avatar, can be challenging because many natural aspects of communication may become unclear, for example, with whom we are communicating, who is following the communication, and how to secure virtual property [5, 6, 28].

In ubicomp, virtual or augmented reality techniques are likely to be used in a context connected to physical reality, such as remote medical diagnosis or surgery. There is a risk that communicative acts in such environments are more ambiguous than in a natural environment, which can cause damage, or that decisions are delegated to the technology in a way that affects the autonomy of the humans involved (both doctor and patient). On the other hand, augmented reality is expected to improve the precision of interventions and the availability of information during operations [13]. Similar arguments may apply in other safety-critical domains.

Ubicomp has shifted the focus of ethical concerns in the context of virtuality from the “within virtual worlds” perspective to the “real-world impact” perspective. This is not surprising, as ubicomp technologies are built to interact seamlessly with real-world processes via sensors and actuators. While in the early days of computing the discourse focused on how to keep control over virtual worlds (e.g., control over avatars or over virtual property), the ubicomp vision created more emphasis on issues of real-world processes controlled by humans and machines via virtual or augmented realities. The main issue here is the risks arising from potential damage caused by ubicomp systems, in particular in medical diagnosis and surgery.

This is linked to the issue of moral and legal responsibility for damage created by the use of computer systems (see Sect. 3.2).

Privacy. Privacy is an individual condition of life characterized by exclusion from publicness. In the context of computing, privacy is usually interpreted as “informational privacy,” which is a state characterized “by controlling whether and how personal data can be gathered, stored, processed or selectively disseminated” [28, p. 58]. As an ethical issue in computing, information privacy is usually discussed as being threatened by computing infrastructures that facilitate the dissemination and use of personal data. The resulting requirement to protect individual privacy against data misuse entered many laws and international agreements under different terms, some of them focusing on the defensive aspect, such as “data protection,” others emphasizing individual autonomy, such as “informational self-determination.” This term first occurs in the HCC proceedings in 1986 [29], 3 years after the German Federal Constitutional Court declared the right to informational self-determination in its census verdict in 1983. At the same conference, “data protection” advanced to become one of the most frequently mentioned specialist terms. Threats against informational self-determination were mainly perceived as originating from governments. Later on, in the 2001 conference [28], the picture had changed in two respects: data protection was now—in the Internet age—discussed in connection with data security and encryption, and the focus had increasingly turned to the private sector. For example, the use of cookies, the creation (and sale) of profiles about individuals’ financial behavior, and the private sector’s interest in geographic data were discussed in the context of data protection in 2001 [28].

In the following conferences, the privacy discourse continued while integrating new and more specific issues, in particular biometric methods [8], health care (e-health) [5], and social media [11].

In the ubicomp discourse, the privacy issue revolves around three aspects:

- Automatic identification: Identifying persons even without their knowledge is much easier in a ubicomp world, because sensor data can easily be collected and combined [13, 18]. The discussion about automatic identification started with RFID [27], which is, however, less powerful than newer technologies of face recognition or device fingerprinting [18]. In a world of ubiquitous automatic identification, the amount of personal data generated and circulated is expected to increase dramatically [18].
- Location privacy: In addition to detecting an *agent*, ubicomp will usually generate data containing a reference to the *location of the action*. The aspect of location or positioning is linked to the general discussion about privacy in social networks [11] to the extent that social networking platforms will start tracking their users’ locations automatically and in real time [18]. Location privacy is an important special case of privacy because public or private sector organizations that process location data can combine them into profiles from which not only the activities, but also the contacts of persons can be inferred [18, 19].
- Implications of transparency: In a ubicomp world, monitoring and recording virtually all processes and calculating indicators which are believed to represent

criteria relevant for making management decisions are feasible and affordable. The resulting “transparency” is not only a threat to privacy, but also to other aspects of self-determination: decisions may first be delegated to bureaucracy (indicator systems) and then from bureaucracy to computers (automated indicator systems), which means relinquishing autonomous decision making, or in fact ceding control to those who define the indicators [9].

The last concern mentioned above goes beyond privacy and will be revisited under the umbrella of responsibility (Sect. 3.2).

Technology paternalism. When someone believes they know the solution to someone else’s problem and imposes this solution on that person even without their consent, this attitude is called “paternalism.” There is a serious ethical dilemma behind paternalism: Imposing the solution violates the autonomy of the other person, whereas by not imposing it, one may not do the best possible thing in the other person’s interest. As pointed out in [32], not only individuals, but any system, including governmental institutions and technical systems, can act in a paternalistic way. Paternalism can be “delegated” to machines by means of technology, and when executed by machines is called “technology paternalism” [32].

In the general discourse about the ethics of computing, paternalism is discussed mainly in two domains: security and e-health. It was implicitly addressed in the HCC 2002 proceedings [8], when anti-terror prevention measures introduced after the 9/11 attacks were discussed by asking the question whether “diminished liberty would be compensated by improved security” [8, p. 196]. In a similar way, technologies of biometrics such as fingerprinting, facial recognition, and iris scanning were discussed 10 years later at the HCC 2012 conference [11]. Paternalism was mentioned explicitly only in the context of e-health: While e-health can increase the autonomy of the patient who is empowered by information (“do-it-yourself healthcare”), doctors may make the “paternalistic decision” not to store important information if they know the patient will access it [5].²

Technology paternalism, however, is considered an inherent tendency in ubi-comp systems, in particular when machine-learning techniques are applied to infer the user’s intentions [9]. This thought is more clearly formulated in the IBM/SwissRe/TA-SWISS study: “(The ubiquitous) computing environment will be unable to perfectly adapt to explicit requests or to correctly read the context or user intentions. New habits will therefore be acquired or ‘tricks’ to let the appropriate interface know what is desired, or even to cheat it in order to avoid undesired reactions. The systems will build user models, and the users will build their own approach to deal with them. The unpredictability and intended unobtrusiveness of the systems will make this a harder task for the user than before” [20, p. 40].

In health care, there is a special aspect of ubicomp raising serious ethical concerns: active implants and other remote methods of personal health monitoring [13]. The dilemma can be described as follows: On the one hand, the quality of life of patients

² Strictly speaking, this case is not about technology paternalism, but about an unintended consequence of introducing computational technology in a paternalistic environment.

who are chronically sick, undergoing rehabilitation, or at high risk can be improved by these technologies, in particular by reducing their dependence on hospital facilities. On the other hand, these opportunities will be accompanied by the risk that active implants might have unexpected side effects or, viewed from a more general perspective, that an “over-instrumented” way of practicing medicine might have a negative psychological impact on patients subjected to close observation [13].

Another important aspect of technological paternalism discussed in the ubicomp context is the use of tracking and tracing devices in dependency relationships. On the one hand, tracking can enhance the safety and security of the tracked persons, in particular patients, children, or employees. On the other hand, tracking represents a serious threat to the self-determination the tracked individual. Who should be given the right to track and trace whom for what purpose? [18].

3.2 Responsibility

Computing professionals work in environments where small causes can have large effects. Decisions made and actions taken during software development may have serious consequences in practical application, as in the famous case of the Therac-25 radiation therapy machine that killed several patients by giving massive overdoses of radiation.

The “small cause—large effect” property of digital technology leads to questions of who is responsible, both in legal and in broader moral terms, for damage that may result from using computer systems. This “attributional” concept of responsibility is also known as “accountability” because it addresses the question of who is accountable for the effects of a chain of actions. In the case of the production and use of computer hardware and software, attributing legal and moral responsibility is difficult due to a problem that has been termed “the problem of many hands” [1].

A different concept of responsibility is social responsibility, which addresses the obligation of an individual or an organization to act with the goal of benefiting society at large.

Legal and moral responsibility. As early as 1980, the issue of who will be responsible for “computer decisions” and “decisions based on wrong information” in an increasingly automated world was discussed on the second HCC conference [25]. A change in the public perception of computers was reported: “The public conviction of objectivity of computer decisions has given way to a feeling of the irresponsibility of such decisions” [25]. This issue recurred later in a critical discussion of the agent concept: “The delegation of any task to a software agent raises questions in relation not only to trust but also to its autonomy of action and decision, and to the location of responsibility, both moral and legal, for the outcomes of those decisions and actions” [8].

The issue of responsibility for decisions delegated to machines was discussed in the context of professional responsibility, which was defined as “a kind of

responsibility that combines traits of legal and of moral responsibility” of the IT professional for the outcome of decisions taken [5].

The application context in which the issue of legal and moral responsibility was discussed shifted from e-health in 2006 [5] to social media in 2012 [11]. In the social media context, the responsibility of the *user* was addressed for the first time: “The people who communicate via social media are morally responsible for that communication and for the foreseeable effects of it. This responsibility is shared with other people who have affected and contributed to that communication as part of a sociotechnical system. This identifies moral responsibility both for those who create the message for its unintended but foreseeable effects, and for those who use a system to wrongfully harm others” [11].

In the ubicomp discourse, the issue of responsibility for decisions made by (increasingly autonomous) computer systems is a central concern. A “basic ambivalence” of ubicomp applications is seen in their impact on human control: Will we gain more control over our environment in a ubicomp world, or will the autonomous systems start to control us? [9]. When the systems make decisions that turn out to be against the user’s intention, it will be difficult to attribute responsibility: “The penetration of everyday life with systems whose behavior is dependent on complex hardware and software in a distributed system makes it quite difficult to identify the cause and causer where harm occurs. This situation could be further exacerbated (...) because there will be a very great incentive to use (...) programs acting on behalf of their users (software agents). The incentive arises from the fact that the flood of possibilities, in conjunction with the social pressure also to use them, is pushing the boundaries of human processing capacity” [13]. The basic problem with regard to responsibility is the fact that machines are not capable of making commitments, leading to a problem called “dissipation of responsibility”³: “A promise made by a machine—e.g. to carry out a particular function—is in principle worthless as it cannot feel obligation and cannot be held responsible. The inability of machines to make commitments in principle excludes them from social interaction. Consequently, there is a danger of a ‘dissipation of responsibility’ (...A) fine distribution of cause and responsibility as a result of the multilayered or networked nature of digital ICT can arise which can no longer be controlled by legal means” [13, p. 265]. However, other authors emphasize that this technology can improve accountability in organizations [7].

To conclude, the ubicomp vision has highly magnified one aspect of the accountability issue already established in the ethics of computing discourse: the implications of increasingly autonomous machines for moral and legal responsibility. These implications are complex, and there is no single standard that could be applied to all potential applications.

³ Dissipation of responsibility addresses the problem of accountability in complex distributed human–machine systems [16, 30] and is not to be confused with what is known as “diffusion of responsibility.” This is the psychological phenomenon that people tend to feel less responsible for their individual actions the larger the group of people who could take action.

Social responsibility. Social responsibility differs from moral and legal responsibility (or accountability) discussed above by addressing an obligation to act toward the benefit of society, regardless whether one is accountable for the outcome of an action. In the HCC discourse, social responsibility was first discussed as an obligation on the part of large companies and the public to pay attention to the negative social impacts of an ongoing new wave of (computer-based) industrial automation [26].

After automation in the 1970s, globalization was recognized in the 1980s as an emerging aspect of computerization that should be dealt with in a socially responsible way: “Because of the marriage between computer technology and telecommunications the globe has shrunk to the size of a ping-pong ball, crowded with our traditional unsolved problems” [29]. In particular, “multinational corporate social responsibilities” of the mainly US-based computer industry were discussed. [29]. More than 10 years later, the contributions of information systems to the transparency of business organizations [5] and to corporate social responsibility (CSR) entered the discourse [11].

Government policies related to new opportunities and risks of computing were discussed as well in the context of social responsibility, such as national policies related to the role of computers in nuclear weapons systems (including President Reagan’s proposed Strategic Defense Initiative, known as the “Star Wars Program”) [29], the introduction of national identification schemes after the 9/11 attacks [8], and policies related to new critical infrastructures [11]. In 1990, technology assessment was discussed as an approach for governments to implement social responsibility in the use of new technologies [4].

Besides companies and governments, the individual IT professional has been addressed by the issue of social responsibility throughout the HCC discourse. In 1980, having a sense of social responsibility still seemed to counter a widespread prejudice: “It is sometimes said that computer—and other—specialists do not appreciate the social effects of their activities” [25]. In the following years, IFIP TC9 became instrumental in motivating, facilitating, and reflecting the development of ethics codes of national computer professional associations around the world [2–6, 8, 11, 28, 29], a process that cannot be reported in detail in this article.

In the ubicomp discourse, there is one additional aspect of social responsibility already mentioned in Sect. 3.1, namely the potential consequences of transparency on automated decision making: Is it socially responsible to allow the diffusion of technologies that could replace human choice with the automated application of indicators and routines defined by a few people [9]?

3.3 Distributive Justice

Distributive justice concerns the allocation of goods (wealth, opportunity, respect) in society and is linked to issues of equality, power, need, responsibility, and other basic concepts discussed in ethics. Ethics in computing relates to two specific issues of distributive justice: the digital divide and sustainable development.

Digital divide. In the HCC conferences, the term “digital divide” first occurred in the 2002 proceedings [8]. The issue as such, however, was discussed at earlier conferences using different terms, such as “the information-rich” versus “the information-poor” [29] and “computer literacy” [4, 8, 29], in the context of information technology and developing countries [29] as well as technology transfer [4], in terms of “digital inclusion” versus “digital exclusion” [2], and finally, as one aspect of intellectual property and the phenomenon of piracy [6].

In the three ubicomp studies, the digital divide was mentioned only in [13], defined here as “the jeopardization of social justice through the division of society into those who have access to the information society and those who are excluded” (p. 41). This study assigns a high probability to the scenario that the digital divide will be reduced by the availability of better user interfaces and the continued diffusion of ICT, a hypothesis that has at least partly become reality through the spread of the mobile phone around the globe as well as programs providing affordable computers to schools in developing countries [33].

Sustainable Development. The aim of sustainable development can be defined as solving a double problem of distributive justice, namely both intergenerational and intragenerational justice [15, 21].

First mentioned at the 1998 HCC conference [28], the relationship between the aim of sustainable development and the information society (or knowledge society) was discussed in 2002 [8] and more broadly in all three succeeding conferences [2, 5, 6]. The 2012 proceedings [11] contain a surprisingly high number of “sustainable X” terms, such as “sustainable innovation,” “sustainable business,” “sustainable growth,” “sustainable computing,” “sustainable consciousness,” and “sustainable governance” [11], whose relation to the concept of sustainable development is not always clear. The term “sustainable development” itself had almost vanished in the 2012 proceedings.

In the ubicomp discourse, the issue of sustainable development was addressed in several ways. First, ubicomp technologies were attributed a higher dematerialization potential (potential to replace physical goods and processes by virtual ones)⁴ compared to traditional computing, thus creating opportunities for sustainable development [13, 16]. Second, the chemical elements (covering half of the periodic table) needed to produce the small ubicomp devices in vast numbers and the increasing problem that they are not recycled⁵ were mentioned as a threat to sustainable development [12, 13, 31]. In addition, the risks of an emerging new critical and vulnerable infrastructure, raising questions of the distribution of safety in society, were mentioned in [18] with regard to positioning technologies: “They are becoming new critical infrastructures the malfunctioning or collapse of which can have far-reaching consequences” (p. XXI).

⁴ Dematerialization effects of computing result in relevant reductions in energy consumption and greenhouse gas emissions, if not compensated by rebound effects [10, 17].

⁵ Embedded ICT hardware can also compromise established recycling processes [22, 23, 34].

Ubicomp seems to be ambivalent with regard to sustainable development; this is also true of computing in general [14], but the connection to physical and ecological aspects can be seen more clearly in the case of ubicomp.

4 Conclusion

Viewed against the background of the general discourse on ethics in computing as it has evolved over four decades in the HCC conferences of IFIP TC9, most of the ethical issues discussed in the ubicomp discourse—as far as it is reflected in the three studies—turn out to be special cases of persistent ethical issues of computing, but with some new aspects that were not anticipated in the earlier discourse. These new aspects are as follows:

- the potential for closer surveillance and around-the-clock availability of employees;
- virtual realities having direct effects on physical realities in safety-critical domains, such as e-health;
- ubiquitous automatic identification and its implications for informational self-determination, including location privacy;
- complete transparency of processes creating incentives to automate indicator-based decisions;
- technology paternalism in health care and other domains where dependency relationships exist, such as parenting;
- legal and moral responsibility (accountability) of autonomous computer systems and the “dissipation” of responsibility;
- opportunities to overcome digital divides or facilitate digital inclusion;
- sustainable use of natural resources, conservation versus dissipation of materials;
- emergence of a new critical infrastructure and the social distribution of safety.

Designers of ubicomp technology should take these aspects into account and consider their complex ethical implications when developing applications. Decision makers in organizations introducing such applications should be aware of their responsibility for the ethical implications of the technology.

References

1. Ad Hoc Committee for Responsible Computing: Moral Responsibility for Computing Artifacts: Five Rules, Version 27. <https://edocs.uis.edu/kmill2/www/TheRules/> (2010)
2. Avgerou, C., Smith, M.L., Van den Besselaar, P. (eds.): Social Dimensions of Information and Communication Technology Policy. In: Proceedings of the Eighth International Conference on Human Choice and Computers (HCC8), IFIP TC 9, Pretoria, South Africa, 25–26 September, Springer (2008)

3. Berleur, J., Brunnstein, K. (eds.): Ethics of computing: codes, spaces for discussion and law: a handbook prepared by the IFIP ethics task group. Chapman and Hall, London (1996)
4. Berleur, J., Drumm, J. (eds.): Information technology assessment. In: Proceedings of the 4th IFIP TC9 International Conference on Human Choice and Computers, HCC-4, held jointly with the CEC FAST Programme, Dublin, Ireland, 9–12 July 1990, North-Holland (1991)
5. Berleur, J., Nurminen, M.I., Impagliazzo, J. (eds.): Social informatics: an information society for all? in remembrance of Rob Kling. In: Proceedings of the Seventh International Conference on Human Choice and Computers (HCC7), IFIP TC 9, Maribor, Slovenia, 21–23 September, Springer (2006)
6. Berleur, J., Hercheui, M.D., Hilty, L.M. (eds.): What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience—9th IFIP TC 9 International Conference, HCC9 2010 and 1st IFIP TC 11 International Conference, CIP 2010, Held as Part of WCC 2010, Brisbane, Australia, September 20–23, Springer (2010)
7. Boos, D., Guenter, H., Grote, G., Kinder, K.: Controllable accountabilities: the internet of things and its challenges for organisations. *Behav. Inf. Technol.* **32**(5), 449–467 (2013). doi:[10.1080/0144929X.2012.674157](https://doi.org/10.1080/0144929X.2012.674157)
8. Brunnstein, K., Berleur, J. (eds.): Human choice and computers. In: Issues of Choice and Quality of Life in the Information Society, IFIP 17th World Computer Congress, TC9 Stream, 6th International Conference on Human Choice and Computers: Issues of Choice and Quality of Life in the Information Society (HCC-6), 25–30 August, Montreal, Quebec, Canada. Kluwer Academic (2002)
9. Kündig A., Bütschi, D. (eds.): Die Verselbständigung des Computers. vdf Verlag, ETH Zürich (2008)
10. Erdmann, L., Hilty, L.M.: Scenario analysis: exploring the macroeconomic impacts of information and communication technologies on greenhouse gas emissions. *J. Ind. Ecol.* **14**(5), 826–843 (2010)
11. Hercheui, M.D., Whitehouse, D., McIver W.J., Phahlamohlaka, J. (eds.): ICT Critical Infrastructures and Society. In: 10th IFIP TC 9 International Conference on Human Choice and Computers, HCC10 2012, Amsterdam, The Netherlands, 27–28 September, Springer (2012)
12. Hilty, L.M.: Electronic waste—an emerging risk? *Environ. Impact Assess. Rev.* **25**(5), 431–435 (2005)
13. Hilty, L.M., Behrendt, S., Binswanger, M., Bruinink, A., Erdmann, L., Froehlich, J., Koehler, A., Kuster, N., Som, C., Wuertenberger, F.: The Precautionary Principle in the Information Society—Effects of Pervasive Computing on Health and Environment. Second Revised Edition. Edited by the Swiss Center for Technology Assessment (TA-SWISS), Bern, Switzerland (TA46e/2005) and the Scientific Technology Options Assessment at the European Parliament (STOA 125 EN) (2005)
14. Hilty, L.M., Lohmann, W.: An annotated bibliography of conceptual frameworks in ICT for sustainability. In: Hilty, L.M., Aebischer, B., Andersson, G., Lohmann, W. (eds.) ICT4S 3013: Proceedings of the First International Conference on Information and Communication Technologies for Sustainability, ETH Zurich, 14–16 February, 288–300. E-Collection ETH Institutional Repository (2013). doi:[10.3929/ethz-a-007337628](https://doi.org/10.3929/ethz-a-007337628)
15. Hilty, L.M., Ruddy, T.F.: Sustainable development and ICT interpreted in a natural science context: the resulting research questions for the social sciences. *Inf. Commun. Soc.* **13**(1), 7–22 (2010)
16. Hilty, L.M., Som, C., Köhler, A.: Assessing the human, social and environmental risks of pervasive computing. *Hum. Ecol. Risk Assess.* **10**(5), 853–874 (2004)
17. Hilty, L.M., Köhler, A., von Schéele, F., Zah, R., Ruddy, T.: Rebound effects of progress in information technology. *Poiesis and Praxis: Int. J. Technol. Assess. Ethics Sci.* **1**(4), 19–38 (2006)
18. Hilty, L.M., Oertel, B., Wölk, M., Pärli, K.: Lokalisiert und Identifiziert. Wie Ortungstechnologien unser Leben verändern. vdf Verlag, ETH Zürich (2012)

19. Hilty, L.M., Oertel, B., Wölk, M., Pärli, K.: Locating, tracking and tracing: from geographic space to cyberspace and back. In: Michalek, T.C., Hebakova, L., Hennen, L., Scherz, C., Nierling, L., Hahn, J. (eds.) *Technology Assessment and Policy Areas of Great Transitions*, pp. 336–341. Informatorium, Prague (2014)
20. IBM Zurich Research Laboratory, Swiss Re Centre for Global Dialogue, TA-SWISS: *Exploring the Business and Social Impacts of Pervasive Computing*. Zurich (2006)
21. Isenmann, R.: Sustainable information society. In: Quigley, M. (ed.) *Encyclopedia of Information Ethics and Security*, pp. 622–630. IGI Global, Hershey (2008)
22. Köhler, A.R., Hilty, L.M., Bakker, C.: Prospective impacts of electronic textiles on recycling and disposal. *J. Ind. Ecol.* **15**(4), 496–511 (2011). doi:[10.1111/j.1530-9290.2011.00358.x](https://doi.org/10.1111/j.1530-9290.2011.00358.x)
23. Kräuchi, Ph, Wäger, P., Eugster, M., Grossmann, G., Hilty, L.M.: End-of-life impacts of pervasive computing. *IEEE Technol. Soc. Mag.* **24**(1), 45–53 (2005)
24. Lignovskaya, E.: *Human Choice and Computers 1974–2012. Eine Diskursanalyse mit Hilfe lexikometrischer Verfahren*. Facharbeit im Fach Wirtschaftsinformatik am Institut für Informatik. Universität Zürich (2013)
25. Mowshowitz, A. (ed.): *Human choice and computers 2*. In: *Proceedings of the Second IFIP Conference on Human Choice and Computers*, Baden, Austria, 4–8 June 1979, North-Holland (1980)
26. Mumford, E., Sackman, H. (eds.): *Human choice and computers*. In: *Proceedings of the IFIP Conference on Human Choice and Computers*, Vienna, 1–5 April 1974, North-Holland (1975)
27. Oertel, B., Wölk, M., Hilty, L.M., Köhler, A.: *Security aspects and prospective applications of RFID systems*. Bundesamt für Sicherheit in der Informationstechnik, Bonn (2005)
28. Rasmussen, B.L., Beardon, C., Munari, S. (eds.): *Computers and networks in the age of globalization*. In: *IFIP TC9 Fifth World Conference on Human Choice and Computers*, pp. 25–28 August 1998, Geneva, Switzerland. Kluwer Academic (2001)
29. Sackman, H. (ed.): *Comparative worldwide national computer policies*. In: *Proceedings of the Third IFIP TC9 Conference on Human Choice and Computers*, Stockholm, Sweden, 2–5 September 1985, North-Holland (1986)
30. Som, C., Hilty, L.M., Ruddy, T.: The precautionary principle in the information society. *Hum. Ecol. Risk Assess.* **10**(5), 787–799 (2004)
31. Som, C., Hilty, L.M., Köhler, A.R.: The precautionary principle as a framework for a sustainable information society. *J. Bus. Ethics* **85**(3), 493–505 (2009)
32. Spiekermann, S., Pallas, F.: Technology paternalism—wider implications of ubiquitous computing. *Poiesis Praxis: Int. J. Technol. Assess. Ethics Sci.* **1**(4), 6–18 (2006)
33. Streicher-Porte, M., Marthaler, C., Böni, H., Schluep, M., Camacho, A., Hilty, L.M.: One laptop per child, local refurbishment or overseas donations? sustainability assessment of computer supply scenarios for schools in Colombia. *J. Environ. Manage.* **90**, 3498–3511 (2009). doi:[10.1016/j.jenvman.2009.06.002](https://doi.org/10.1016/j.jenvman.2009.06.002)
34. Wäger, P., Eugster, M., Hilty, L.M., Som, C.: Smart labels in municipal solid waste—a case for the precautionary principle? *Environ. Impact Assess. Rev.* **25**(5), 567–586 (2005)