# Internet Research

Privacy and fair information practices in ubiquitous environments: Research challenges and future directions

Maria Karyda, Stefanos Gritzalis, Jong Hyuk Park, Spyros Kokolakis,

# Privacy and fair information practices in ubiquitous environments

## Research challenges and future directions

Maria Karyda and Stefanos Gritzalis
*Department of Information and Communication Systems Engineering, University of the Aegean, Karlovassi, Greece*
Jong Hyuk Park
*Department of Science and Engineering, Kyungnam University, Kyungnam, South Korea, and*
Spyros Kokolakis
*Department of Information and Communication Systems Engineering, University of the Aegean, Karlovassi, Greece*

**Abstract**

**Purpose** – This paper aims to contribute to the ongoing discourse about the nature of privacy and its role in ubiquitous environments and provide insights for future research.

**Design/methodology/approach** – The paper analyses the privacy implications of particular characteristics of ubiquitous applications and discusses the fundamental principles and information practices used in digital environments for protecting individuals' private data.

**Findings** – A significant trend towards shifting privacy protection responsibility from government to the individuals is identified. Also, specific directions for future research are provided with a focus on interdisciplinary research.

**Research limitations/implications** – This paper identifies key research issues and provides directions for future research.

**Originality/value** – This study contributes by identifying major challenges that should be addressed, so that a set of "fair information principles" can be applied in the context of ubiquitous environments. It also discusses the limitations of these principles and provides recommendations for future research.

**Keywords** Intelligence, Privacy, Data security, Computer networks

**Paper type** Literature review

## 1. Introduction

Ubiquitous computing (UC) refers to environments where most physical objects are enhanced with digital qualities. It implies that small, often tiny-sized devices, with computing capabilities that are wirelessly interconnected, are embedded almost invisibly into most objects used in everyday life. These devices can be anything from a device that only allows identification or positioning of the user to a fully featured mobile device that is capable of intense interaction with the user. The concept of ubiquitous computing draws on the ideas introduced by Weiser (1991) and refers to a digital world where electronic devices are embedded into distributed networks.

Internet Research
Vol. 19 No. 2, 2009
pp. 194-208
© Emerald Group Publishing Limited
1066-2243
DOI 10.1108/10662240910952346

Ambient intelligence (AmI) is an extension of the idea of UC describing digital environments that are aware of and, most importantly, responsive to the presence of people through intelligent and friendly user interfaces. AmI environments are focused on users and their interaction with electronic devices, and their primary aim is to respond, or even better, to foresee, users' needs and preferences. In the AmI vision humans are empowered and their everyday life is improved through interaction with their "smart environment" resulting in time and cost savings, increased convenience, safety and security, and more entertainment.

Ubiquitous or ambient intelligence environments introduce a range of new fundamental problems related not only to technology (for instance, designing unobtrusive devices, dynamic networks, and natural user interaction) but also to social, ethical and legal considerations, such as privacy protection, social cohesion and control ISTAG (2001). Violations against individuals' privacy, more specifically, are considered unavoidable in such environments (Solove, 2004) due to the application of invasive technologies, whereas, at the same time regulatory provisions are constantly outpaced by technological developments. In a digitized world that is populated of intelligent devices that communicate with each other keeping one's seclusion is very difficult. Critics to UC and AmI even suggest that these technologies could bring a big brother type of society where all human actions, even thoughts, are recorded to become reality (Brey, 2005).

This paper aims to address the question whether or if, invasive/intrusive usage of ubiquitous technologies can be prevented and explores how privacy protection, in terms of commonly accepted fair information practice principles can be accommodated in these applications. It contributes to the exploration of UC implications for society and especially implications on individuals' fundamental rights, such as the right to privacy. It also demonstrates the importance of a multidisciplinary approach and the value of input from related fields. Furthermore, this paper identifies a number of privacy challenges that should be overcome before ubiquitous applications become reality. These challenges are based on the analysis of research in progress and the analysis of fundamental practices for privacy protection.

The rest of the paper is structured as follows: section two discusses the concept of privacy and describes the basic principles and information practices for privacy protection. Section 3 focuses on the particular characteristics of ubiquitous environments and their privacy related implications and presents an overview of privacy research in ubiquitous computing. Section 4 identifies major privacy challenges in ubiquitous environments which arise in the effort to apply fair information practices for privacy protection. Finally, section 5 presents our conclusions and provides suggestions for future research.

## 2. Privacy

### *2.1 The concept of privacy*

The concept of privacy can generally be defined as the individuals' ability to control the terms by which their personal information is collected and used. It has also generally been defined as the right "to be left alone", meaning that it represents a sphere where it is possible to remain separate from others, anonymous and unobserved; thus it represents an aspect of freedom and, more specifically, freedom from interference (Gritzalis, 2004). The need for privacy emerges from within the society, from the various social relationships that people form with each other, with private sector institutions and with the government. Thus, privacy is not merely a right possessed by individuals; it is a form of freedom built into the social structure (Solove, 2006). Privacy protection is of critical importance both at the individual and the society level; the right to privacy protection is considered critical for a democratic society and it is recognized as a fundamental right in all major international treaties and agreements on human rights (Dumortier and Goemans, 2002). Different aspects of an individual's privacy that need to be protected include: bodily privacy; territorial privacy; privacy of communications; information privacy; and location privacy.

Generally, the basic approaches used to protect an individual's privacy include the adoption of regulatory and technical means and their combination. Privacy protection regulations can take different forms: within the European Union (EU), privacy is protected according to the EU Directive 95/46/EC on personal data protection. This directive regulates the collection, use and transfer of personal data, the rights data subjects can exercise and the obligations data controllers have. Compliance is monitored by independent public supervisory authorities. The US has a different approach to personal privacy protection: sector-specific laws are applied, each regulating a specific aspect, for instance, communications privacy, financial privacy etc. In most countries, independently of the type of the existing regulation of privacy, personal data protection is also pursued through self-regulation. The EU directive, for example, introduces the concept of "codes of conduct" that should be followed by organizations and trade associations. Other types of self-regulation include use of standards, such as privacy enhancing technologies (PETs), and privacy seals, which are used by websites to inform their visitors that their data will be treated according to certain data protection principles, as certified by the trust mark organization. Approaches to support privacy protection through the use of technical means primarily involve the use of some type of PETs (Gritzalis, 2004).

It thus becomes evident that the concept of privacy and the subsequent need for its protection is culture-dependent; different approaches can be traced not only to legislation, as previously described, but also to other privacy protection schemes such as self-regulation and privacy enhancing technologies. However, there is a number of commonly accepted principles and practices that should be followed by entities that need to manage personal data, while, at the same time, taking individual privacy into account, as will be shown in the following paragraphs.

### *2.2 Basic principles and fair information practices for privacy protection*

A set of basic principles for respecting an individual's privacy include the elements of necessity; finality; transparency; and proportionality. Necessity refers to the identification of purposes and benefits for identifying, or using personal information and also involves the considerations of possible alternatives. The principle of finality refers to the collection and use of personal data for specific and explicit purposes, which must be legitimate. The principle of transparency states that individuals should be aware of these purposes, as well as of the means used for the collection of their personal information; thus they should be notified. In some cases it is also supported that individuals should be able to choose (principle of choice) and give their consent (principle of consent) to the collection and use of their personal information. Finally, proportionality refers to the accordance between the type and the extent of personal data that are collected to the pursued objectives.

Besides the above mentioned fundamental principles, different approaches to managing personal information in a "fair way" are currently proposed. These approaches are known as "fair information practices" and define the ways and conditions under which personal information should be collected and treated. Following one approach, these include notice of users, choice over how their personal information is used, right to access collected information, reasonable security of the information and accountability of the collector's side (Center for Democracy and Technology, 2000). With regard to the design of privacy-aware ubiquitous systems the following set of principles for guiding are proposed:

- notice: users should always be aware of what data are being collected;
- choice and consent: users should be able to choose whether their personal data are used;
- anonymity and pseudonymity should apply when identity is not needed;
- security: different levels of protection depending on the situation; and
- access and recourse: users should have access to data about them (Langheinrich, 2001).

Overall, the self-regulatory paradigm of fair information practices can be considered to include the following set of basic information practices:

- notice and awareness;
- choice and consent;
- access and participation;
- integrity and security; and
- enforcement and redress (FTD, 1998).

Providing notice to users of the information practices followed by entities manipulating their personal data is required essential, so that they can make informed choices about what personal information they disclose. Thus, individuals should also be made aware of their rights. Notified users should then provide their consent to their data being manipulated and be able to choose how this information is used. Individuals should also be able to access data that have collected about them. In this way they can ensure that data kept about them is error free and up to date and control its quality. Access to one's personal data should also be combined with a scheme that allows users to correct any mistakes or provide updated information to the entity processing their data. For effective privacy protection, an enforcement scheme should be present to ensure compliance with fair information practices and relevant guidelines. Enforcement can take the form of self-regulation, where data processing entities can undergo external audits or certification procedures, or the form of legislation and regulatory schemes.

The above principles and practices have formed the basis for privacy legislation, such as the EU Directive 95/46/EC (European Parliament, 1995). Nevertheless, substantial doubts have been expressed as to whether the attempt to enforce fair information principles through legislation has actually benefited privacy. Bonner and

Chiasson (2005) argue that the fair information principles that underlie such legislation paradoxically lead towards reducing privacy, rather than protecting it. This paradox is mainly attributed to these principles reflecting a procedural approach to maximizing individual control over data thus placing the burden of protection to the individual rather than society and its institutions (Cate, 2006).

## 3. Privacy related characteristics of ubiquitous environments

### *3.1 Characteristics with privacy implications*

A ubiquitous computing environment is typically envisioned as a space populated with a large number of invisible, collaborating computers, sensors and actuators interacting with user-held and/or user-worn devices. Ubiquitous environments comprise of hardware and software elements, as well as social elements since it is humans who receive services and interact with each other. Up to now and by far, the vision of ubiquitous computing is mainly hardware-driven (Eymann and Morito, 2004). Research in software has also been active in the field, with research in smart agents and web services to prevail. The least researched into aspect of ubiquitous environments is the social one. The role of human principals in ubiquitous environments is primarily goal definition, preferences setting and strategies definition.

Ubiquitous applications and AmI environments in particular share some basic characteristics, including context awareness, user interaction, wireless communication, massive collection and storage of information and intelligent user interfaces. In Langheinrich (2001) reference is made to the following characteristics as related to privacy:

- ubiquity: the omnipresence of devices with computing capabilities;
- invisibility: the technological trend of constructing smaller computing devices with more functions which are embedded into everyday objects ("the disappearing computer");
- sensing: ubiquitous applications make sense of the environment using sensors and similar context-aware devices; and
- memory amplification: continuous recording of personal data combined with declining costs of storage make it possible to create "life-logs" for individuals, containing a complete record of their past.

Brey (2005) adds two more characteristics with privacy related implications:

1. *Profiling*. Smart objects can create unique profiles of users they interact with.
2. *Connectedness*. Personal information may move freely over *ad hoc* networks which are formed by devices using wireless connections.

Overall, our analysis has showed that ubiquity of devices and communications, context awareness, intelligent user interaction, dynamic nature of networks and massive information storage have privacy related implications and that they can affect the application of privacy preserving approach in ubiquitous and AmI environments.

Context awareness is an important attribute for ubiquitous and AmI applications. Context is a broad concept and is used to describe the physical, geographical, digital and social surroundings of a smart device, as well as how it is being used by the user. Dey describes context as "any information that can be used to characterize situation" and distinguishes among several types of context, the most important of which are location, identity, time, and activity (Crowley *et al.*, 2002). In Persson (2001) the concept of context is extended so as to include also the history of all relevant parameters. Context-awareness, in general, refers to the ability of computing systems to identify and adapt to their environmental context and contextual aware applications rely on the use of sensors that are seamlessly integrated in the environment and communicate all information that is needed for the application to determine that certain events or states have occurred (e.g. a specific person has entered the room). This information refers to the identification of individuals that can even extend to biometrics or vital signs of persons, to their location and usually their preferences, whether these are given explicitly, e.g. through queries, or are inferred by previous interactions.

Continuous interaction with the user through natural interfaces is another characteristic of ubiquitous and AmI environments. Designing user-friendly, natural interfaces for devices that are almost invisibly embedded in everyday objects is a critical design challenge for their acceptance by users. In AmI environments the technology is in the background, almost invisible to the user, and interfaces are highly natural, responding to inputs like voice and gestures. Under this perspective, AmI applications are user-centric; individuals communicate with their ambient intelligence surroundings through speech, tactile movements or gestures. Interaction with the user is accomplished through devices, some of which can be portable, such as personal digital assistants (PDAs) and mobile phones, or they might be static devices, such as, for example, storage devices or large servers. These devices can be further characterised by the source of energy they require, into autonomously-empowered devices which can empower themselves, such as certain types of tags and sensors and devices that require external sources such as batteries (battery-empowered) or mains (net-empowered). Energy supply is directly connected to the information-processing capabilities of a device; it is thus a central point for designing ubiquitous environments and their components.

Ubiquitous and AmI environments also rely on the constant interaction among the different entities; typically wireless communication infrastructures are used so as devices can exchange any type of information, including data, audio and video. Furthermore, the dynamic use of services and formation of networks is another privacy-related characteristic of ubiquitous environments. Mobile and portable devices, such as smart tags and sensors, personal digital assistants and mobile phones become parts of different networks, following a person’s movements. Finally, UC is characterized by the ability to learn from the past and to adapt services accordingly; thus computing systems are required to “remember” and therefore store personal data for a long period of time (Cas, 2005). In this way the amount of information about individuals’ everyday movements, actions, and their preferences is rapidly exceeding, thus augmenting privacy related threats.

Besides these characteristics, it is important to note, that ubiquitous applications can span without discretion both public spaces (such as outdoors, transportation means, working places, shopping areas) and private spaces (homes, clothes etc.).

### *3.2 Privacy preserving trends*

In this section we analyse some of the basic technologies and methods for privacy protection proposed by research. The “Platform for Privacy Preferences Project (P3P)” approach (W3C, 2001) specifies a privacy preserving architecture to be used by web sites that comprises user agents, privacy reference files, and privacy policies. Web sites that use the P3P platform announce their privacy practices to visitors and let them decide to accept or reject interaction. Within the P3P, the World Wide Web Consortium (W3C) provides guidelines that allow the encoding of privacy policies into XML, allowing automated processes to read such policies and take actions on them. P3P uses the APPEL language for capturing user privacy preferences. In Myles *et al.* (2003) a general, component-based platform that functions as a middleware service is proposed; this framework allows users apply general policies to control distribution of their information.

PawS (Langheinrich, 2002) is a privacy awareness system for ubiquitous computing environments, which like P3P, provides users with tools in order to facilitate them in protecting their personal privacy. Its basis is primarily social and legal rather than technical. PawS uses privacy beacons that announce the privacy policies to the user who enters an environment in which services are collecting data. Users' privacy proxies, which act similarly to P3P's user agents, check the announced policies, with regard to the user's predefined privacy preferences. If the policies agree, users utilize the services and their information can be collected; if the policies are incompatible then users are notified by the system, and can choose their preferred course of action, which can vary from accepting or not the service, to leaving the area in which information collection is taking place.

Other approaches to privacy protection in ubiquitous environments include the use of the idea of trust systems and certification authorities that have been applied in other fields, such as digital rights management (DRM), the concept of intermediate layers such as privacy proxies, the introduction of a "digital safe" between citizens and public authorities as an alternative for traditional access rights, and the use of anonymity and pseudonymity. Finally, some researchers argue that privacy expectations vary (Jiang *et al.*, 2002) and depend on context (Kobsa and Schreck, 2003). Therefore, privacy preserving technologies should be flexible and context-dependent.

In general, privacy research in ubiquitous computing is characterized by the belief that it is the individuals who are responsible, and thus should manage, their privacy and that privacy can be evaluated and exchanged, e.g. for the benefit of receiving customized, and thus higher-value services. For this reason, it is largely based on managing user's privacy preferences, i.e. users decide what information is disclosed to which entity; as, for example, in Sadeh *et al.* (2006). However, this approach is better suited for static environments or environments where components and their interaction is known in advance; in ubiquitous applications that rely on dynamic, distributed networks and pervasive devices managing user's preferences can be ineffective.

Moreover, despite the effort to provide individuals with tools that facilitate them in protecting their privacy, it is doubtful whether common people will ever be able to exercise their privacy-related rights effectively. UC technology is too complex for people without technical training to understand and they are almost always in a weak position when negotiating with corporations and organizations that operate ubiquitous environments.

Finally, there is a stream of privacy research in ubiquitous environments that adopts the opinion that user perceptions of risk and benefit can determine their willingness to adopt technology. Multiple research endeavours explore the hypothesis that people are more likely to accept potentially invasive technology if they think its benefits will outweigh its potential risks (Hann *et al.*, 2002; Zugenmaier, 2002).

## 4. Privacy challenges in ubiquitous environments

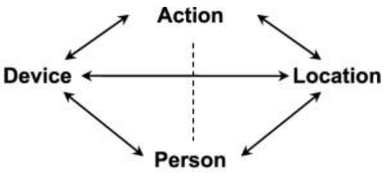
Ubiquitous computing is populated both by privacy enhancing technologies and privacy threatening technologies. Privacy enhancing technologies, mainly based on encryption and anonymization techniques, allow prevention or reduction of identification. Sensors and RFID technology are prominent examples of privacy threatening technologies; for instance RFID tags embedded in badges, clothing or other objects can provide information on a person's movements and whereabouts. Ubiquitous sensor networks, combined with robust data mining techniques and the decreasing cost of information storage amplify the tracking and profiling capabilities of personal information collectors, thus augmenting privacy intrusion capabilities. As smart devices increasingly pervade public as well as private places, it is expected that individuals will implicitly create continuous streams of personal related information regarding their actions, preferences and locations.

Currently, major threats to privacy originate from personal data aggregation and the increasing strength and capacity of search engines. The amplitude of information sources and the potential to aggregate or combine these sources so as to create a person's profile are threatening individual privacy. Other privacy related threats include theft of personal data, and their manipulation for malevolent causes, such as blackmailing etc.

The privacy diamond, depicted in Figure 1 (Beckwith, 2003), shows the interaction in ubiquitous environments between (smart) devices, the individual, and the information system or service provider. For this type of interaction to be realized, some sort of identification is needed. Data collected are mainly personal data, or they can be easily transformed into personal data. This personal information gathered typically includes data with regard to the identity, location and activity of a person. In some cases, the device placed between the user and the information system or service provider can also be used to provide anonymous or pseudonymous access. However, it is the individuals who consciously request, or unconsciously launch, the collection of their personal data to receive services. It should also be noted that authentication between the device and the user is critical. However, due mainly to technical limitations (e.g. low computing power or lack of interaction ability) ubiquitous devices often do not support any authentication scheme.

### *4.1 Applying information fair practices in ubiquitous environments*

A major difficulty for protecting individuals' privacy in ubiquitous computing applications stems from the fact that regulation based on legislation has very limited



**Source:** Beckwith (2003)

**Figure 1.**
The privacy diamond

impact and, thus, limited effectiveness. Standardization efforts with regard to privacy protection are still at an early stage and could more appropriately be characterized as "recommendations". The effectiveness of approaches such as privacy seals is also difficult to be evaluated, since users, as a rule, lack the knowledge and necessary information to evaluate the protection provided. Codes of conduct, on the other hand, present varying levels on effectiveness, based on the quality of their content, their application context and the quality of enforcement and compliance monitoring schemes. Approaches such as the application of "fair information practices" are gaining approval and industry seems to support this type of self-regulation scheme for privacy protection. Ubiquitous environments, however, have intrinsic characteristics, as discussed in previous paragraphs that pose challenges to the application of these principles.

*4.1.1 Providing notice and awareness*. An important issue that should be addressed with regard to users' notification stems from the fact that ubiquitous environments comprise devices which are often invisible to them, or devices which are embedded into everyday objects. Furthermore, the use of natural interfaces that aim to make user interaction acceptable can make identification of the types of information and the means used for their collection hard to identify. For the notification of the user to be complete, issues such as the nature of data required (i.e. required or voluntary), the consequences of declining the provision of information as well as possible secondary uses and the security measures adopted for protecting the confidentiality and integrity of the data should also be included in the communication. Another important issue concerns the fact that notification implies that uses of personal data (and subsequently entities that will share these data) are known beforehand, that is before the collection of personal data. This requirement is obviously hard to be met in *ad hoc* and dynamic networks.

In digital environments, deciding the level and type of required identification can be designed. However, in ubiquitous environments, the main question of how much identification is needed cannot be easily answered. The issue of whether, and which type of (personal) information is needed for the communication is not straightforward and depends on the situation. Generally, service providers depend on personal information to deliver personalized and location-based services. Thus, the everyday negotiation of privacy through interactive ubiquitous computing systems is considered an open issue. Furthermore, power supply is a key issue for the computing abilities and information processing of devices interacting to form an AmI environment. Since most traditional approaches to privacy preservation are applied through the use of cryptographic techniques the issue of limited information processing capability is an issue that should be taken into consideration in designing privacy enhanced AmI applications (Aarts and Roovers, 2003).

Notification techniques currently applied in Internet applications include banners, pop-ups and so on. User interaction with ubiquitous devices does not always involve displays but it is usually based on movements or speech, thus rendering traditional notification means inappropriate to a large extend. It is also important to note, that all information should be communicated to users in a clear, concise and understandable way. Conclusively, user notification and awareness schemes in ubiquitous environments need to make use of friendly interfaces which will allow the bi-directional communication of information in a clear but unobtrusive way. Important technical challenges that should be met refer to the dynamic, possibly real-time communication of information with regard to new entities joining *ad hoc* networks and the protection of personal information propagated through them.

*4.1.2 Providing choice and consent*. In internet-based activities, user consent is usually obtained using either the opt-in or the opt-out scheme. Following the first approach, users provide their explicit consent allowing the collection and use of their personal data; in the second approach users are expected to provide their explicit objection to the collection and use of their data. In most cases, users express their will through a yes/no type of communication; such a scheme could also be adopted in the interface of smart devices in ubiquitous environments. In this way, however, users cannot express their choice with regard to certain conditions, such as for example, that they accept the use of a subset of their personal information for certain reasons, or that they do not consent to their use for secondary purposes or by other entities and so on. Privacy preserving approaches in current ubiquitous applications such as myCampus (Sadeh *et al.*, 2006) use special entities that handle user expressed privacy preferences. This approach can be effective in centrally managed networks but it is not suitable for dynamic *ad hoc* environments.

Finally, it should be mentioned that adopting the principle of choice and consent implies that users can make an informed choice and can freely express it. It is not easy, however, for users to make informed choices, since that would mean that they have full knowledge of technology, of the possible use of their personal data and its implications, as well as that they are aware of all their privacy rights. In digital contexts, where asymmetry of information prevails, that is seldom the case. Moreover, even if users had access to and the capability to comprehend all related information, their choice would not necessarily be free, since, they would possibly be declined access to certain services. This effect is called the asymmetry of power, and is usually experienced by users who employ some privacy enhancing technologies, for instance cookies blockage, to find out that they cannot have access to all websites. Consequently, users should be able to express their privacy preferences free form technical or other constraints (including issues such as bandwidth availability, computing capabilities or interface design).

*4.1.3 Providing access and participation*. Ubiquitous applications users should also be provided with access to the information stored about them. In this way they can control the quality of stored data, meaning that data are accurate, complete and up-to-date. This principle poses the need to design and apply mechanisms that provide users with the required access. Moreover, such mechanisms should be cost effective and easy to use. Finally the application of this principle also implies the application of data validation schemes in ubiquitous applications.

Another challenge that should be addressed with regard to providing access to one's data concerns the amounts of data stored and the need for effectively managing them. With the declining information storage costs and the exponential growth of information gathered, data mining technology provides solutions for combining and locating information that pose further privacy related threats. Finally, issues such as how and by whom corrective actions should be included, in case errors are found need also to be resolved.

*4.1.4 Providing integrity and security*. Generally, both technical and managerial measures are used to protect against loss and the unauthorized access, destruction, use, or disclosure of personal data. In ubiquitous environments, as explained in previous paragraphs, technical approaches prevail.

Currently, major research efforts in privacy protection with regard to ubiquitous environments adopt a decentralized approach, mainly by using some sort of middleware or proxy, that require the participation of the user, who has the ultimate responsibility to manage her privacy, by setting privacy preferences and by making decisions, automatically supported in most cases, on whether information practices are acceptable or not at each case.

*4.1.5 Enforcement and redress*. In ubiquitous environments the distinction between the private and the public sphere is blurred; however, fair information practices and legal frameworks for data protection have a point of reference, which means that they apply in the public or the private sphere.

If we accept the definition that regards privacy as the individuals' ability to control the terms by which their personal information is collected and used, it will be natural to draw the conclusion that privacy is closely related to the concept of control. However, in the dynamic and volatile environment of ubiquitous applications, where individuals often maintain no direct physical contact with the computing devices, which may be tiny-sized, embedded and often difficult to be spotted, the span of a user's control over the information collected is generally very limited.

Thus, in the case of distributed ubiquitous environments depending on legislation and regulatory schemes for privacy protection appears problematic. On the other hand, industry self-regulation approaches such as the application of fair information practices can be a feasible solution, provided issues such as compliance mechanisms and redress schemes are resolved. It is evident that the adoption of a fair information practice code, such as the one referred to in this paper can only be a suggestive approach to privacy protection rather than a prescriptive mechanism, since it cannot ensure compliance with core fair information practice principles. However, a combined approach including the adoption of self-regulation by industry, the institutionalization of users' initiatives and the adaptation of the relevant legal and regulatory framework can provide privacy protection mechanisms at multiple levels.

### *4.2 Discussion*

In the previous paragraphs we have presented the technical and social challenges of preserving privacy in ubiquitous environments. We have discussed the application of fair information practices and we have shown that there are both technical obstacles (e.g. computing power limitations of small devices) and social obstacles (e.g. asymmetry of power). In addition to that several researchers reject the fair information practices scheme on the basis that it considers privacy as a right possessed by individuals, rather than a form of freedom built into the social structure.

If the right to privacy is treated as akin to property, meaning that privacy is bargainable and that it can be exchanged with other rights and privileges, then the element of individual dignity is totally ignored. However, dignity is inherent in the concept of privacy: dignity connotes the recognition of an individual's personality, respect for other people, non-interference with another's life choices and the possibility to act freely in society (Rodota, 2004). Human dignity, as source and expression of privacy, is not generated by the individual (it) "is instead created by one's community and bestowed upon the individual. It cannot therefore be bartered away or exchanged" (Lasprogata *et al.*, 2004).

## 5. Conclusions

Managing privacy in the physical everyday life is a situated social process, and in most cases it is intuitively performed. People disclose different versions of personal information to different parties under different conditions. In ubiquitous environments this issue is still not resolved, neither technically nor conceptually, meaning that there is not yet a clear and generally accepted idea of what exactly privacy protection in a dynamic, pervasive environment means.

Currently, privacy research is dominated by a technical perspective, where the subtleties and deeper meanings and implications ubiquitous technology can have are not further examined. This paper has provided a critical analysis in the field of privacy protection in ubiquitous environments, aiming to bring in the foreground characteristics that have important privacy implications and identify major challenges that should be met in order for such environments to accommodate basic information practices providing privacy protection for personal data.

Ubiquitous environments have intrinsic characteristics, such as pervasiveness of devices and communications, context awareness, intelligent user interaction, dynamic nature of networks and massive information storage with privacy implications. These characteristics make the adoption of widely acceptable privacy protection schemes in digital environments, such as self-regulation, problematic. This paper has provided an analysis of the issues that arise when core information practices for privacy protection in traditional digital environments are applied in ubiquitous environments. It has identified critical issues that limit the effectiveness of information practices in ubiquitous environments and should be further investigated. The challenges discussed in this paper span a wide range of disciplines, from microelectronics and user interface design to legal and ethical considerations.

For this reason, one of the first conclusions of this paper refers to the need that privacy research with regard to ubiquitous applications is informed and enriched with insight from other related fields, for instance law and psychology. A multidisciplinary approach is needed because researchers should be informed about the different facets of privacy so as to make informed choices when exploring, designing or evaluating privacy protection schemes to be applied in the context of ubiquitous environments. It is also important to note that although these challenges have been divided for the purposes of discussion, they are interconnected and overlaps can be found among them.

The second conclusion of this paper concerns the contradiction between the characteristics of ubiquitous environments, and efforts to apply fair information practices for privacy protection. We have identified a list of issues that should be resolved for accommodating core privacy principles in ubiquitous applications; these include:

- the need to provide users with all necessary information so that they can make free and informed choices prior to giving their consent for the collection and use of their personal data;
- the question of deciding how much authentication is needed in each case;

- the issues of the asymmetry of power and data ownership;
- the application of controls of data quality;
- the problems of managing the privacy of data in dynamic, *ad hoc* networks; and
- the difficulties of applying enforcement and compliance schemes.

These are some of the issues that prohibit, currently, the application of fair information practices in ubiquitous applications. It is evident, that solving them will not resolve the issue of privacy protection as a whole, but it is reasonable to believe that ubiquitous applications designers will be able to face privacy threats easier and that it will be easier to build users' trust to ubiquitous applications.

This paper has also shown how ubiquitous applications' characteristics and different privacy aspects are interwoven; this interaction brings us to the conclusion that privacy protection in ubiquitous environments is a multi-faceted, hard-to-address problem that requires a multidisciplinary approach.

Finally, the last conclusion of this paper is that we are witnessing a significant change: up to now, it was the role of the government to provide the framework for privacy protection, as part of their role in the development of a welfare state for their citizens (Dumortier and Goemans, 2002); however lately there is a tendency to shift privacy protection into the hands of the individuals and to provide them with privacy protection mechanisms and tools. IT industry and related research have adopted the approach that end-users need to control information disclosure.

The main implication of this approach is that the protection of individual privacy in ubiquitous environments is envisioned that can be managed, bargained and even traded. This, however, contradicts with the fundamental principle that privacy is one of the basic freedoms of people and the protection of privacy is a social responsibility. Thus, resolving the individual versus social responsibility dilemma is a key issue and a prerequisite for technical advancement.

For Weiser's vision of ubiquitous computing to come true it is not only technology that needs to advance computing capabilities and blend them seamlessly into the fabric of every day life; close cooperation is needed among all stakeholders to resolve major privacy issues arising from the characteristics of the ubiquitous environment.

## References

Aarts, E. and Roovers, R. (2003), "IC design challenges for ambient intelligence", in *Proceedings of the Design, Automation and Test in Europe Conference and Exhibition* (DATE'03), IEEE.

Beckwith, R. (2003), "Designing for ubiquity: the perception of privacy", *IEEE Pervasive Computing*, Vol. 3 No. 2, pp. 40-6.

Bonner, W. and Chiasson, M. (2005), "If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy", *Information and Organization*, Vol. 15 No. 4, pp. 267-93.

Brey, P. (2005), "Freedom and privacy in ambient intelligence", *Ethics and Information Technology*, Vol. 7 No. 3, pp. 157-66.

Čas, J. (2005), "Privacy in pervasive computing environments: a contradiction in terms?", *IEEE Technology and Society Magazine*, Vol. 24 No. 1, pp. 24-33.

Cate, F.H. (2006), "The failure of fair information practice principles", in Winn, J.K. (Ed.), *Consumer Protection in the Age of the Information Economy*, Ashgate, Aldershot.

Center for Democracy and Technology (2000), "Fair information practices", available at: www.cdt.org/privacy/guide/basic/fips.html (accessed 13 August 2008).

Crowley, J.L., Coutaz, J., Rey, G. and Reignier, P. (2002), "Perceptual components for context aware computing", *Proceedings of Ubicomp, LNCS*, Springer, New York, NY.

Dumortier, J. and Goemans, C. (2002), "Roadmap for European legal research in privacy and identity management", Interdisciplinary Centre for Law and ICT (ICRI), K.U. Leuven, December, available at: www.law.kuleuven.be/icri/publications/421rapid.pdf (accessed 13 August 2008).

European Parliament (1995), "Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data", *Official Journal of the European Communities*, L281/31, 23 November.

Eymann, T. and Morito, H. (2004), "Privacy issues of combining ubiquitous computing and software agent technology in a life-critical environment", *Proceedings of the 2004 IEEE International Conference on Systems, Man and Cybernetics*, IEEE Press, Piscataway, NJ.

FTD (1998), "Privacy online: a report to congress", *Federal Trade Commission*, available at: www.ftc.gov/reports/privacy3/priv-23a.pdf (accessed 13 August 2008).

Gritzalis, S. (2004), "Enhancing web privacy and anonymity in the digital era", *Information Management and Computer Security*, Vol. 12 No. 3, pp. 255-88.

Hann, I., Hui, K., Lee, T. and Png, I. (2002), "Online information privacy: measuring the cost-benefit trade-off", *Proceedings of the 23rd International Conference on Information Systems*, ACM Press, New York, NY.

ISTAG (2001), "Scenarios for ambient intelligence in 2010", European Commission Community Research, IST Advisory Group, available at: www.cordis.lu/ist/istag.htm (accessed 13 August 2008).

Jiang, X., Hong, J.I. and Landay, J.A. (2002), "Approximate information flows: socially based modeling of privacy in ubiquitous computing", *Proceedings of the 4th International Conference on Ubiquitous Computing*, LNCS 2498, Springer, New York, NY, pp. 176-93.

Kobsa, A. and Schreck, J. (2003), "Privacy through pseudonymity in user-adaptive systems", *ACM Transactions on Internet Technology*, Vol. 3 No. 2, pp. 149-83.

Langheinrich, M. (2001), "Privacy by design: principles of privacy-aware ubiquitous systems", in Abowd, G., Brumitt, B. and Shafer, S. (Eds), *Proceedings of Ubicomp 2001*, LNCS 2201, Springer, New York, NY, pp. 273-91.

Langheinrich, M. (2002), "A privacy awareness system for ubiquitous computing environments", *Proceedings of Ubicomp*, LNCS 2498, Springer, pp. 237-45.

Lasprogata, G., King, N. and Pillay, S. (2004), "Regulation of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada", *Stanford Technology Law Review*, Vol. 4.

Myles, G., Friday, A. and Davies, N. (2003), "Preserving privacy in environments with location-based applications", *IEEE Pervasive Computing*, Vol. 2 No. 1, pp. 56-64.

Persson, P. (2001), "Social ubiquitous computing", *Proceedings of the Workshop on Building the Ubiquitous Computing User Experience*, ACM/SIGCHI, Seattle.

Rodota, S. (2004), "Privacy, freedom and dignity", closing remarks at the 26th International Conference on Privacy and Personal Data Protection, Wroclaw; available at: http://26konferencja.giodo.gov.pl/data/resources/RodotaS.pdf (accessed 13 August 2008).

Sadeh, N., Gandon, F. and Kwon, O. (2006), "Ambient intelligence: the MyCampus experience", in Vasilakos, T. and Pedrycz, W. (Eds), *Ambient Intelligence and Pervasive Computing*, Artech House, Norwood, MA.

Solove, D. (2004), *The Digital Person: Technology and Privacy in the Information Age*, NYU Press, New York, NY.

Solove, D. (2006), "A taxonomy of privacy", *University of Pennsylvania Law Review*, Vol. 154 No. 3, pp. 477-564.

W3C (2001), "The platform for privacy preferences 1.0 (P3P1.0) specification", World Wide Web Consortium, available at: www.w3.org/P3P/ (accessed 13 August 2008).

Weiser, M. (1991), "The computer for the twenty-first century", *Scientific American*, Vol. 165 No. 3, pp. 94-104.

Zugenmaier, A. (2002), *Anonymity for Users of Mobile Devices through Location Addressing*, Rhombos Verlag, Berlin.

**Corresponding author**
Maria Karyda can be contacted at: mka@aegean.gr

**This article has been cited by:**

1. Ge Zhan, Zhimin Zhou. Mobile internet and consumer happiness: the role of risk. *Internet Research* **0**:ja, 00-00. [Abstract] [PDF]
2. Ismini Psychoula, Liming Chen, Feng Chen. Privacy modelling and management for assisted living within smart homes 1-6. [Crossref]
3. Shuchih Ernest Chang, Anne Yenching Liu, Wei Cheng Shen. 2017. User trust in social networking services: A comparison of Facebook and LinkedIn. *Computers in Human Behavior* **69**, 207-217. [Crossref]
4. Patrice Caire, Assaad Moawad, Vasilis Efthymiou, Antonis Bikakis, Yves Le Traon. 2016. Privacy challenges in Ambient Intelligence systems. *Journal of Ambient Intelligence and Smart Environments* **8**:6, 619-644. [Crossref]
5. Yean-Fu Wen, Ko-Yu Hung, Yi-Ting Hwang, Yeong-Sung Frank Lin. 2016. Sports lottery game prediction system development and evaluation on social networks. *Internet Research* **26**:3, 758-788. [Abstract] [Full Text] [PDF]
6. S. Arunkumar, M. Srivatsa, M. Rajarajan. 2015. A review paper on preserving privacy in mobile environments. *Journal of Network and Computer Applications* **53**, 74-90. [Crossref]
7. Munyaradzi Gudo, Keshnee Padayachee. SpotMal 1-6. [Crossref]
8. Shu Chen Yang, Wei Ting Chang, Yi Ting Hsiao, Bo Yu Chen. The Effects of Perceived Value on Facebook Post Sharing Intention 444-450. [Crossref]
9. Torsten J. Gerpott, Sabrina Berg. 2012. Präferenzen für Pay-As-You-Drive-Versicherungsmerkmale bei Privatkunden — Eine conjoint-analytische Untersuchung —. *Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung* **64**:4, 456-492. [Crossref]
10. Xin Tan, Li Qin, Yongbeom Kim, Jeffrey Hsu. 2012. Impact of privacy concern in social networking web sites. *Internet Research* **22**:2, 211-233. [Abstract] [Full Text] [PDF]
11. Ulrike Hugl. 2011. Reviewing person's value of privacy of online social networking. *Internet Research* **21**:4, 384-407. [Abstract] [Full Text] [PDF]
12. S. Arunkumar, A Raghavendra, D Weerasinghe, D Patel, M Rajarajan. Policy extension for data access control 55-60. [Crossref]