

# A Critical Approach to Privacy Research in Ubiquitous Environments – Issues and Underlying Assumptions

Maria Karyda<sup>1</sup>, Stefanos Gritzalis<sup>1</sup>, and Jong Hyuk Park<sup>2</sup>

<sup>1</sup> Dept. of Information & Communication Systems Engineering, University of the Aegean, Greece

{mka, sgritz}@aegean.gr

<sup>2</sup> School of Computer Engineering, Kyungnam University, Masan-si, Kyungnam-do, Korea  
parkjonghyuk@gmail.com

**Abstract.** This paper explores the different aspects of ubiquitous environments with regard to the protection of individuals' private life. A critical review of the relative research reveals two major trends. First, that there is a shift in the perception of privacy protection, which is increasingly considered as a responsibility of the individual, instead of an individual right protected by a central authority, such as a state and its laws. Second, it appears that current IT research is largely based on the assumption that personal privacy is quantifiable and bargainable. This paper discusses the impact of these trends and underlines the issues and challenges that emerge. The paper stresses that, for the time being, IT research approaches privacy in ubiquitous environments without taking into account the different aspects and the basic principles of privacy. Finally the paper stresses the need for multidisciplinary research in the area, and the importance that IT research receives input from other related disciplines such as law and psychology. The aim of the paper is to contribute to the on-going discourse about the nature of privacy and its role in ubiquitous environments and provide insights for future research.

**Keywords:** Ubiquitous Computing, Privacy Protection, Privacy Rights, Asymmetry of Power, Asymmetry of Information.

## 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 which 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.

It has been suggested that security and privacy are among the major obstacles that do not allow the proliferation of ubiquitous applications. The concept of privacy is not new and can generally be defined as the individuals' ability to control the terms by which their personal information is collected and used. It is also widely acceptable

that privacy protection is of critical importance both at the individual and at the society level.

Although research on privacy in the area of ubiquitous computing expands in many different directions and covers various topics, privacy issues are still open and it appears that feasible and effective solutions are still quite far from being realized.

A critical analysis of current research on privacy in ubiquitous environments reveals 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 [1]; 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. Another finding, stemming from the analysis of relevant research, is that privacy is viewed as a quantifiable attribute that can be negotiated and possibly exchanged by individuals in return for certain benefits.

This paper examines these assumptions and explores their implications with regard to fair information practices. The aim of the paper is to contribute to the on-going discussion about privacy in the area of ubiquitous computing and to substantiate the importance of a multidisciplinary approach and the value of input from related fields.

The rest of the paper is structured as follows: Section two presents an overview of the field, focusing on the particular characteristics of ubiquitous environments and the basic principles for privacy and data protection. Section three identifies the major streams of research in ubiquitous computing with regard to privacy and section four discusses the implications of the underlying assumptions that prevail in privacy research. Finally, section five presents our conclusions and provides suggestions for future research.

## 2 Background

### 2.1 Characteristics of Ubiquitous Environments

A ubiquitous computing environment, also known as pervasive, is typically envisioned as a space populated with 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 or human elements since it is humans who receive services and interact with each other. Thus, ubiquitous environments span both the physical and the logical space. The physical space is the realm of the human staff, the devices and locations, whereas in the logical space actions are performed through the software. Up to now and by far, the vision of ubiquitous computing is mainly hardware-driven [2]. 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.

An important attribute for ubiquitous applications is *context awareness*. 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. In some cases, context may also include information on the biometrics of 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 [3]. The author of [4] extends the concept of context, stating that it also means the *history* of all of these parameters. Context-awareness, in general, refers to the ability of computing systems to identify and adapt to their environmental context.

Another major characteristic of a ubiquitous environment is the dynamic nature of the use of services as well as the changes in the location. Furthermore, 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 [5].

## 2.2 Privacy

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 [1]. Privacy has also been defined as the right “*to be left alone*” [6]. Generally, many different types of privacy have been identified, including bodily, territorial, communication and informational privacy. In a digital environment, privacy can be defined as the individuals’ ability to control the terms by which their personal information is collected and used. Under this perspective, privacy implies control over personal information. Privacy rights are recognized in relation to an identifiable individual. Up to now, the basic approaches that have been 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 general EU Directive 95/46/EC on personal data protection. This Directive and its amendments regulate 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 United States 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 web sites 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 [6].

The basic and most commonly accepted principles for respecting an individual’s privacy include the elements of *necessity*, *finality*, *transparency* and *proportionality*.

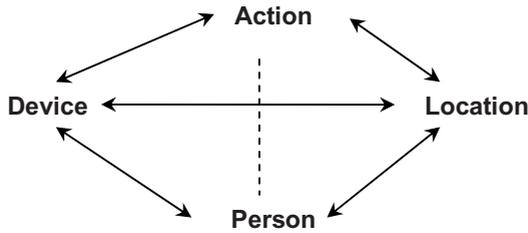
*Necessity* refers to the identification of purposes and benefits for identifying, or using personal information and also involves the considerations of possible alternatives. The principle of *finality* refers to the collection and use of personal data for specific and explicit purposes, which must 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 types and extend of personal data that is collected and used with regard to the pursued objectives. In other words, personal data collected should be relevant and appropriate with the aims of the UC system. It should be noted that the concept of privacy is culture dependent and no universal agreement as to its content exists; however, among these privacy principles, *necessity* is the one that is the most generally accepted.

The paradigm of fair information practices, which is a regulatory paradigm defining how personal information should be collected and treated, includes *notice* of users, *choice* over how their personal information is used, the *right to access* collected information, reasonable *security* of the information and *accountability* of the collector's side [7]. The author of [8] proposes the following set of principles for guiding privacy-aware ubiquitous system design: (a) Notice: users should always be aware of what data is being collected; (b). Choice and Consent: users should be able to choose whether their personal data is used; (c) Anonymity and pseudonymity should apply when identity is not needed; (d) Security: different amounts of protection depending on the situation; and (e) Access and recourse: users should have access to data about them.

### 2.3 Privacy in Ubiquitous Environments

Ubiquitous computing is populated both by privacy enhancing technologies and privacy decreasing 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 the latter; 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.



**Fig. 1.** The privacy diamond [9]

The privacy diamond shows [9], as depicted in Figure 1, that in ubiquitous environments (smart) devices operate between the individual and the information system or service provider. For this type of interaction to be realized some sort of identification is needed. Distinction should be made between devices that enable user request services from the system and devices that function automatically. 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.

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.

To further discuss and comprehend the issue of privacy in the context of ubiquitous computing, we need to identify the stakeholders involved. In the first place, individuals, whose personal data are continuously monitored, collected and manipulated, are the major interested parties with regard to privacy protection. Other involved stakeholders include: IT industry, which provides the technical infrastructure and the privacy enhancing and privacy degrading tools; Organizations, or generally service providers that exploit the capabilities provided by ubiquitous computing to deliver services to individuals; and Governments, legal and regulatory authorities that provide the framework for privacy protection.

A major difficulty in the global digital environment where ubiquitous computing applications are realized is that the regulation approach based on legislation has very limited impact and thus limited effectiveness. 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. Standardization efforts with regard to privacy protection are still at an early stage and could more appropriately be characterized as ‘recommendations’. Finally, the effectiveness of privacy seals is also difficult to be evaluated, since on line visitors as a rule lack the knowledge and necessary information to evaluate the protection provided by them.

It has been argued that privacy threats in ubiquitous environments are minimized due to the large number of devices in use, which make individual signals identification difficult. If millions of people use many different UC devices at home, on the road, at work or on their body, then the result will probably be “privacy by obscurity”. However, technically it is still achievable to filter information on a specific individual, especially if sophisticated technology is used. Thus, privacy remains an open issue, even if not as a generalized threat [2].

### **3 Streams of Privacy Research in Ubiquitous Computing**

#### **3.1 Digital Identities and Identity Management**

In the physical world, identities distinguish one person from the other and are used as evidence for various purposes, such as access to services, authorizations, rights etc. For this reason, an identity typically comprises an aggregation of a person’s unique characteristics. On the logical sphere, the concept of ‘digital identity’ or ‘on-line identity’ or ‘virtual identity’ has emerged to connote personal data in digital form, such as, for example, usernames, passwords, tokens, PINs etc.). Digital identities are typically used in a similar way to physical ones: individuals receive services or are granted access, rights and privileges and according to their identity. However, in a digital environment individuals can have multiple digital identities, depending on their different roles. Consequently, a digital identity should not be equally treated or taken for granted as an identity in the physical world.

In ubiquitous environments, the digital identity is a concept mostly used to describe the appearance of a user, or a human entity. Such data are both generated by the infrastructure (for instance the MAC- or IP-address, which are automatically provided by the applications or the operating system) and the individual (e.g. by filling in forms with name and address, as well as other personal data, such as preferences). The “digital identity” is thus a construct of the receiver; the sender can only influence it by restricting the amount of personal data sent [2]. Virtual identities can be managed, created or abolished at the user’s will. Thus, virtual identities can be used as pseudonyms, and in this way function as privacy enhancing techniques due to their level of indirection between the real-world identity and the electronic data. It is generally known that opportunities to create fictitious virtual identities are highly exploited in the digital world not only for reasons of convenience and leisure, but also as a means to protect one’s privacy.

Identity management refers to the rules and procedures followed for manipulating different digital identities. Currently, many products and solutions are available on the market with regard to identity management: they provide different functionality ranging from provisioning and accounting, authentication, authorization to data consolidation.

### 3.2 Privacy Preserving Approaches

The “Platform for Privacy Preferences Project (P3P)” approach [10] 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. The authors of [11] propose a general, component-based platform that functions as a middleware service that allows users apply general policies to control distribution of their information.

PawS [12] is a privacy awareness system for ubiquitous computing environments, which like P3P, provides users with tools in order to facilitate them protect their personal privacy. Its basis is primarily social and legal rather than technical. PawS uses privacy beacons that announce the privacy policies to user who enter 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 [13] and depend on context [14].

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.

## 4 Discussion

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, be setting privacy preferences and by making decisions, automatically supported in most cases, on whether information practices are acceptable or not at each case.

This approach however, suffers the following limitations: it is very hard for the users to make an *informed choice*, 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 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 web sites.

Another basic stream of privacy research in ubiquitous environments embraces the opinion that user perceptions of risk and benefit can determine their willingness to adopt technology. Multiple research endeavors explore the hypothesis that people are more likely to accept potentially invasive technology if they think its benefits will outweigh its potential risks [15, 16].

Privacy 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 [6]. 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. Privacy is not merely a right possessed by individuals; it is a form of freedom built into the social structure [17].

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 [18]. 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*" [19].

Moreover, in ubiquitous environments the distinction between the private and the public sphere is blurred; fair information practices and legal frameworks for data protection have a point of reference; that is they apply in the public or the private sphere.

Since we have defined the concept of privacy as the individuals' ability to control the terms by which their personal information is collected and used, it is natural to draw the conclusion that privacy is closely related to the concept of *control*. However, in a dynamic and highly volatile environment, 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.

## 5 Conclusions

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.

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. However in the ubiquitous environment this issue is still not resolved, neither technically nor conceptually, meaning that there is not yet a clear and generally accepted idea of exactly privacy protection in a dynamic, pervasive environment means.

Up to now privacy research is dominated by a pure technical perspective, where the subtleties and deeper meanings and implications technology can have are not further examined. This paper has provided a critical analysis of research in the field of UC privacy, aiming to bring in the foreground hidden assumptions and discuss their implications. Our analysis of current research approaches has revealed two underlying assumptions which are commonly and unquestionably accepted by IT researchers: first, that privacy protection is the user's responsibility and second that privacy is considered 'bargainable' and 'quantifiable'. The main implication of these assumptions is that the protection of individual privacy in ubiquitous environments is envisioned that can be managed, even exchanged, in a distributed and measurable way; this, however, contradicts with the fundamental privacy and data protection principles that are currently supported. For this reason, this paper has argued that there is an imperative need that privacy research with regard to ubiquitous applications is informed and enriched with insight from other related fields, for instance law and psychology. Thus, a multidisciplinary approach is needed; researchers need to 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.

## Acknowledgments

Jong Hyuk Park's research work was supported by Kyungnam University, Korea.

## References

1. Dumortier, J., Goemans, C.: Roadmap for European Legal Research in Privacy and Identity Management, Interdisciplinary Centre for Law and ICT (ICRI), K.U. Leuven (December 2002)
2. Eymann, T., Morito, H.: Privacy Issues of Combining Ubiquitous Computing and Software Agent Technology in a Life-Critical Environment. In: Proceedings of the IEEE International Conference on Systems, Man and Cybernetics (2004)
3. Crowley, J.L., Coutaz, J., Rey, G., Reigner, P.: Perceptual Components for Context Aware Computing. In: Borriello, G., Holmquist, L.E. (eds.) UbiComp 2002. LNCS, vol. 2498, Springer, Heidelberg (2002)
4. Persson, P.: Social Ubiquitous Computing. In: Workshop on Building the Ubiquitous Computing User Experience, ACM/SIGCHI, Seattle (2001)
5. Čas, J.: Privacy in Pervasive Computing Environments – A Contradiction in Terms? IEEE Technology and Society Magazine, 24–33 (Spring 2005)
6. Grizalis, S.: Enhancing Web Privacy and Anonymity in the Digital Era. Information Management and Computer Security 12(3), 255–288 (2004)
7. Center for Democracy and Technology, Fair Information Practices, <http://www.cdt.org/>

8. Langheinrich, M.: Privacy by design – principles of privacy-aware ubiquitous systems. In: Abowd, G.D., Brumitt, B., Shafer, S. (eds.) *UbiComp 2001*. LNCS, vol. 2201, pp. 273–291. Springer, Heidelberg (2001)
9. Zugenmaier, A.: *Anonymity for Users of Mobile Devices through Location Addressing*. Rhombos Verlag, Berlin (2002)
10. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, World Wide Web Consortium (September 2001), <http://www.w3.org>
11. Miles, G., Friday, A., Davies, N.: Preserving Privacy in Environments with Location-Based Applications. *Pervasive Computing*, 56–64 (2003)
12. Langheinrich, M.: A Privacy Awareness System for Ubiquitous Computing Environments. In: Borriello, G., Holmquist, L.E. (eds.) *UbiComp 2002*. LNCS, vol. 2498, pp. 237–245. Springer, Heidelberg (2002)
13. Jiang, X., Hong, J.I., Landay, J.A.: Approximate Information Flows: Socially Based Modeling of Privacy in Ubiquitous Computing. In: Borriello, G., Holmquist, L.E. (eds.) *UbiComp 2002*. LNCS, vol. 2498, pp. 176–193. Springer, Heidelberg (2002)
14. Kobsa, A., Schreck, J.: Privacy through Pseudonymity in User-Adaptive Systems. *Transactions on Internet Technology* 3(2), 149–183 (2003)
15. Beckwith R.: Designing for Ubiquity: The Perception of Privacy. *Pervasive Computing*, 40–46 (April-June 2003)
16. Hann, I., Hui, K., Lee, T., Png, I.: Online Information Privacy: Measuring the Cost-Benefit Trade-Off. In: *Proc. of the 23rd International Conference on Information Systems* (2002)
17. Solove, D.J.: A taxonomy of privacy. *University of Pennsylvania Law Review* 154(3), 477–564 (2006)
18. Rodota, S.: Privacy, freedom and dignity – Closing remarks at the 26th International Conference on Privacy and Personal Data Protection, Wroclaw (16.09.2004)
19. Lasprogata, G., King, N., Pillay, S.: 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*, 4 (2004), [http://stlr.stanford.edu/STLR/Article?04\\_STLR\\_4](http://stlr.stanford.edu/STLR/Article?04_STLR_4)