AN ABSTRACT OF THE PROJECT OF

Riad Lemhachheche for the degree of Master of Science in Industrial Engineering presented on June 7, 2006.

Title: Management and Deployment of Ubiquitous Computing Environment

Abstract approved:

J. David Porter

Designing a ubiquitous computing (Ubicomp) system involves more than just designing computing devices or services to satisfy user needs. To successfully integrate the user with an Ubicomp system, there is a need to integrate all the aspects of the user's experience with the system.

New practices and design principles need to be defined to help the transition from the focus on pure technological improvements to an enhanced user experience of computing.

The main objective of this research was to identify the critical design questions that will support the activity of designing, deploying and maintaining an Ubicomp environment. To achieve this objective, a framework that encompasses the main design requirements of an Ubicomp environment was first developed. These design requirements

were synthesized from the literature to unveil the components' impact on the user experience within an Ubicomp environment.

A second objective was to show how a multidisciplinary perspective on the design of an Ubicomp environment is not only beneficial but fundamental to improve the user's experience. For this purpose, the developed framework was applied on a wireless local area network (WLAN) infrastructure to illustrate how future information system designers will have to deal with usability, legal, economic and social perspectives to achieve successful systems designs.

An online survey on the use of Wi-Fi was used to evaluate some of the findings obtained from the application of the framework. Survey results confirmed that a multidisciplinary approach to the evaluation of Wi-Fi network design could identify user experience issues and provide insights to solutions. Issues that were identified include the lack of distinction between privacy and security, the mismatch between the information available to the user and the one expected from him, and the confusion surrounding the legal implications of open Wi-Fi access.

In summary, the design framework applied to an Ubicomp environment helped identify some of the design issues in regard to the user experience.

Management and Deployment of Ubiquitous Computing Environment

by

Riad Lemhachheche

A PROJECT

Submitted to

Oregon State University

In partial fulfillment of

the requirements for the

degree of

Master of Science

Presented June 7, 2006

Commencement June 2007

Master of Science project of Riad Lemhachheche presented on June 7, 2006

APPROVED:

Major Professor, representing Industrial Engineering

Head of Department of Industrial and Manufacturing Engineering

Dean of Graduate School

I understand that my thesis will become part of the permanent collection of Oregon State University libraries. My signature below authorizes release of my thesis to any reader upon request.

Riad Lemhachheche, Author

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my major professor, Dr. J. David Porter, for his close advising and strong guidance throughout my thesis writing process and my stay here at Oregon State University. I also thank Dr. Porter for giving me the opportunity to work with him both on academics and on research. I would also like to thank my minor professors, Dr. Erik Larson, Dr. Toni Doolen for being part of my defense committee and taking the time to revise my document.

I would like to thank all the professors from whom I have received instruction here at OSU for the valuable knowledge and experience I have gained. Also, thanks to the administration of the Department of Industrial and Manufacturing Engineering for the continued support and advising during my studies.

Special thanks to Dr. Lawrence Lessig, Dr Carlos Jensen, Dr Anthony Townsend and Dr Bill Loges for their help in extending the breath of my knowledge to new areas. Special thanks to Margaret Mellinger and the librarians at OSU Libraries for their help with the numerous research resources I requested.

Thanks to my family and friends in the distance for their continued support during all these years that I have been away from home.

DEPLOYMENT OF SERVICES IN A UBIQUITOUS COMPUTING ENVIRONMENT

TABLE OF FIGURES

1. Introduction

"*The most profound technologies are those that disappear*" [111]. This is how Mark Weiser, then a senior researcher at Palo Alto Research Center (PARC), described the computer of the future in his article titled "The Computer for the 21st Century" published in 1991. This publication, recognized by the Institute for Scientific Information as a "Citation Classic", explains why Weiser is considered by the human-computer interaction community as the founder of the field of ubiquitous computing. Ubiquitous computing can be formally defined as the integration of computing in the environment rather than considering computers as separate entities. Instead of being a world on its own, computing equipment and information technologies become part of the environment. Ubiquitous computing (or Ubicomp, for short) is also referred to as pervasive computing, ambient intelligent computing or invisible computing.

1.1. From ENIAC to Ubiquitous Computing

In their early days, computers and computing devices were limited in number and in the array of possible uses. Computers were first employed for scientific research, especially complex calculations. The Electronic Numerical Integrator And Compute (ENIAC) designed in 1946 was the first all-electronic computer [50]. ENIAC was able to perform up to 5,000 simple additions or subtractions and was mainly used by the military to calculate ballistic trajectories. ENIAC was a one of a kind design that weighed 27 tons, took up 167 squared meters and consumed 160 kilowatts of power. The only way to reprogram it was by physical rewiring. Between 1950 and the mid-1970s, inventions such as programming languages, operating systems and the transistors transformed the computer from a highly expensive, highly specialized and voluminous machine to a multi-purpose, more compact equipment affordable by large and mid-size companies. Following that trend, microcomputers, aimed at home users, started to appear in the mid 1970s [84]. The field of computing was once again revolutionized in 1981 with the introduction of the first Personal Computer (PC) by IBM. The PC was named “Person of the Year” by Time Magazine in 1982. From there on, computers were no longer limited to business and industrial settings but started to gain acceptance into homes for applications such as word processing, accounting and gaming.

The World Wide Web [18], a technology to link simple content distributed over networks like the Internet, started to become popular around 1994. The Internet grew from less than half a million users in 1994 to more than 850 million by early 2005 [57]. Since 1965, the number of transistors per square inch on integrated circuits has double every 18 months [77] allowing computing devices to be integrated in virtually any manufactured product. Machines that were considered supercomputers a couple of years ago are now considered commodity devices that are small enough to fit in somebody's pocket. Advances in low power wireless communication such as Wireless Fidelity (also known as Wi-Fi) make it possible to wirelessly link a wide variety of devices [83]. As mobile computing allows for easier access to computing services and information from any location and at anytime, it constitutes an opportunity for radical changes from what “used to be accessible only while users were tethered to a computer at home or in an office” [21].

As computers become an integral part on most people's lives and provide support to an increased number of human activities, the computers and associated computing devices need to be tightly integrated into people's environment. Ubicomp is the field of research interested in this relationship, seeking to bring a new vision to computers, networks and their applications [113]. The path towards building and deploying an Ubicomp environment can be formally defined as "saturating an environment with computing and communication capability, yet having those devices integrated into the environment such that they 'disappear'" [52].

The vision of Weiser [111] is now closer to becoming a reality thanks to several advances in computing technologies and related fields. The computer of the pre-Ubicomp era possessed most of these characteristics:

- Required more or less specific hardware and software (until 1981, different computers brands were not compatible).
- It was expensive.
- It was considered a single point of access. Most of the time, applications and data saved on a computer could only be accessed on this computer.
- Possessed limited in storage capability [72].

The emergence of wireless and mobile computing, data exchange standards with distributed system technologies, the Internet and a phenomenal drop in prices have made computing something closer to a commodity. As the Internet reduced the physical and geographical constraints associated with computing activities, information can now be easily accessed and shared between computer, laptop and mobile phone [24]. Thanks to these advances, researchers in the field of Ubicomp have a better opportunity to study "the informal and unstructured activities typical of much of our everyday lives" [3] and try to integrate them more tightly with our computing environment.

1.2. Motivation of the Research

The Ubicomp research tries to depart in some ways from the traditional concept of computing. First, it requires a user-centered approach to study human-computer interaction that emphasizes activities rather than tasks. Its goal is to bring the user and its needs to the foreground while keeping the computing environment that supports the user in the background.

The theory of diffusion of innovation [91] has proved that every innovation follows a S-shaped curve in regard to diffusion. In regard to technology, this diffusion process progresses from "consumers want more technology, better performance" to "consumers want convenience, reliability, low cost…"[81]. Market researchers explain the concept of overshooting [26] where "the pace of technological progress frequently exceeds the rate of performance improvement that mainstream customers demand or can absorb. As a consequence, products whose features and functionality closely match market needs today often follow a trajectory of improvement by which they overshoot mainstream market needs tomorrow" [27]. As shown on Figure 1, computing has reached a stage of maturity in terms of technology and therefore research should shift to improving the user experience associated to computing activities. This shift implies a complete reconsideration of the relationship between users and computing resources. New practices and design principles need to be defined to help the transition from the focus on pure technological improvements to an enhanced user experience of computing.

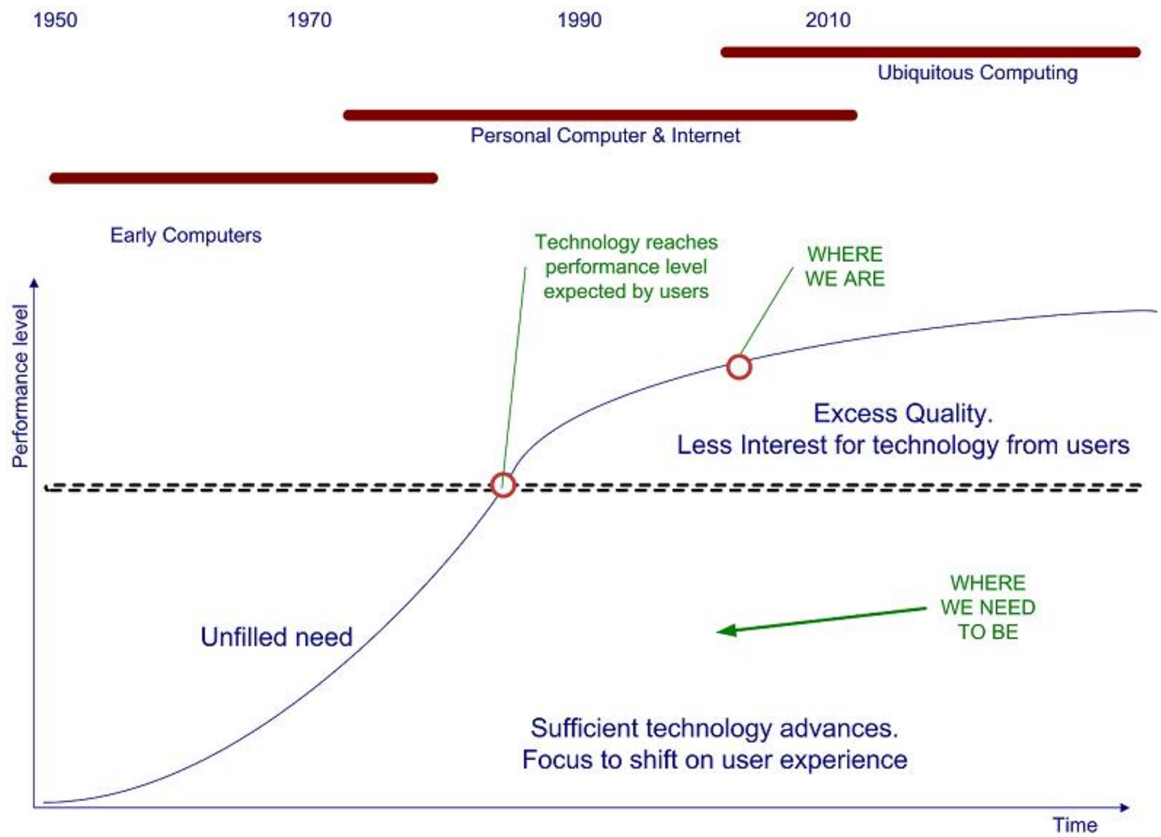


Figure 1. Needs-Satisfaction Curve of Computing (Inspired by Norman 1998)

Therefore, there is a need for a pluridisciplinary approach to integrate social factors such as context, privacy and adaptation with computer engineering and information technologies. While researchers have isolated most of the social and technological requirements for Ubicomp to come closer to reality, a framework of design principles relying on social, technological as well as legal aspects of the user experience is yet to be defined.

1.3. Research Objectives

According to the literature review, the user experience in a computing environment is dependent upon aspects that reach beyond and across several scientific disciplines. While technology plays an important role in fulfilling a user's computing needs, designing a successful ubiquitous environment requires for the technology to be supported (if not balanced) by the social, legal and economic forces that put constraints on any system as defined by Lessig [69]. This complex set of relationships is illustrated on Figure 2.

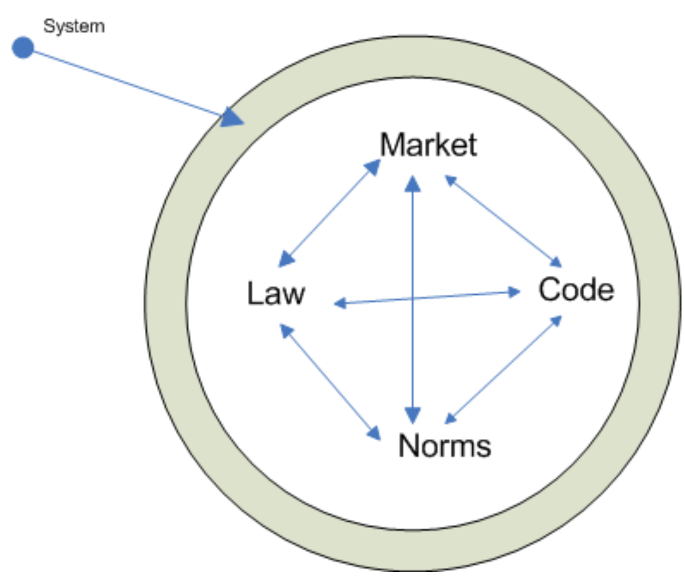


Figure 2. Forces Affecting a Computing System (Lessig)

All of the forces depicted in Figure 2 have an important impact on how the field of Ubicomp will develop and how an Ubicomp system will be designed. Therefore, the main objective of this research was to identify the critical design questions that will support the activity of designing, deploying and maintaining an Ubicomp environment. To achieve this objective, a framework that encompasses the main design requirements of an Ubicomp environment was first developed. These design requirements were synthesized from the literature to unveil the components' impact on the user experience within an Ubicomp environment.

A second objective was to show how a multidisciplinary perspective on the design of an Ubicomp environment is not only beneficial but fundamental to improve the user's experience. For this purpose, the developed framework was applied on a wireless local area network (WLAN) infrastructure to illustrate how future information system designers will have to deal with usability, legal, economic and social perspectives to achieve successful systems designs.

2. Literature Review

Designing a ubiquitous computing (Ubicomp) system involves more than just designing computing devices or services to satisfy user needs. To successfully integrate the user with an Ubicomp system, there is a need to integrate all the aspects of the user's experience with the system [16]. This can be done by reviewing how all the diverse technologies being researched, as well as requirements set on the system by users, can interact and be integrated to make the experience successful.

Technology advancements like distributed computing or context-aware systems provide the foundation to build a Ubicomp system as long as they are balanced with the users' requirements and expectations, such as privacy concerns and user-centric design. As a matter of fact, the location of the "user interface" has been pushed farther and farther out of the computer itself, deeper into the user and the work environment" [51]. In consequence, innovative design techniques need to be used to address the interactions between the user and the computing environment.

Table 1 shows a compilation of prototype Ubicomp environments developed by several different research institutions in the US. All these projects make extensive use of new technologies to provide users with more control over their environment and they provide some insight on what the future of computing may bring. Despite the fact that each of the projects shown in Table 1 has different goals and follows specific procedures to reach these goals, they all emphasize the user experience. Therefore, by drawing from their results, it can be better understood how to come closer to building an "ideal" Ubicomp environment.

Table 1. Selected Major Projects in Ubiquitous Computing

Name	Location	Start Date	Goals	Specifics
PARCTab	Palo Alto Research Center	1992	Palm-sized computers communicating wirelessly to	Portable. Constant Connectivity. Location reporting
Active Badge (Bat)	AT&T Labs Cambridge	1992	Locate colleagues and route phone calls	Use sensor networks and radio transmitters
Classroom 2000 / eClass	Georgia Institute of Technology	1996	Prototype classroom environment. Seamlessly capture rich interaction	Web pages with timelines, electronic whiteboard, audio and video. Automatic
Advanced User Resource Annotation system	Microsoft	2000	Build a collectively authored database rating, reviewing and commenting on a wide	Access and author annotations on objects and places using machine readable tags
Cooltown	HP Labs	2000	Web technologies to support users in their interaction with their	Every resource is associated to a web page. Support for
Oxygen	MIT	2000	Interaction through Speech and Vision Automation Knowledge Access Collaboration	Support for: Distributed Computing Mobility Personalities
Labscape	University of Washington	2001	Provide cell biology researchers with tools to support collaboration and	Recording of lab sessions following scientist configuration. Later access and

The PARCTab project shown in Table 1 was one of the first research projects related to mobile computing. PARCTab had two main goals:

1. To give people a continuous, always-on connectivity to their data and applications,
2. To enable employees to locate their colleagues within the research lab.

The first goal was successfully achieved. The second goal, however, could not be achieved due to the lack of mobility of the devices available at the time and the fact that the testing was constrained to a small geographic location. Similarly, the Active Badge project researched the effect of location capabilities in corporate settings. One of the factors that became critical in both of these projects was the privacy concern associated with the availability of real-time localization.

While privacy concerns were not really the major focus of these projects, it surfaced later on in projects like Oxygen or Cooltown where the privacy implications were a main component of the study. For example, the privacy issues identified in PARCTab included:

- Centralized architectures require users to trust the operators of the service, both to properly use location data and to sufficiently protect it;
- End-user control over location data should provide more granularity than a binary on- or off-switch, and should allow control over when, to whom, and how much location information is shared;
- Users want to know when and to whom systems share their user location information. [55]

The privacy concerns grew large enough that several research groups are focusing their research on this topic and a series of workshops have been organized every year since 2002 on the topic at Ubicomp, the conference dedicated to the study of ubiquitous computing.

Another area that has emerged from this initial research is the subfield of context-aware computing. Context-aware computing focuses on understanding what information a Ubicomp system should collect and organize on behalf of its users. Projects like Classroom 2000, Cooltown, AURA and Labscape are examples of such system awareness to its context. While Cooltown and AURA were trying to capture the details of everyday life, Classroom 2000 was focused on being able to replicate college classroom experience and Labscape was interested in supporting a biology laboratory setting.

While privacy and context awareness have proved to be areas of research in regard to designing an Ubicomp system, the main goal of such a system is to make computing invisible [111-113]. All of the projects shown in Table 1 share the vision of ultimately making computing devices and services an afterthought for their users. The capacity of adaptation will make "machines that fit the human environment, instead of forcing humans to enter theirs." [111]

2.1. Parameters that Affect Ubiquity

Based on the research projects shown in Table 1 , three elements can be said to define the promises and challenges faced by an Ubicomp environment. These elements are privacy, adaptation and context and their relationships are depicted on Figure 3. Figure 3 also shows that there are other sub-elements in an Ubicomp environment that affect the interaction of the main elements described above. For example, memory and filtering are sub-elements that influence the interaction between context and adaptation, whereas laws and norms play a role in the interaction between privacy and adaptation. Interactive learning and user control, on the other hand, are sub-elements that have an influence on the interaction of all the main elements.

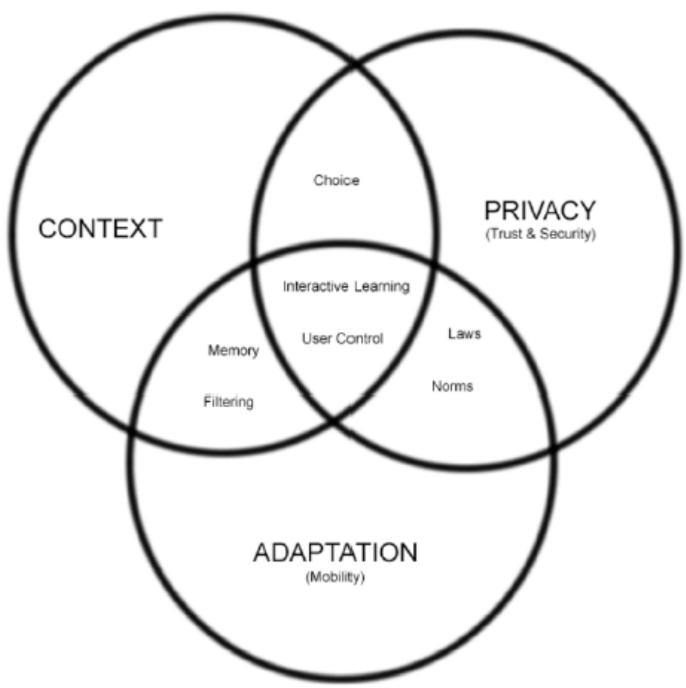


Figure 3. Simplified Model of an Ubiquitous Computing Environment

2.1.1. Context Awareness

The concept of context aware computing applications was first formalized after Mark Weiser's vision in the beginning of the 1990's as "software that examines and reacts to an individual's changing context" [96]. A computing system is said to be context-aware when it has the ability to adapt its behavior based on specific characteristics in which it is operating at the time. Such characteristics are not only limited to geographic location [98] but can also be user identification, time, device, language or any settings previously configured by or for the system user.

Figure 4 shows that computing has moved from the mainframe, where many people access one device, to the personal computer era and then to the Ubicomp era (i.e., many devices, one person)[112]. Even if the timeline fixed by Weiser for the adoption of Ubicomp proved to be inaccurate, the "tipping point" [91] for its adoption may not be too far ahead of us.

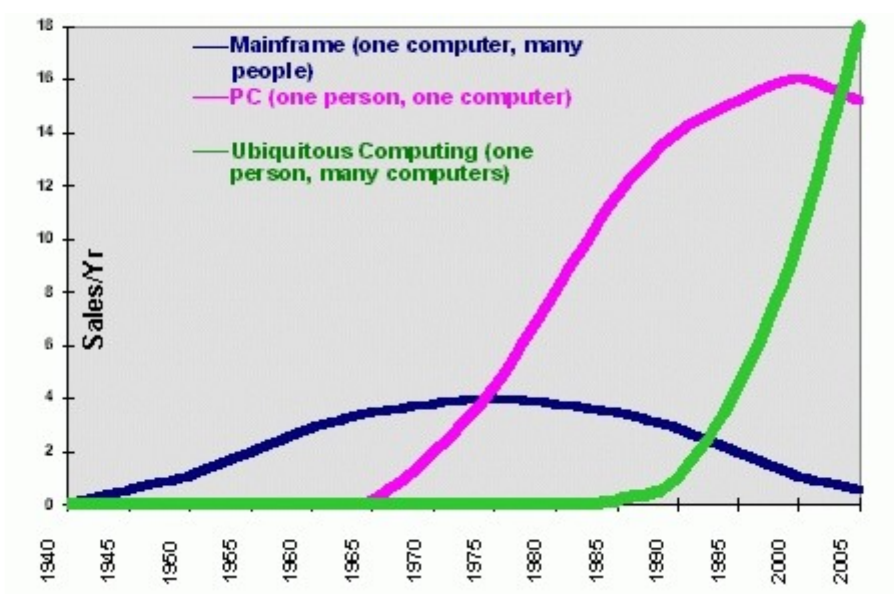


Figure 4. Major Trends in Computing (Xerox PARC, 1995)

As exemplified by personal Internet portals such as Yahoo! [70], the focus of the interaction moved from the device to the user and the notion of context needed was then redefined to more closely match the concept of “one person, many computers” [96]. The characteristics of context in information systems have in consequence become highly dependant on the surrounding environment. Therefore, context can be better defined as “any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves” [36]. Dey warns against trying to enumerate all the aspects of context to be considered as important, since these will change from situation to situation. The Context Toolkit [93] is therefore aimed at facilitating the design and deployment of context-aware applications. According to this project, context-aware applications need to support at least the following features:

- **Independence of application operation from context-aware system**: The system in charge of managing context should perform independently from the application it may serve.
- **Storage capability**: Historical information is an important part of context; therefore storage of support should be provided.
- **Distributed architecture of context-aware system**: Devices that sense context can differ from the ones that run the application.
- **Aggregation support**: A central application, named context aggregator, needs to collect the entire context for a particular entity.

2.1.1.1. Context Awareness and Interactive Learning

One of the challenges of context awareness is to make the best use of all the information available concerning the user and its current context. While this kind of information is often already available in digital form, the challenge becomes to properly link the different elements of context based on the current situation. To reach a state of "situation abstraction" where the context can be determined dynamically from the state of the different entities of the system, an environment needs to be setup to learn not only about context, but also to learn *from* context [36].

The first step towards learning from context is to gain the ability to precisely associate different elements of context with the user. A large amount of research has been dedicated to defining frameworks and systems for capturing context information using, for example, sensor networks and automatic data capture technologies. Examples include PARC's computer [111], HP CoolTown [60] and UW Labscape [8] where an emphasis was placed on the user-system relationship; this is, the system learned as the user performed activities and the user was kept informed by the system based on available context. The Cooltown project, for example, gave users the control over linking between elements of context. Each resource, whether it is a physical component or a service, was associated to a web page and accessed through a portal (known as "place manager"). Such systems show successful designs of environments able to capture contextual user data through automatic data capture or sensors networks.

2.1.1.2. Context Awareness and User Control

Privacy requirements and user control coupled with context capture show the need for a multi-level design regarding context capture and personal information disclosure [4]. It emphasizes that the balance between the intelligence of the environment and user involvement cannot be set globally. Mechanisms to link context acquisition and context use should also be designed since there is a need to "agree on representations" of context [97]. This could only be achieved by putting users in control.

2.1.1.3. Context and Choice

As a consequence, an interactive level system in regards to context awareness, data capture and privacy is a more realistic approach in this regard [66]. A study done by the Graphical User Interface Research (GUIR) group at the University of California Berkeley shows that factors such as inquirer and situation can be associated with different levels of privacy preferences among users. Interaction between the user and the system in regard to context management can even be defined according to three levels: personalization, passive context-awareness and active context-awareness [9].

In order to manage users' preference in terms of personal context information disclosure, an efficient Ubicomp environment should be able to remember user's preferences.

2.1.1.4. Context and Memory

Therefore, context awareness needs to be supported in the environment in terms of memory. Context awareness would provide continuity of experience to the user only if the system can remember previous user's experiences and have the ability to exploit them properly [93]. The environment should support intelligent capture, collaboration [22] and efficient data exchanges between the different components of the Ubicomp system. As a matter of fact, memory is also important to support the fact that actions have often neither clear beginning nor clear end. Actions may also be interrupted by the user at any point to be resumed later [2].

The wealth of information available to collect and organize concerning a user and its interactions with the system would prove to be helpful in providing greater user integration with the environment.

2.1.1.5. Context and Information Filtering

The Ubicomp system should also protect users from information overload. Research has been conducted to optimize interactions between computing devices and the user based on location and anticipated user expectations. Examples include the Labscape project bringing ubiquitous computing to a cell biology laboratory [8]. Records of lab session settings and operations were made during experiments in the cell biology laboratory. If a particular session needed to be reviewed, the precise data of interest could be accessed based on the formal representation designed by system users and used in representing data collected during the experiment. As shown on Figure 5, this project provides automated capture of live experiences and a later access to these experiences that is adapted to the audience.

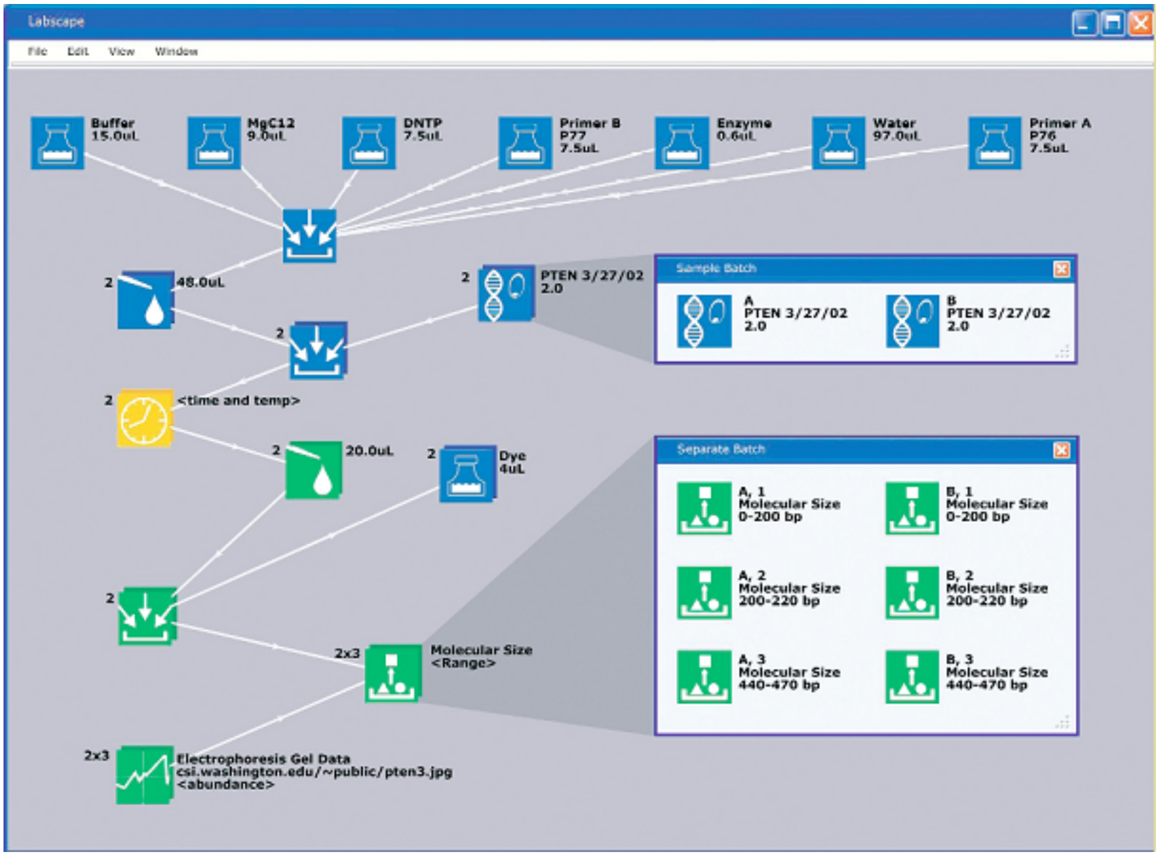


Figure 5. Screenshot of a Polymerase Chain Reaction Procedure in Labscape [8] © IEEE

Systems able to learn from their context can also help limit information. Technologies like collaborative filtering [54], also known as community knowledge, are able to match present and past experiences of the user with other users' to observe patterns and make predictions. Movie recommendation systems like MovieLens [32] learn users' tastes and try to match them with similar users in order to make more accurate recommendations. As the user enters more information, the service becomes more accurate and able to learn from the user's experience.

Context awareness of the system can only be made possible by obtaining relevant and up-to-date information from and about the user in the most efficient fashion.

Automatic data capture technologies such as sensor networks can provide this kind of information while minimizing the inconveniences experienced by the user. However, context awareness of a system would only be supported by the user if the data flow of information is well balanced with the user's rights to privacy.

2.1.2. Privacy

Privacy can generally be defined as "claim of individuals, groups or organizations to determine for themselves when, how and to what extent information about them is communicated to others" [114]. As interactions between the user and his computing environment now include practices such as location tracking [13] and log of personal transactions or phone calls, it raises questions about the preservation of personal privacy.

In the early days of computers, personal data collection was usually limited by system capabilities and physical location. Applications saved personal data in formats usually only understandable by the system where the data was created. These data would also rarely be accessed outside of the physical space surrounding the system where the data was generated. The Internet, web services and data exchange standards changed this since they "facilitate unobtrusive access, manipulation and presentation of personal data"[15]. In addition to facilitating information access across services, the separation of the user's experience from one particular device [33] means that information is no longer associated to a physical space and therefore privacy may be more easily compromised.

2.1.2.1. Privacy and Laws

In addition to trying to balance information flow and privacy rights, research about information disclosure management has to deal with culture specifics [14]. Indeed, laws considerably influence the degree of privacy that users can or are willing to release to an Ubicomp environment. For example, the Electronic Communications Privacy Act, an US law [39], provides only limited "expectation of privacy" in regard to communications made within companies [19]. Employers have the right to review employees' stored company voicemail and emails. Companies are allowed to distribute or sell employees' and customers' personal information to third parties [45]. In contrast, European Union laws such as EU 95/46/EC [108] give citizens more rights on how and what information can be collected and disclosed about them. The possibility to design a uniform solution for privacy demands is therefore highly unlikely. A study of personalized systems conducted at the University of California Irvine has concluded that "privacy will have to be dynamically tailored to each individual user's needs, and to the jurisdiction at both the location of the personalized system and that of the user" [64].

2.1.2.2. Privacy and Cultural Norms

Cultural norms can also affect the perception of privacy. Behavior can be influenced by community experiences since "as a community of users appropriates an innovation, the users develop and communicate norms about acceptable use, which can influence the behavior of their peers and subsequent generations" [30]. As the diverse technologies affecting the operation of an Ubicomp environment will diffuse, they may or may not gain acceptance among users and affect their behavior and sensibility toward their environment and their privacy.

One example of this evolution is materialized in the adoption of Internet etiquettes and the new phenomenon of unsolicited mail, commonly known as spam [29]. The Arpanet (and Internet consequently) was created in the 70s primarily as a communication tool. It was intended to enable researchers to exchange messages quickly regardless of their location. Mail programs included functionalities so that a user can communicate with several correspondents at once enabling him to send the exact same message to a large group of persons simultaneously. As this functionality was misused to send large number of commercial messages over the Internet starting in the mid-90s, new norms appeared regarding desirable and acceptable use of this functionality [86]. At first, the society tried to define norms on what constitutes spam and then regulations surfaced to combat this form of abuse. [67]

What constituted a normal form of communication earlier (entering in communication with people without being solicited) has been redefined to take into account advances in information technology to fight abuse that came from an automated process in the delivery of large amounts of messages over computer networks.

2.1.2.3.Privacy and User Control

The development of such a dynamic system would require user participation in managing the disclosure of personal information. Even if the goal is to make the system invisible to users [81], users should have the opportunity to control their privacy. Researchers have designed frameworks to provide users with feedback and control [15] but also explicit choices in terms of personal information that can be collected [4]. According to these researches, control needs to be applied on:

- **The capture**: when to and when not to give out what information
- **The construction**: what happens to personal information
- **The access**: who can access user's data
- **The purposes**: what people want information about the user for.

The user also expects feedback from the system about:

- **The notice**: clear notice of what type of information is collected, its use and which third party will have access to it
- **Security**: what measures were taken to secure data from unauthorized access.

Also, the system should take into account the fact that people may not want to show the same "face" [65] at anytime and anywhere. Extending on this idea of user control, the notion of faces is based on the fact that "people disclose different versions of personal information to different parties under different conditions" [49]. The availability of somebody's schedule or contact information while at work can be seen as acceptable; however, it could be deemed to be totally inappropriate when somebody is walking on the street or during weekends or vacation [66]. To ensure everyday privacy, the system needs therefore to be able to interact dynamically with the user through control and feedback to always provide the right amount of precision in information disclosed to the environment [65].

2.1.2.4.Privacy and Choice

User's privacy is an important feature to be supported and projects like MIT's Oxygen [75] are looking at ways to balance privacy and context-awareness in an Ubicomp system. The principle of face, described in the previous section, is based on the fact that users want control over their personal information. An Ubicomp system needs to manage privacy on two levels. First, users should be able to choose to disclose or not their personal information; then, they would have control over what, where, when and to whom. The interface for the "Everyday Privacy in Ubiquitous Computing" project at the University of California Berkeley introduced the concept of face that summarizes these types of disclosure (see Figure 6).

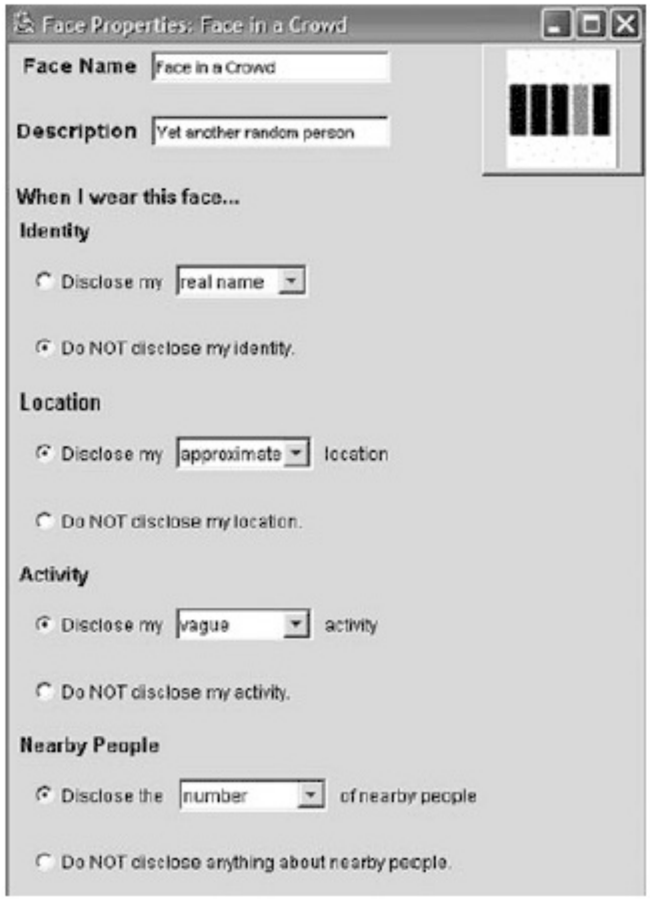


Figure 6. Everyday Privacy in Ubiquitous Computing Project - Face Properties Interface

© Scott Lederer, UC Berkeley

2.1.3. Adaptation

In his vision, Weiser referred to an environment where adaptation would take place without human intervention. The principle of calm computing or invisible computing [81] describes how the computing environment must become invisible to the user. Becoming invisible is not only a matter of hardware integration or size but most importantly of perception [97]. Indeed, the goal of the system is to reach "minimal user distraction … to … allow him to interact almost at a subconscious level" [94]. As the Ubicomp environment is made of complex relationships between the user and the components of the environment, adaptation requires both the user and the environment to adjust to these evolving interactions in order to maintain the dynamics of the relationships alive.

The system needs to be persistent as well as highly available [7]. Consistency can be hard to obtain materially when using fast-evolving equipment like computers or handheld devices. “Separating the environment from its physical instantiation on a particular device” [102] is then required to obtain a successful pervasive environment.

The continuity of experience is also an important aspect of adaptation. Tasks are usually defined as a sequence of actions with a definite beginning and end. Computers can efficiently run tasks following this definition on a well-defined input and usually generate a clear output. However, human activities cannot be as easily and efficiently represented only through tasks.

As outlined by Abowd [3], human activities have specific characteristics that can not be addressed simply through tasks, such as:

- Daily human activities rarely have a clear beginning and end
- Interruption is expected
- Multi-tasking should be supported
- Information needs to be reusable

2.1.3.1.Adaptation and Norms

According to consumer behavior research [73], technology is a paradox by itself. For example, technology provides consumers with the benefits of the latest scientific development but also can generate frustration as people can have difficulties keeping pace and may feel that their investments are being outmoded faster than before. Moreover, Mick and Fournier also noted that “appliances purchased for saving time regularly end up wasting time”. Technology can be said to evolve on its own without taking care of users’ expectations. Indeed, computers are still based on a trade-off made fifty years ago when “computer time was much more expensive than your time or mine” [37]. This trade-off has not evolved in the redesign of computers as expected but mostly in the way people have to deal with computing devices. [63]

Also, as computing is moving from computers and mainframes to small embedded devices, miniaturization brings new tradeoffs like between battery life and computational prowess [61].

2.1.3.2.Adaptation and User Control

Adaptation of the environment can not be easily achieved without giving some kind of control to the user. The research on recombinant computing, defined as an approach which enables devices and services on a network to be fluidly ”recombined” with no advance planning [42], is supporting such an adaptable user-centered design. Contrary to typical frameworks where system administrators create and manage interactions between devices and services, recombinant computing empowers the user to create, destroy and alter interactions between devices even if there were not explicitly designed to interact. This requires the development of frameworks similar to the one defined in the Speakeasy research project from PARC [78]. The Speakeasy framework is built on the assumption that no prior knowledge of another service or device should still make it possible for services and devices to interoperate with each other. Also, collaborative filtering techniques make it possible for the user to decide the type and quality of information he/ she wishes to provide to the system. Accordingly, the system will take decisions and make recommendations corresponding to the level of detail and the quality of data provided by the user [40].

2.1.3.3.Adaptation and Interactive Learning

As users expect to be able to interact as seamlessly and invisibly as possible with their environment, the environment will need to adjust itself to the user's expectation and provide more customized and efficient interactions. The environment should then be able to change its behavior based on user's situations and surroundings, for example it "would typically not disturb the user at inopportune moments except in an emergency" [94].

The corporate environment has first seen the deployment of systems close to the Ubicomp vision, such as Enterprise Resource Planning (ERP) systems. ERP systems help increase productivity of employees, customers and suppliers via the use of data exchange and automatic data capture across company departments and also third party suppliers. Successful implementations have occurred; however, a number of these deployments have been unsuccessful due to a lack of consideration for the system user [115].

2.1.3.4.Adaptation and Cultural Norms

As the focus is moving outward from the technological artifact to the use made of it and the settings in which it happens [10], the overview of the Ubicomp system needs to take into account entities such as institutions and social settings that impact the user in everyday encounters.

Also, a system is rarely built from scratch and adaptation will also require taking into account the present and past relationship in the environment as well as the social norms in place. For example, building an ERP system without taking into account the existing process or the user role in the system in terms of power or expertise will assure the failure of the implementation [115].

The adaptation factor will also become more and more critical as people tend to count on mobility and continuity of experience in regard to their interaction with their computing environment.

2.1.3.5.Adaptation and Information Filtering

Designers are faced with choices on the source of the data to use while building systems or applications. Often, it can be beneficial to use existing data to assure a better user experience. Some features like recommendations offered by the system to the user may require the collection of large amounts of data before the system can start being useful. Large amounts of data form single users or data from a large pool of users may even be required for the application to perform. For example, a movie recommendation system like Movielens will not be able to make any recommendations if it does not have any data to work on [32]. In this case, the need for a startup dataset should be clearly defined during the design process.

2.2. Technology Options in a Ubicomp Environment

An Ubicomp system is influenced by many different forces including market, laws, norms and codes. Due to its highly technological nature, the design of an Ubicomp environment is naturally more influenced by the code, which refers to both the infrastructure of the information system and the software, computing service or hardware that constitutes it. Therefore, the design of an Ubicomp system cannot be studied without describing the diverse technologies that will bring the concept of Ubicomp to life. The different technologies mentioned in the following subsections are some of the most promising candidates in enabling designers to build Ubicomp systems. The combination of these technologies will provide designers with opportunities to respond to some of the questions and concerns that have been outlined in section 2.1.

2.2.1. Mobile and Distributed Computing

Wireless networks and embedded computing devices can offer a seamless experience to the user. When deployed properly, they provide mobility to the user through roaming. In addition, they facilitate inter-component communication as the wireless connection could be used as a common interface for multiple devices and services.

As computing devices become more prevalent in our environment, they rely on distributed computing to communicate and provide services to the user through the use of a group of computing devices dispersed across a network.

2.2.1.1.Client-Server Architecture

One of the typical setups of distributed computing is the client-server architecture. The client, which can be any end-user device like a personal computer or a simple terminal, makes a request to a server, which will retrieve and process the necessary data and/or provide services to answer the request. The server will then return a response adapted to the specific client. The three-tier architecture shown in Figure 7, a variant of the client-server architecture, goes further to separate data, applications and user access. This architecture is highly used in Ubicomp systems, making it possible for different applications to access the same data simultaneously on behalf of different users.

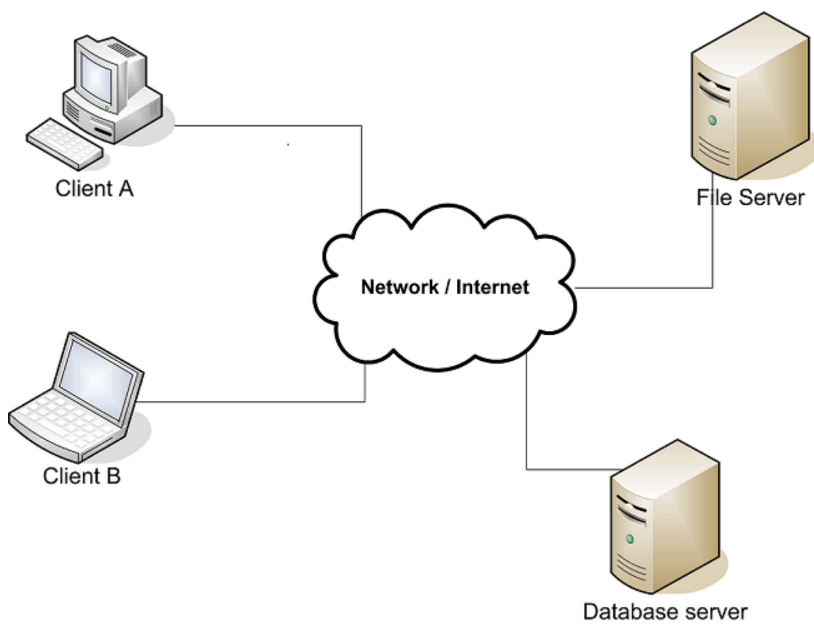


Figure 7. Three-Tier Architecture

2.2.1.2. The World Wide Web

The introduction of the World Wide Web in 1994 [18] was one of the most important achievements of distributed computing and also a major step towards the fulfillment of the vision of an Ubicomp environment. By providing access to resources from anywhere and anytime, the Web and all the associated technologies are at the center of the foundation of a system that will integrate computing devices and information into the user's environment. The Web fulfills the requirement set by Weiser for a network that ties low-power computers and software for ubiquitous applications [111].

In Weiser's vision, developed prior to the Internet-era and the establishment of the Web as a major communication tool, he highlighted that an Ubicomp environment would only be made possible when the "capabilities of physically dispersed computers" as well as making use of location information could be exploited. The Internet, in general, and the Web in particular make it now possible to provide users with access to the digital world; however, this access is dissociated from the particular device they use (e.g., laptop versus cell phone). The users are now identifying themselves more and more with particular points of the digital space (e.g., Internet portals and services, web-based email) rather that with the device they use to get access. As specified by Davies and Gellersen, the particular device has become by itself more and more irrelevant to the experience [33]. The next steps are to make distributed computing more powerful with standardization of exchange and interface as well as notions of location awareness as described next.

2.2.2. Automatic Data Capture and Sensor Networks

In an Ubicomp environment, interactions should be as seamless and invisible as possible. Automatic Data Capture (ADC) technologies are focusing on automating and facilitating the flow of data between the different actors of a system. Sensor networks, for example, use a collection of sensors to capture diverse information about the environments they are set in. By communicating amongst themselves, these sensors can provide a global picture of the complete environment and its evolution [8].

ADC technologies such as bar codes or magnetic cards now enable people to easily enter data into systems or interact with products or machines. ATM, self-checking stores and libraries provide examples of convenience brought by ADC systems [104].

Industry projects aim to generalize and facilitate automatic data capture. The open-source project Semacode [100], illustrated on Figure 8, enables consumer camera-phones to acquire two-dimensional bar code symbols and retrieve the URL associated with them. By taking a picture of a symbol, users can retrieve relevant information about the object or location the symbol is attached to. The interactions between the user and his environment are reduced and the information flow can be simplified.

Figure 8. Semacode 2D Barcode Associated to Web Address

© Semacode

Radio Frequency Identification (RFID) tags are small devices usually attached or embedded into products. They operate over radio frequencies and store data that can be remotely retrieved. RFID tags can be used for applications such as access control, pallet or library tracking [76]. Active Badge from AT&T Cambridge Labs [110] used wearable badges to locate users in conjunction with networked sensors between 1989 and 1992. At the time, the system consisted of 200 sensors and over 100 badges (see Figure 9) on four sites in Cambridge and was mostly used by researchers. This was primarily done in order to route phone calls as well as transporting remote applications interface to the nearest terminal for mobile users.

Figure 9. An Active Bat (left) and an Associated Application to Locate People at AT&T Labs Office Cambridge (illustration from [2]) © IEEE

ADC will become even more prevalent as more and more devices act as service agents. According to a report from the International Telecommunication Union (ITU), there will soon be more devices behaving as intelligent agents connected on the Internet than human beings [56]. This evolution can also be observed in manufacturing systems where intelligent agents will automatically capture relevant information in context and make decisions on their own while coordinating with the rest of the system infrastructure as needed [46]

2.2.3. Intercomponent Communication and Exchange Standards

2.2.3.1.On-Demand Information and Services

On-demand information was first made popular with the push technology [48] which promised a decade ago to provide users with the data they were interested in automatically. While the concept was not successfully implemented at the time, it was recently revived through the popular service of "blogs."[12] A blog is an online personal journal where entries are organized in reverse chronological order. The Really Simple Syndication (RSS) protocol was selected as the standard to support the exchange between the blogs and their readers. [117] The adoption of this standard was followed by the integration of intermediary services known as ping. Ping will enable aggregators to collect information from an RSS feed and send them to matching subscribed clients. The use of this kind of technology could help in providing on-demand services where the relevant information or application could be delivered to the client as it become available or necessary.

2.2.4. User Generated Content and Context

2.2.4.1. Folksonomy

Folksonomy is the result of personal free tagging of information and objects (anything with an URL) for one's own retrieval. The tagging is done in a social environment; in other words, it is shared and open to others. The act of tagging is done by the person consuming the information." [109]

The application of this concept implies relationships between three different components: the person, the resource and some metadata. Applications based on folksonomy rely on the fact that any two components of the relationships, when associated, will point to the third element of the relationship. In an Ubicomp context, this means that information could be associated based on their users, source or metadata. This approach puts the control of information into the user's hands since the metadata creation is decided by the user itself and the relationship only exists as long as the resource is seen in the context of the metadata of this particular user.

One of the most famous examples of folksonomy is the online application del.icio.us [95] where the metadata is called tags. As shown on Figure 10, the webpage is linked based on its URL, which is augmented with information such as keywords (tags), notes and descriptions that are personalized for this user.

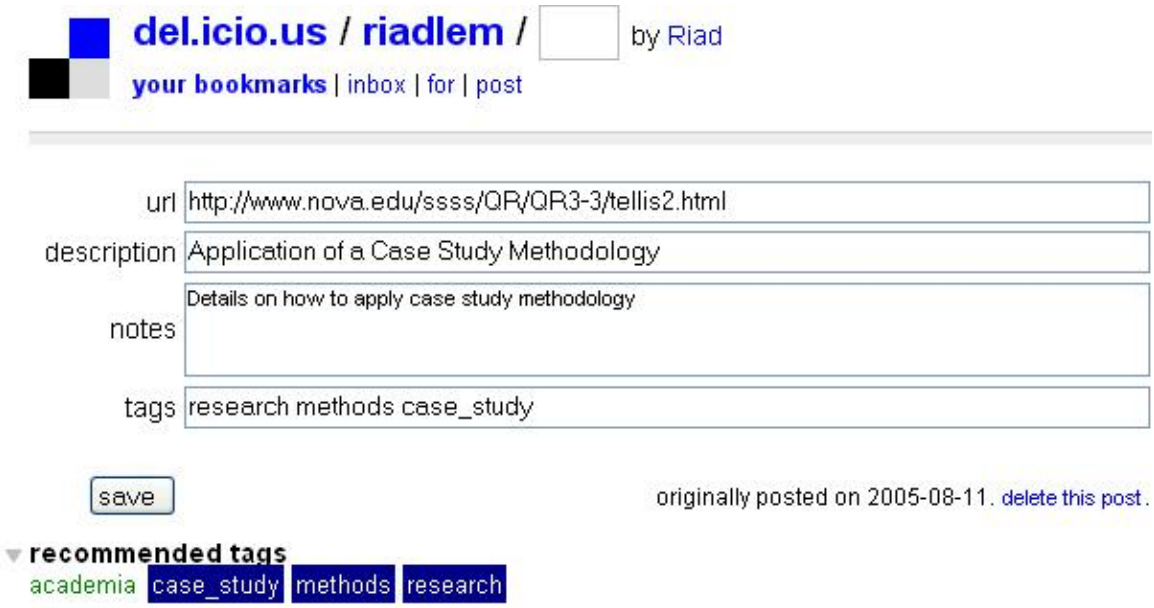


Figure 10. Del.icio.us URL Tagging System

2.2.4.2.Metadata

The literal meaning of the word Metadata is "data about data." Metadata refers to any kind of data that serves to describe another piece of information and it can also be indirectly acquired through the communication infrastructure. Geolocalized information [107] can be inferred from nearly any networked device whether this is a cellphone, computer or access badge. In addition to this spatial information, temporal information can also be easily collected through the network infrastructure. But collecting and using metadata like social connections is also possible. Short distance ad-hoc communication protocols like Bluetooth make it possible to associate users with their neighbors. Mobile Media Metadata (MMM) [34], a project from Garage Cinema Research at the University of California Berkeley, demonstrates how these three level of metadata can be combined to support the sharing of photos taken with a Bluetooth [53] powered camera phone (see Figure 11). Based on these social, spatial and temporal parameters, the MMM system can determine the people who are statistically more likely to be included in the sharing list and populate the sharing menu on the phone accordingly.

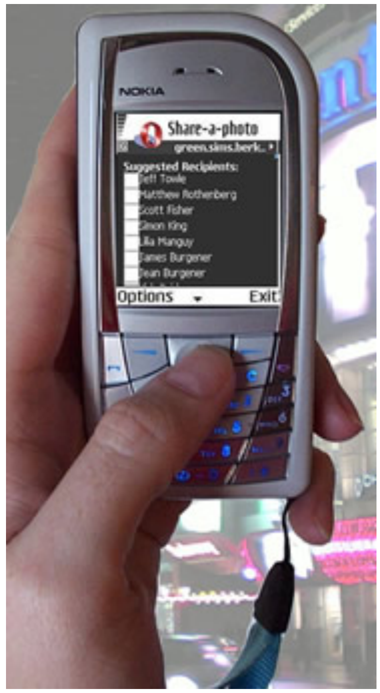


Figure 11. Mobile Media Metadata Sharing Menu

Metadata can also be considered to be at the core of some systems that make recommendations like MusicStrands (Figure 12) or Movielens. The Musicstrands [58] system creates relationships between songs by associating songs that are played together in a play list and matching users based on similar listening patterns in their listening habits.

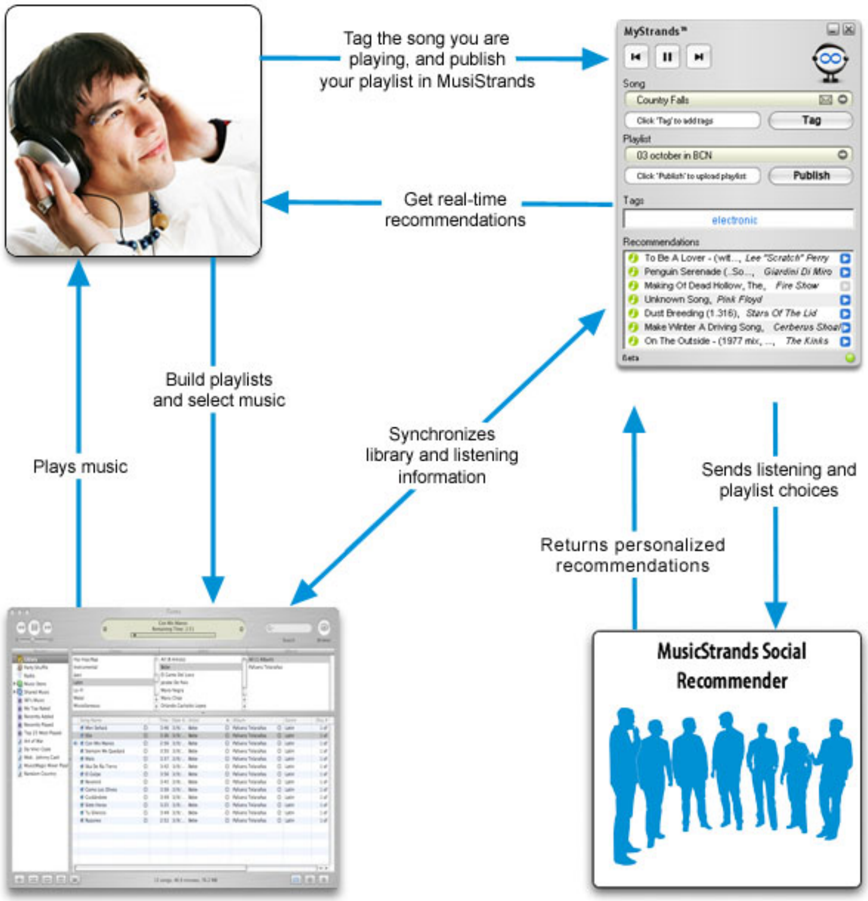


Figure 12. MusicStrands Platform Architecture © MusicStrands

2.2.4.3.Communication Standards and Collaboration

As outlined earlier, an Ubicomp system relies on an efficient collaboration among its components, particularly in regard to exchange of information. Computing devices have now the ability to store, process and exchange larger amounts of data than they could just 20 years ago. Since the ARPA project that gave birth to the Internet in 1969, computer networks have become a primary means of information exchange. New network technologies like TCP/IP [62] or wireless networking provide broader opportunities to connect all kinds of devices more easily.

Collaboration between devices will provide the ground for newer applications centered on the user's expectations [22]. Network design and communication standards like TCP/IP as well as intelligent frameworks like recombinant computing will make consistency of experience more likely to happen as well. Also, personalization [78] and context awareness will be more efficient as wireless networks provide opportunities for localization and behavior analysis. A "personal profile" will be able to follow the user through the day and adapt to his/her context [94].

Collaboration can only be made possible through the use of common standards and formats in the exchange of data and services. One of the key concepts guiding development of new data exchange standards is the separation of content from its presentation. Indeed, the goal is to make information available through any possible channel with the minimum of adaptation. Data exchange technologies such as Simple Access Object Protocol (SOAP), eXtensible Markup Language (XML) or Really Simple Syndication (RSS) [117] are aimed at providing common information structure for any service or application to exploit on any device. For example, as shown on Figure 13, XML helps information providers interoperate easier since information content is separated from information rendering.

```xml
<People>
  <Person>
    <Name>
      <FirstName>John</FirstName>
      <LastName>Smith</LastName>
    </Name>
    <Address>
      <Street>118 Covell Hall</Street>
      <City>Corvallis</City>
      <State>OR</State>
      <ZipCode>97330</ZipCode>
    </Address>
    <Job>
      <Title>Student</Title>
      <Description>Information System Engineering</Description>
    </Job>
  </Person>
</People>
```

Figure 13. Student Contact Information in XML format

As XML and associated technologies are getting acceptance as standard format for data exchange, research is now focusing on how to manage and interact with standardized information in a more efficient way [106]

2.3. Information Systems Design Methods in Ubicomp

The challenges associated with evaluating Ubicomp systems require designers to carefully examine the best technique and/or tool to use in order to assess the performance of the system. Ubicomp, drawing from various fields such as Human-Computer Interaction, Cognitive Science and Computer and Information Sciences, has seen a large array of techniques used to evaluate system design. After a description of the specifics of performing evaluation of Ubicomp systems, some of the more popular evaluation techniques are reviewed next.

2.3.1. Interaction Design in Human-Computer Interaction

"*User-centered design emphasizes that the purpose of the system is to serve the user, not to use a specific technology, not to be an elegant piece of programming*" [82]. As computing systems have encompassed more and more human activities, "traditional" design techniques applied to computers have become more and more irrelevant. In the early 90's, the emergence of new techniques, more focused on interacting with the user during the design process, have gained acceptance. These techniques have proven to bring increased quality to the design of applications and systems; however designers are reluctant to use the full range of usability engineering methods available as they tend to bring a high cost overhead to the project [71].

2.3.2. Challenges of Ubicomp Systems Evaluation

Evaluating Ubicomp systems has been recognized as a challenge [99]. Scholtz describes the need to establish a discipline to evaluate Ubicomp applications. Despite the fact that techniques to evaluate information systems like desktop applications have drawn a lot of attention from the Human-Computer Interaction community since the spread of the Personal Computer [79, 80, 103], these techniques do not transfer easily to Ubicomp systems. This is due to the fact that standard applications and Ubicomp systems differ in several ways [35]:

- Ubicomp systems operate over large physical spaces
- Ubicomp systems are designed for greater availability over time
- Ubicomp systems support interactions with and between more people

Also, researchers create Ubicomp systems using cutting-edge technologies which may not be well understood by developers. In these circumstances, creating reliable systems able to support activities on a continuous basis can become difficult. Therefore, “a good portion of reported Ubicomp work remains at this level of unrobust demonstrational prototypes” [2].

Novel evaluation techniques focused at evaluating the design process itself could help designers in bringing more perspective and parameters to take into account while designing an application. Several of these techniques have recently emerged and will be reviewed with regards to how they can augment the user experience in terms of ubiquity.

2.3.3. System Evaluation Techniques in Human Computer Interaction

2.3.3.1.Contextual Design

Interaction design techniques for information systems have emerged since the early 1990s. Contextual design [118] is a technique for examining and understanding users in context. The procedures of contextual design, based on the need to integrate the user earlier in the design process, try to put the user perspective in the middle of the design of computing services and artifacts. In this regard, interviews are conducted where field data is gathered from users. Usually, interviewers perform the interview with one user at the time. However, Ubicomp systems are specific in the sense that they need to support interactions with several users at once. Therefore, contextual design cannot fully represent the interactions between users and the system.

2.3.3.2.Wizard of Oz

The Wizard of Oz technique [31] has received a lot of interest in the design and evaluation of large and complex information systems. Wizard of Oz studies can be defined as studies “where subjects are told that they are interacting with a computer system through a natural interface, though in fact they are not.” Wizard of Oz simulation tries to close the gap between humans and computers.

A human operator (i.e., the Wizard), mediates the interaction and therefore more freedom of expression can be given to the subject. But such simulation can easily become really complex in regard to the design of an Ubicomp system because interactions take place with and between more people when compared to a traditional “desktop” application. Mapping all these relationships is probably not feasible today using a technique as focused and dedicated as the Wizard of Oz.

2.3.3.3.Quantitative Methods

Quantitative methods (i.e., surveys) have proved to be efficient tools to measure specific criteria of an information system. Surveys are easy, well defined and accepted methods to measure parameters of a system objectively. However, several difficulties arise when it comes to the use of surveys to evaluate and orient the design of Ubicomp systems. First, an Ubicomp system can be characterized by its multi-causality. Setting up an Ubicomp system usually means introducing multiple changes at once. Thus, “it is hard to tell which part has played the major role” [97]. It could be argued that rich applications designed for the desktop interface have the same characteristics. But more conventional interfaces provide with means to separate evaluation for each of the changes. While it is possible with an application well contained in a user interface, it cannot be reproduced in an Ubicomp system where the interaction is by definition diffuse in the whole system.

In addition, the multi-causality of Ubicomp systems makes it harder to evaluate them through surveys. Surveys usually measure a limited and well defined set of parameters quantitatively and try to infer causality relationships between groups of parameters. Therefore, to validate such surveys in an Ubicomp environment would require a very large number of respondents and a high level of precision in the items discussed. It is questionable that such a precision can be obtained in regard to the design of systems as subjective as Ubicomp systems.

2.3.3.4.Case Studies

The use of case studies in information system design [119] provides with the opportunity to study complete systems without much of the restrictions encountered with previous methods. While case studies do not provide with quantitative means to analyze a system, especially early in the design, they can contribute to assess the performance of a system in regard to a large number of criteria and identify success and failure based on experience. They also illustrate how components like privacy settings [65], context [36] or personalization [41] can affect visibly the system and the user experience.

2.3.3.5.Evaluation Applied to Ubicomp Systems

In the context of Ubicomp systems, any of these techniques may not be sufficient by itself. In the case of contextual inquiry, for example, the user is interviewed in a context that is in the environment where he/she performs the task or activity of interest to the interviewer. This design technique can bring a lot of insight into the design of a system by examining the system and the user in context. Unfortunately, designing an experiment in context is not only intrusive but also requires a large amount of resources to be successful. While testing in real world conditions is difficult, quantitative tools like surveys may not enable the capture of the complexity of an Ubicomp system. In the case of an Ubicomp design, submitting a design to a survey analysis will necessitate the assessment of numerous relationships that have been identified in the framework while also measuring user satisfaction at the same time. Combining quantitative methods with some alternative evaluation techniques like a case study or a controlled experiment like

Wizard of Oz would probably provide designers with a more flexible and efficient way to evaluate their design.

2.4. Summary

As demonstrated by the review of previous work in the field of Ubicomp and user-centered design, major design aspects of an Ubicomp environment have been overlooked by system and applications designers. Therefore, there is a need to define how these parameters and the technology used to support them can be integrated more closely in the design process. In doing so, the user experience with the computing environment will become closer to Mark Weiser's vision of an Ubicomp environment.

Defining the requirements to integrate all technologies needed to build a Ubicomp environment while taking into account at the same time all the limitations brought by the parameters of ubiquity will be challenging. However, it is necessary to formalize as much as possible the design process in an Ubicomp environment. Indeed, this formalization will enable researchers to collaborate on their results and learn from them [99].

The interactions between the different components of a ubiquitous computing system are numerous and complex. Evaluating an ubiquitous computing system is a complex task and literature shows that little successful methodology has been defined so far [2]. The association of the framework of user values in Ubicomp with appropriate technologies and evaluation techniques can provide valuable insights in the design of complex systems like Ubicomp environments.

2.5. Design Framework

Based on the literature review, we can define the following framework to be used in informing the design of a ubiquitous computing environment.

Ubicomp System Design Principles	
User Control	Granularity of context capture
	Granularity of personal information disclosure
	Standard representation of context
	Creation of new interactions with the system (re-invention)
	Management of interactions with the system
	Dynamic management of disclosure
Choice	Different level of privacy preferences among users
	Personalization of services
Memory	Remember user preferences
	Support for activities (with no clear beginning or end)
	Intelligent capture
	Support for collaboration
Information filtering	Anticipate user activities
	Match information representation and usage
	Use of community knowledge and collaborative filtering
	Capture only relevant data
	Build from scratch or integrate with existing data model
Interactive learning	Precise association between different element of context and user
	System learn based on usage
	System adapt to circumstances of use
Laws	Expectation of privacy
	Adapted to user and context
	Respect local laws
	Acceptable use
	Acceptable data
	Re-invention of technology
	Appropriation and evolution of system

Norms	Tradeoffs between system complexity and complexity for user
	Tradeoffs between technological requirements and user expectations (ex: Battery life versus Performance)
	Integration with institutions
	Integration with everyday life
	Pre-existing conditions

3. Methodology

While designing a system, designers should look for principles to help them define the scope and requirements associated with the system. We can define our methodology according to the steps described in Table 2.

Table 2. Process for Evaluating Ubicomp Systems

1. Define system ecology	Identify existing similar systems
	Related systems to integrate or interact with
	Activities to support
1b. Analyze existing architecture (case study)	Define types of users
	Existing usage
	Issues of interest
2. Apply framework to system	Apply design principles to system design
	Identify requirements
	Relate requirements to existing systems, technology and activities
3. Additional specifications (focus group/ interviews/ survey)	Collect additional data regarding issues where no literature is available
4.Design	

3.1.1. System Ecology Study

In this regard, a study of the ecology surrounding the system to be created is important in order to capture the specifics of the environment. A system can be constructed around existing sub-systems, activities and requirements that should not be ignored.

3.1.2. Heuristic evaluation and case study

Following our framework, designers can build a heuristic evaluation of the requirements to include in their design in regard to the seven categories we have identified in our review of the literature. While a heuristic evaluation of the system to be built can provide a lot of insight into the design, most designs, especially in the space of ubiquitous computing environment, are rarely built from scratch. Therefore, basing the evaluation on existing systems that replicate some of the activities or functions of the systems to be designed can also be helpful. If the design work is related to iterative work on an existing system, a case study can also be helpful in defining the activities associated with the system and the type of users involved.

3.1.3. Framework of design principles

The framework defined in section 2.5 provides design questions that the designer should study in regard to the seven categories of the user experience we have defined as being relevant to the design of user-centered ubiquitous computing environment.

Each of the design questions should not only be answered with regards to how the system will serve the user but also in how the existing infrastructure (if it already exists) fulfills the user's expectations.

3.1.4. Additional data collection

Once the framework has been applied to the system of interest, issues may arise that have not been documented in enough detail. To enable the designer to take them into account, additional methods such as focus groups, interviews or surveys may be performed to help inform the design sufficiently.

3.2. Experimental setup in similar research projects

Table 3 shows a compilation of projects in the field of ubiquitous computing and user interaction. These projects were used to define the methodology used in this research and helped illustrate the variety of approaches used to study the design of user interaction in Ubicomp systems.

Table 3. Major Research Study Projects Related to User Interaction in Ubicomp

Author or project title	Location	Topic	Number of participants	Type of experimentation
IO Project	UC Berkeley	Privacy in Ubiquitous Computing	12 subjects	90 min scenario-based interview
Balfanz	PARC	Setting up PKI for wireless network clients	8 experts (PhD in Computer Science or related	Usability analysis of step-by step walkthrough
STRAP	Georgia Tech	Structured Analysis of	80 subjects	Controlled experiment
Labscape	Univ of Washington	Context aware data collection	5 biologists	Contextual Field Research
MMM2	UC Berkeley	Context aware photo sharing	77 subjects	System implementation + questionnaire
Classroom 2000	Georgia Tech	Classroom interaction using mobile devices	35 students	System implementation + questionnaire
Grinter	Georgia Tech	Home network study	14 individuals in 7 homes	Empirical study
PARCTab	PARC	Handheld computing	25 users	System implementation +Usage Data

3.3. Application to Wi-Fi

To evaluate our framework, we applied it to the design process of computer wireless network environments based on Wi-Fi technology. This environment was chosen because wireless networking is usually considered one of the core elements in the design of an Ubicomp system [23, 85, 94, 96]. While Wi-Fi cannot be considered as an Ubicomp environment by itself, the design of an Ubicomp environment pursues the principle that devices, connectivity, applications, services and information are seamlessly integrated in a unified user experience. Due to the expected prevalent role of Wi-Fi in providing connectivity in Ubicomp systems, studying the Ubicomp characteristics of Wi-Fi could help build better Ubicomp systems using this technology. Therefore, we applied our framework to the actual design of Wi-Fi systems through a case study analysis of Wi-Fi environments. Once we had identified issues and potential for design changes, we identified possible improvements to the design of Wi-Fi systems using some of the technologies we had described earlier. Then, we conducted a survey to assess the impact of some of the issues identified. The survey was also used to quantify the use of Wi-Fi technology in order to orient future work on some design improvement in this area.

4. Wi-Fi Study

In this study, we analyzed the design of different computing environment in regard to their use of Wi-Fi in terms of user experience. After describing some of the perspectives on the use of Wi-Fi technology, we introduced our findings and a model for improved interactions. We conducted an online survey to explore some of these findings and validate the relevancy of the model.

4.1. Perspectives

Since the early 1990s, wireless networking has become increasingly sophisticated due to the improvement in radio frequency technology. After being adopted for voice communication, computer networks saw an opportunity to eliminate wiring by using radio frequency communication. Weiser, in his seminal paper about Ubicomp, defined the need for three different types of connectivity: "tiny range wireless, long-range wireless and very high speed wired." [111]

Building a large scale wireless network or "wireless commons" could provide long-range wireless and the equivalent of very high speed wired at once. Therefore, wireless computer networking has emerged as a promising candidate in the foundation of any ubiquitous computing environment.

From the many available wireless computer networking technologies, Wi-Fi has become a popular choice to extend or build local area networks for businesses and homes. Wi-Fi has the advantage to reduce the cost of deploying the network infrastructure while providing flexibility and mobility to its users. Internet Service Providers (ISP) now offer commercial Wi-Fi service in public venues (generally known as wireless hotspots) like conference centers, airports and coffee shops. Initiatives have been proposed in several metropolitan areas including Philadelphia [87] and San Francisco [47] to provide citywide Internet access using wireless networking technologies. Wireless networks are expected to not only provide an ubiquitous Internet access to its residents but also to help improve fire and emergency service communications, support educational programs, and reduce the digital divide between communities.

Such implementation implies that wireless networking will indeed spread beyond the home, the university and the work sphere and into the global user environment, therefore likely becoming one of the components necessary to fulfill Weiser's vision [111]. It also means that some people will discover the Internet and experiment with computer networking technologies through the use of WLAN connectivity for the first time. The learning curve could prove to be steep since wireless networking has intrinsically specific requirements, issues, and interaction opportunities associated with it. Therefore, viewing wireless networks as a wire-free version of wired computer networks may be an extremely limited vision of the technology. Just as researchers have identified the differences in landline phone and mobile phone use [23], this research will try to distinguish some of the specifics of wireless networking.

The Internet, and the TCP/IP suite of protocols that supports it, have been designed more on a technological level than a political or social one. This is best summarized by the Lessig's description of the architecture of control in 1999: "The minimalism in design is intentional. It reflects both a political decision about disabling control and a technological decision about the optimal network design. The designers were not interested in advancing social control; they were concerned with network efficiency. Thus, this design pushes complexity out of the basic Internet protocols, leaving it to the applications, or ends, to incorporate any sophistication that a particular service may require. "[69]

Lessig goes on to argue that the Internet was transformed by commerce to enforce regulability. We believe that, similarly, wireless networking infrastructure will evolve to support citywide commercial deployment and similar large-scale endeavor. While the Internet of today is more regulated than the Web of 1994, there are several factors that limit the implementation of these regulations on today's wireless network infrastructure. Indeed, interactions with users on a wired network had evolved to support some sort of identity, authentication and policy:

- The wire(s) identified the network as well as associated permissions and privileges.
- The connectivity was tangible: location and availability were represented by the wire connection.
- Rules and regulations were usually associated with the wire's physical location.
- Rules and regulations could be reinforced through physical marking in the area surrounding the connection.

Most of these elements, used to enforce some regulation on the access to a wired network, cannot easily be transposed to wireless computer networks. After examining the context of wired networking, we feel there is a need to look at whether or not designers of wireless networking technology have integrated interaction design theories.

4.2. Wi-Fi Study Methodology

We conducted this research by focusing particularly on how the user experienced Wi-Fi technology and looked for elements to enhance the existing infrastructure while considering the limitations imposed by the technology.

To this effect, we studied the IEEE 802.11 standard [83] as implemented in popular operating systems. We enhanced this study with the analysis of complementary or add-on systems that bridge the gap between users and designers. Services like Plazes (see Figure 14) and JiWire (see Figure 15) are examples of such add-on systems to wireless networking. Both services [59, 88] are geo-localization applications built on top of the existing wireless network infrastructure.

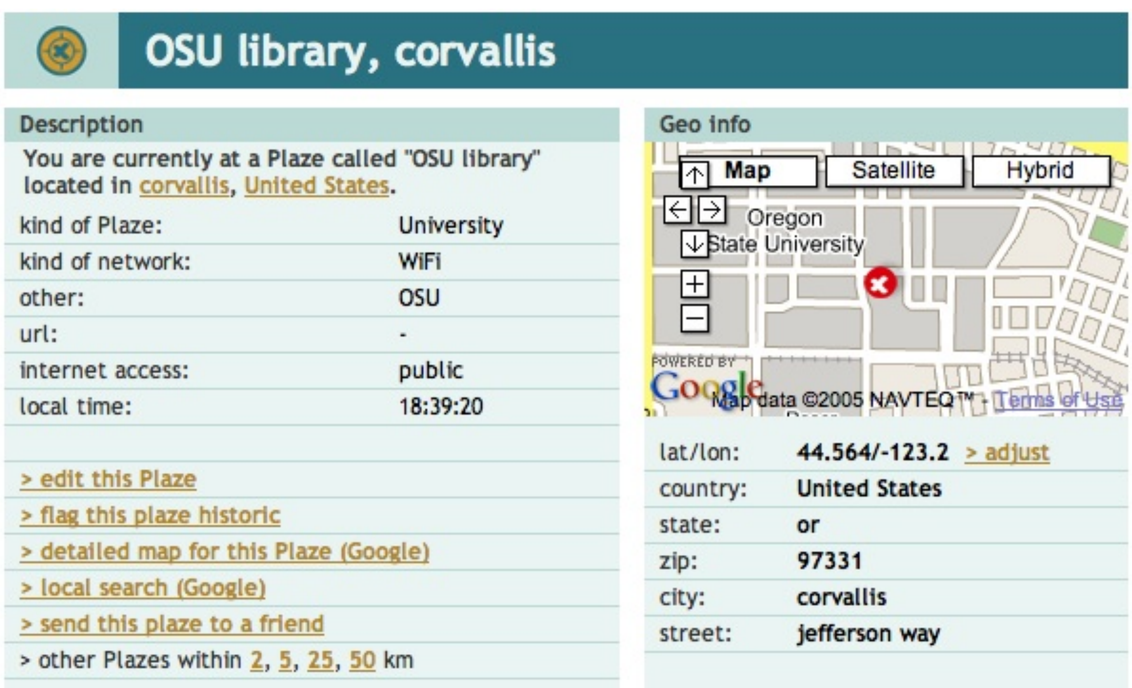


Figure 14. OSU Library Wireless Network Information in Plazes

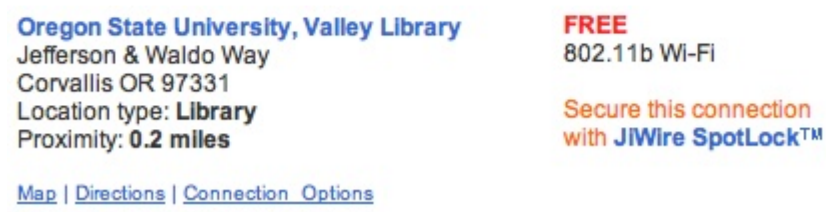


Figure 15. OSU Library Wireless Network Information in JiWire © JiWire

Matt Jones' concept of Warchalking [11] (see Figure 16) also highlighted some of the issues encountered with wireless computer networking. Its goal was to provide physical space labeling of the wireless service availability.

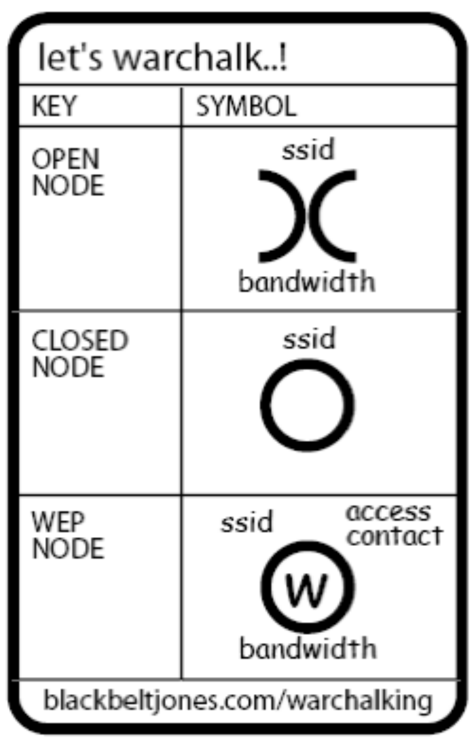


Figure 16. Warchalking Symbols (source: blackbeltjones.com)

These various elements of a Wi-Fi information system were analyzed according to the different elements outlined in the model we developed from the literature review. We analyzed the WLAN support as implemented by default in popular operating systems. Then, we added add-on applications to our study. After describing the basics of wireless networking technology in section 4.3, the analysis based on our model provides with the insights described in section 4.4. Our model is then described in section 4.6.

4.3. Overview of the Technology

Based on the IEEE 802.11 specification a wireless network can be setup in two different modes: ad hoc and infrastructure. In infrastructure mode, the network may be composed of the following elements: station(s) (also referred to as clients), access point(s) (AP), Basic Service Set(s) (BSS) and a Distribution Service (DS), as shown in Figure 17.

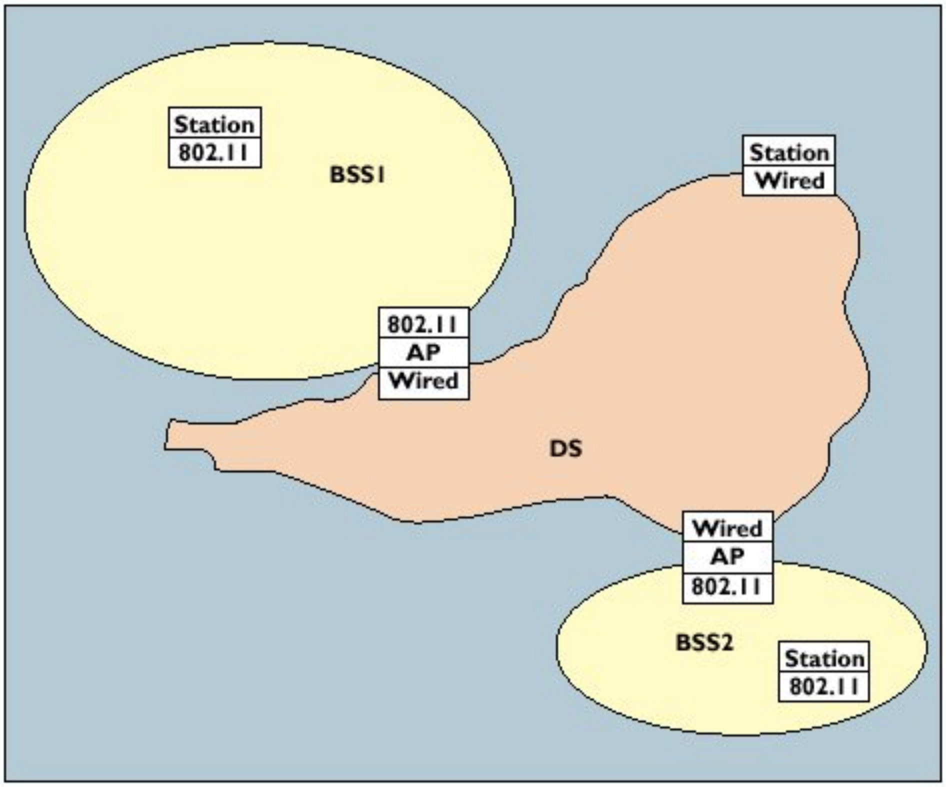


Figure 17. Typical WLAN Configuration © ACM [92]

Stations access the network via an access point, which serves as the link with the distribution service. The access point provides access to the station through a two-step procedure: authentication and association. Access points can be federated together by the use of a common service set identification (SSID) also generally known as the wireless network name.

4.4. Findings

4.4.1. Notice

In the process of connecting to a WLAN, users should be provided with the necessary information to help them make an informed decision.

4.4.1.1.General Implementation

Table 4 provides a summary of the main information provided by the Wi-Fi network infrastructure and some selected add-on applications.

Table 4. Information Disclosure in Wireless Networking

Information Provided to Users Regarding Wireless Connectivity		
System		Values
IEEE 802.11	SSID Name	Alphanumeric value
	Security type	Secured / Unsecured
	Signal Strength	Numerical Value or Percentage
Plazes / JiWire	Geographic Location	
	Entity	
	Cost	
	Access	Public /Private

4.4.1.2.Network Restrictions

4.4.1.2.1. Connectivity Restrictions

Based on the implementation illustrated in Table 4, there is no possible way for the user to know the exact requirements and restrictions enforced on a wireless network before connecting to it. This situation has both legal as well as technical implications as described in the next section.

For example, wireless networks may require the user to run a specific application to start the connection process. A large number of providers have chosen to use browser-based identification schemes to authenticate and authorize users. As explained in section

4.4.6.1, all potential clients may not support these schemes, sometimes simply because they do not have a compatible browser. Therefore, wireless clients would benefit from knowing in advance the type of restrictions or requirements encountered when trying to establish a connection to a particular wireless network. These clients could then easily eliminate from the array of possibilities any connection that requires technical capabilities that they have not implemented.

4.4.1.2.2. Applications and Service Restrictions

Restrictions may also be placed on the applications and services provided by the wireless network administrators. No technical specification or protocol enables yet to inform the user about this fact. Information about these limitations can not be easily provided by the wireless infrastructure as of now and even if connected to the network, there is no simple information delivery system that could provide this information.

4.4.1.3.Troubleshooting

The main source of information regarding the wireless network is the network itself. Information about the state of the connection or the rules to connect can be provided through a software or webpage displayed to the client at connection. However, if the client is not able to connect, there is no easy way to provide her with information on how to address this problem. Indeed, the problem can be located at the wireless client, at the wireless access point or somewhere between the access point and the rest of the core network. As the general wireless infrastructure is currently designed, it is extremely difficult for non-expert users to be able to pinpoint the source of the problem. Even experts in computer networking could find it difficult to troubleshoot the connection unless they use specialized tools. As we described later in section **Error! Reference source not found.** and in our model (see section 4.6), some additional information could be broadcast by the access point to help in this task.

4.4.2. Norms and Laws

Legislators and popular media have frequently discussed rules and laws applying to wireless computing connectivity. However, existing protocols and laws are inadequate. Rules that could be clearly defined for wired connections based on physical access restrictions and visual markings have not been adapted to wireless networking. WLAN can easily be dissociated from a physical space even if its geographic coverage is limited; walls, doors and buildings do not stop the radio signal from leaking outside of the signal's original location. A consensus to resolve this inadequacy has not yet been reached to implement universal policy. Nevertheless, some initiatives have tried to address these issues with limited success.

4.4.2.1.Authentication

Access to the wireless medium can be restricted to users registered with the system that provides the wireless connectivity. In most cases, this mechanism commonly referred to as the authentication service, has already been employed by the system upon which the wireless network depends. As a consequence, the wireless network is then simply an extension of the core wired network. A study of university deployment of campus wireless networks [90] has shown the existence of no less than seven different methods to secure the wireless medium and authenticate the users [68].

4.4.2.2.Security procedures

Research has shown that end-users experience numerous difficulties in adopting and using networking security systems [105] . Since there is no physical barrier to prevent access to the medium, there is a greater need for security mechanisms in wireless communications. As wireless communications are transmitted over the air, there is no easy way to prevent the signal from being intercepted by third parties. Security mechanisms implemented in the IEEE 802.11 protocol for wireless computing communications were mainly aimed at protecting the secrecy of the transmissions between the device and the access points to which it was associated. These mechanisms have seen their use evolved to a greater level than what they were intended for. It is not uncommon to see the wired equivalency protocol (WEP), a mechanism primarily designed to encrypt Wi-Fi transmissions over the air, be used as a tool to control access to a local network.

4.4.2.3.Authentication and security

In the context of wireless networking, the line between authentication and security has been blurred in the use of these mechanisms. Providing a secure transmission through protocols like WEP or Wi-Fi protected access (WPA) also means that only users sharing the secret key can access the network. Therefore, only people who have set up the security measures can be authenticated to access the network resources. A common misunderstanding amongst users is that restricting the access to their wireless network and securing their communications means the same thing. Table 5 illustrates the differences between security and authorization features in wireless networks.

Table 5. Authentication and Security Mechanisms in Wireless Networking

Mechanism	Secure	Authorization / Access	Authenticatio
None	No	No	No
WEP/ WPA	**Yes**	Limited	Maybe
MAC filtering	No	Limited	**Yes**
Login (ex	No	**Yes**	**Yes**
VPN	**Yes**	Maybe	Maybe

We explain later the reasons why both authentication and security are required for an optimal experience when using wireless network connectivity. However, we first need to explain the results from the table above and how none of the widespread mechanisms in use satisfy authentication, authorization and security requirements alone.

While WEP and its successor WPA could be considered as satisfying both security and authentication requirements, we will argue that their authentication mechanism are not scalable. Indeed, WEP and WPA can only authenticate a limited number of different clients. In fact, WEP can only distribute and authenticate four different keys, and therefore cannot distinguish between more than four distinct groups of clients.

While virtual private networks (VPN) also provide security to wireless users, it also fail on the authentication side but for different reasons that WEP or WPA. Contrary to them, VPN is not a part of the wireless protocol. Because of VPN being an external component to the wireless infrastructure, it cannot be used to directly authenticate and authorize clients on the wireless network. Also, the non-integration of VPN with the wireless network means that the security features offered by a VPN tunnel can be provided as effectively by a local server than by one which is distant and non-related to the wireless network operator. Besides securing the transmission, setting up authorization has significant impact both for the owner of the wireless network and for potential users.

4.4.3. U.S Laws

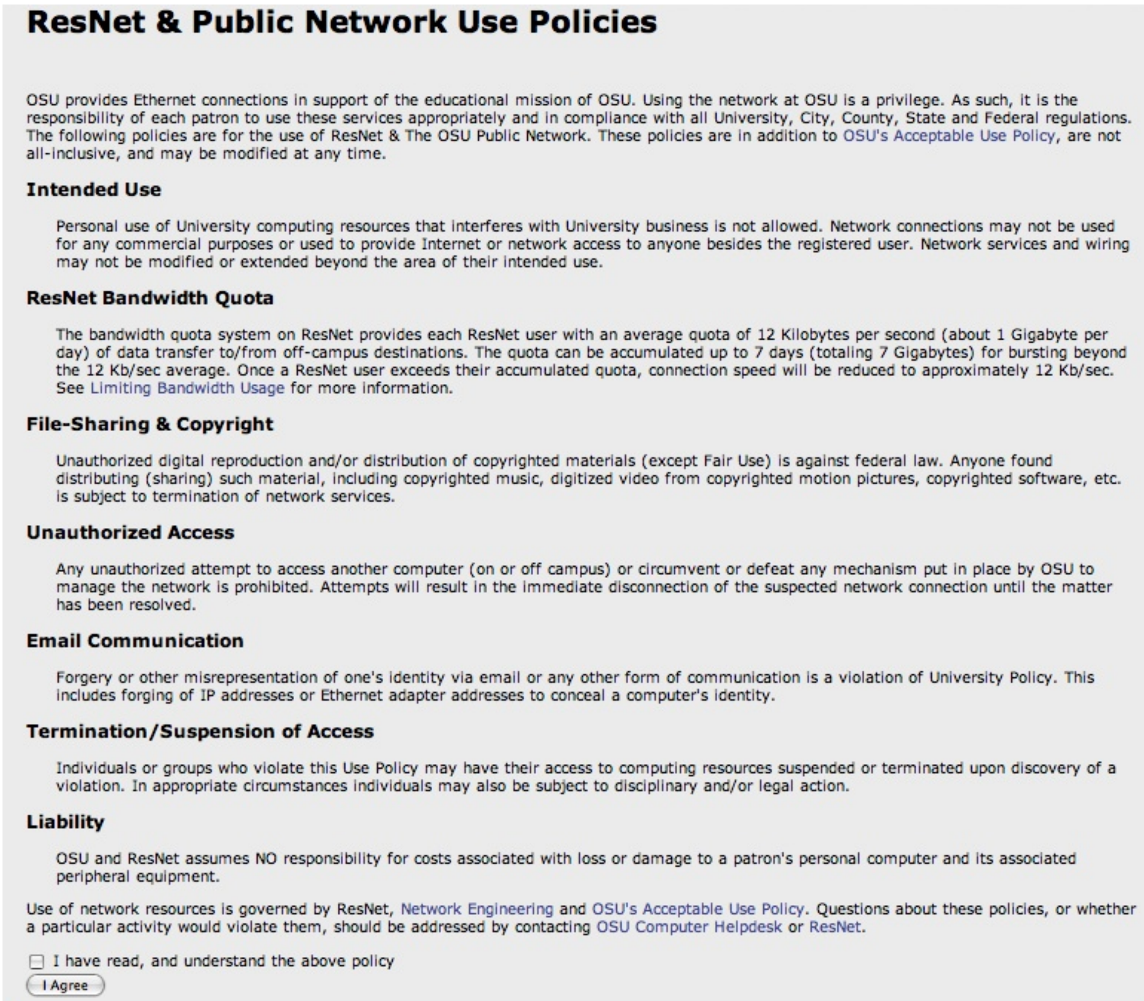
4.4.3.1.Federal and state laws

According to the U.S. Computer Fraud and Abuse Act of 1986 [28], anyone who "intentionally accesses a computer without authorization or exceeds authorized access" can be charged with a crime. Some users may be unaware of this law and therefore connecting to an open wireless network could put them at risk of prosecution. A few states have started to protect wireless networking users from this risk by implementing new legislation. According to New Hampshire's state bill HB 0495 [1] that was passed in early 2004, "the owner of a wireless computer network shall be responsible for securing such computer network. It shall be an affirmative defense to a prosecution for unauthorized access to a wireless computer network if the unauthorized access complies with the conditions set forth in subparagraph I(a)(1)-(3)." Basically, this kind of legislation places the responsibility of access control not on the users of the wireless network but on its operator. However, most of the states in the US have not implemented such legislation or have voted texts that may assimilate accessing an open Wi-Fi network as trespassing.

4.4.3.2.Acceptable Use Policy

In some networks, such as Oregon State University's public network, the issue has been resolved by mandating user agreement of acceptable use policy (AUP) upon the first connection to the network (see Figure 18).

The user agreement presented to the users of the OSU wireless network, OSU_PUB, contains the same terms as the policy applied to user of the network through an Ethernet connection. However, this policy does not tackle most of the specific issues related to Wi-Fi access.



ResNet & Public Network Use Policies

OSU provides Ethernet connections in support of the educational mission of OSU. Using the network at OSU is a privilege. As such, it is the responsibility of each patron to use these services appropriately and in compliance with all University, City, County, State and Federal regulations. The following policies are for the use of ResNet & The OSU Public Network. These policies are in addition to OSU's Acceptable Use Policy, are not all-inclusive, and may be modified at any time.

Intended Use

Personal use of University computing resources that interferes with University business is not allowed. Network connections may not be used for any commercial purposes or used to provide Internet or network access to anyone besides the registered user. Network services and wiring may not be modified or extended beyond the area of their intended use.

ResNet Bandwidth Quota

The bandwidth quota system on ResNet provides each ResNet user with an average quota of 12 Kilobytes per second (about 1 Gigabyte per day) of data transfer to/from off-campus destinations. The quota can be accumulated up to 7 days (totaling 7 Gigabytes) for bursting beyond the 12 Kb/sec average. Once a ResNet user exceeds their accumulated quota, connection speed will be reduced to approximately 12 Kb/sec. See Limiting Bandwidth Usage for more information.

File-Sharing & Copyright

Unauthorized digital reproduction and/or distribution of copyrighted materials (except Fair Use) is against federal law. Anyone found distributing (sharing) such material, including copyrighted music, digitized video from copyrighted motion pictures, copyrighted software, etc. is subject to termination of network services.

Unauthorized Access

Any unauthorized attempt to access another computer (on or off campus) or circumvent or defeat any mechanism put in place by OSU to manage the network is prohibited. Attempts will result in the immediate disconnection of the suspected network connection until the matter has been resolved.

Email Communication

Forgery or other misrepresentation of one's identity via email or any other form of communication is a violation of University Policy. This includes forging of IP addresses or Ethernet adapter addresses to conceal a computer's identity.

Termination/Suspension of Access

Individuals or groups who violate this Use Policy may have their access to computing resources suspended or terminated upon discovery of a violation. In appropriate circumstances individuals may also be subject to disciplinary and/or legal action.

Liability

OSU and ResNet assumes NO responsibility for costs associated with loss or damage to a patron's personal computer and its associated peripheral equipment.

Use of network resources is governed by ResNet, Network Engineering and OSU's Acceptable Use Policy. Questions about these policies, or whether a particular activity would violate them, should be addressed by contacting OSU Computer Helpdesk or ResNet.

☐ I have read, and understand the above policy

I Agree

Figure 18. Network Use Policies of Oregon State University Public Network

4.4.4. Shared resources

4.4.4.1.RF Channel Interference

Wi-Fi uses unlicensed wireless communication spectrum in the 2.4 and 5GHz Industrial, Scientific and Medical (ISM) range. This means that Wi-Fi compliant equipment can freely use a channel of the spectrum as long as certain conditions of transmission power are followed as stated by the Federal Communication Commission (FCC) [43, 44]. In the case of IEEE 802.11b/g networks, the most popular as of today, 11 channels are available. However, only three of these channels (channel 1, 6, and 11) are non-overlapping channels. This is due to the fact that the bandwidth required by the wireless signal is greater than the channel spacing as shown on Figure 19.

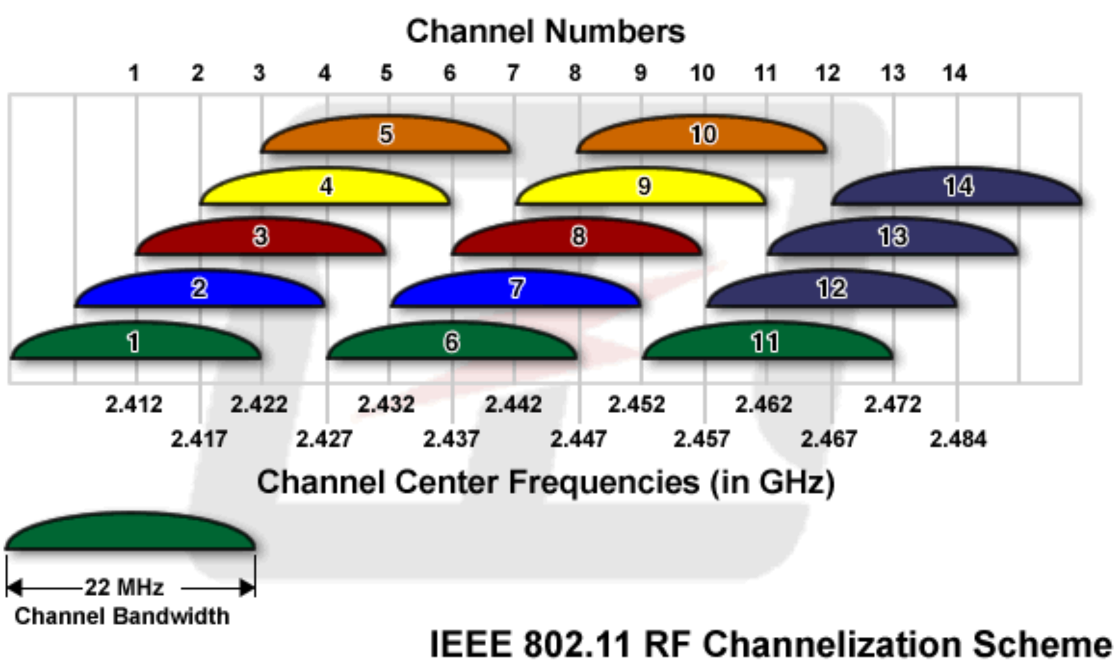


Figure 19. Channel Spacing in IEEE 802.11b © HyperLink Technologies, Inc.

Therefore, while there are 11 channels available, optimal performance will be obtained when no more than 3 channels are used for transmission and they are spread accordingly on channels 1, 6 and 11, respectively. This may become a source of problems when home networking equipment has to compete with Wireless Internet Service Provider (WISP), city-wide offerings, and neighbors' equipment for the scarce resource of the wireless spectrum in the ISM band. Projects like San Francisco TechConnect [47] or Wireless Philadelphia [87] are planning to cover the whole city with Wi-Fi signals. How these projects will co-exist with personal networks, community networks and commercial WISPs has not yet been defined.

While we do not intend to solve the issue of managing the available spectrum with our design, we can note that a global and standardized system of information disclosure like the one we describe (section 4.6) could serve to detect RF channel interference and overuse of the spectrum earlier.

4.4.4.2.Limited throughput

Clients connected on the same wireless network have to share a fixed amount of data throughput. The more clients that are connected to a wireless network, the less available the network access is. In fact, each client sends and receives data on the channel while it is free of any other communication, which is more infrequent as the number of clients increase.

4.4.4.3.Network neutrality

The principle of network neutrality can be defined as "a principle of internet regulation with particular relevance to the regulation of broadband. It suggests that (1) to maximize human welfare, information networks ought be as neutral as possible between various uses or applications, and (2) if necessary, government ought to intervene to promote or preserve the neutrality of the network." [116] According to Michael Powell, then chairman of the FCC:

- Consumers are entitled to access the lawful Internet content of their choice;
- Consumers are entitled to run applications and services of their choice, subject to the needs of law enforcement;
- Consumers are entitled to connect their choice of legal devices that do not harm the network; and
- Consumers are entitled to competition among network providers, application and service providers, and content providers.

The reason that network neutrality is so important in the case of wireless networks is that wireless networks rely on shared resources, such as radio frequency spectrum, as described in section 4.4.4. Therefore, network administrators may have to compromise on the number of services made available in order to satisfy a larger user base. High data rate services such as video streaming can clog the network and disrupt access to most of the network's patrons. Compromises between the size of the audience and the level of services to be provided are then decided on an administrative level. This usually explains why network administrators block high data rate services in order to serve the maximum number of users. This raises the issue of which services should be blocked or restricted and how to inform network users of such limitations.

4.4.5. User tracking

The fact that wireless networks are getting more ubiquitous creates opportunities to provide also geo-localization services [34] [96] on top of the wireless infrastructure. Research projects such as Intel Placelab [20] are looking for ways to use the wireless networking infrastructure in order to relate computing services to user's geographic location. As MIT iSpots, a similar project at the Massachusetts Institute of Technology has shown (see Figure 20), a user can be fairly accurately mapped to his or her current location based on information provided by the Wi-Fi network infrastructure. While geo-localized services described earlier (section 4.1) make use of this information, the privacy implications of the availability of this information have yet to be seen.

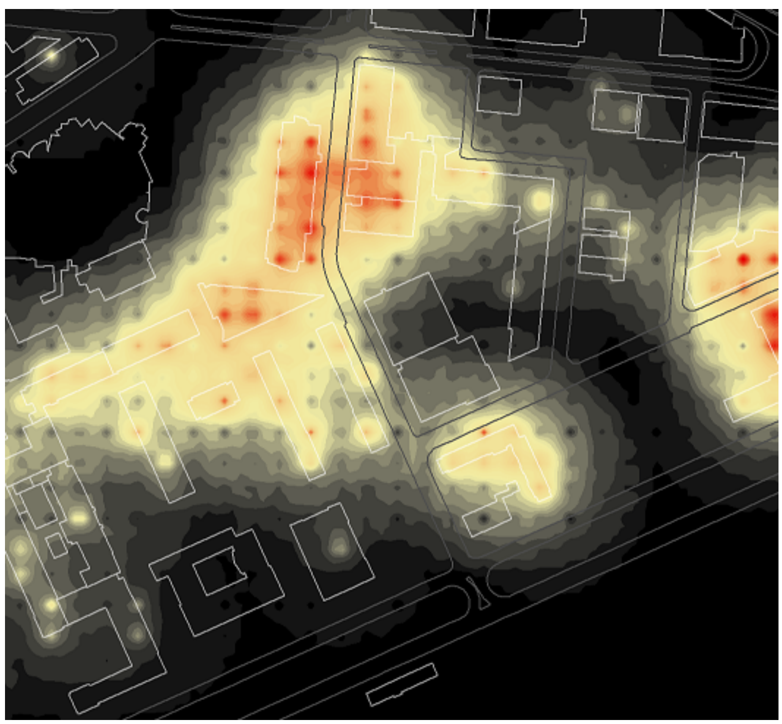


Figure 20. MIT iSpots User Tracking System © MIT

4.4.6. Choice and User control

4.4.6.1.Adaptation and scalability

As shown earlier, the very nature of wireless networking makes it necessary to enforce security for transmission of sensitive information. While securing all wireless transmissions should be the goal, economic, technical or usability constraints may not make the implementation of wireless security possible. A lot of work in the field of Ubicomp has focused in system adaptability in regard to the context in which the user is. [38] Context awareness [36] [96] is even a field of study by itself. However, in regard to the setup of a particular wireless connection, all users of the network are generally subject to the same exact requirements. While this has made the technical specification easier to design and networks easier to deploy, it does not scale well to support all the devices and services in a computing environment. This issue has surfaced recently in the discussion of the design of San Francisco TechConnect citywide network as devices that do not implement a browser software would have no possibility to access the network in its current design.

4.4.6.2.Legacy system and lightweight computing

For example, if one device of the system does not support the authentication or security scheme provided by the network, no local action can be easily taken to support this device. A legacy system or a lightweight device that do not know the security protocol in place will not be able to connect to the network in any way. The only way for the network to support a wireless toy or a sensor which do not integrate the security encryption level may come down to shut down the security on the whole network.

While designing Wireless Andrew [17], one of the first large scale wireless networks, Carnegie Mellon University network administrators were faced with this same issue. “Some of the robots that use wireless cannot even do [dynamic host configuration protocol]. So the idea of forcing Sony or other robotics manufacturers to add a virtual private network (VPN) implementation in their robots for CMU is probably not practical.” [5]

4.4.6.3.Automatic connection

One of the features that helped wireless networking to spread was the “automatic connect” function integrated by default in most client software. Not only it would remember the previous settings for security and authentication as set up by the user, but it will also help to establish the connection. For example, Microsoft Windows XP integrates in its client an option named “Automatically connect to non-preferred networks” [74]. The software will attempt to connect on behalf of the user whether or not it is a known wireless network. This feature could potentially generate legal issues as described in section 4.4.2.

Also, preferred networks are identified by their network name (SSID) which is not a unique identifier. Networks that serve different locations and belong to different organizations can bear the same name. This was especially true a couple years ago when the access points were still complex to configure and a large number of them were named “tsunami”, Cisco’s default name for its wireless access points or “linksys.” Thus, the preferred networks settings may connect a client automatically to a network it does not belong to.

4.4.6.4.Decision support

The user has basic controls on his wireless network connectivity. The ability to connect and disconnect at will are offered in the technical specifications. The user can also make choices on which network he is willing to connect to. Unfortunately, the capacity of user control stops there. While the user can choose which network to connect to, he does so based on extremely limited information. The only information made available by default is the network name, the signal strength and whether or not security is enforced (Figure 21). Conversely, criteria such as connection speed, cost, reliability or trust cannot be assessed by the user based on standard implementation of the protocol.

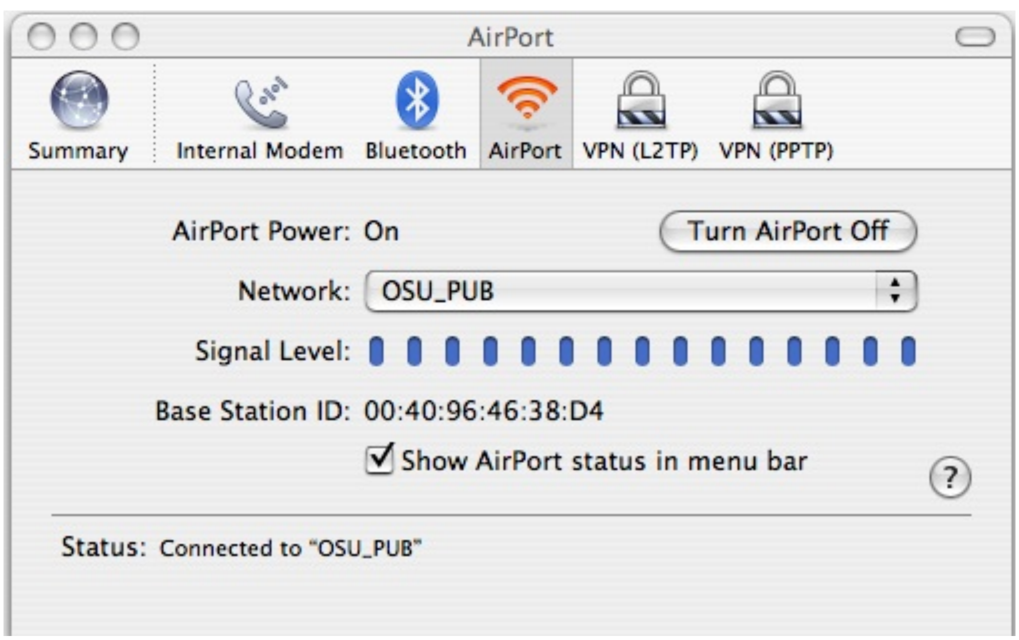


Figure 21. Screenshot of the Wireless Control Panel in Mac OS While Connected to OSU Public Wireless Network

4.4.6.5.Connection Speed and Signal Strength

Signal strength is one of the pieces of information generally provided to the user and may serve as a selection factor between connections, favoring connections providing a higher signal strength. However, signal strength and speed are not always correlated. Indeed, the stronger signal strength may not provide the best throughput or the best experience. "Hot spots are location-centric, which means that one hot spot can be more actively used than another hot spot depending on their locations. If a wireless common has a very low ratio of active to not-so-active hot spots, the active hot spots are likely to take on unduly high burden of supporting the common." [89]

When the available connectivity options are:

- connecting to a 5-bar access point and contend with 150 users to get a low 2 Kbps
- a 4-bar access point where connection speed is at an average of 20 Kbps

Then, the user is to rely on what can be considered as incomplete information to make decisions.

4.4.6.6.Backhaul connection

Several elements need to be taken into account when accessing a wireless commons. Key resources used are the access points and the associated backhaul throughput available. While the access point may integrate the latest technological advancements and offer a highly reliable and fast local wireless connection, the access point is dependent on the backhaul throughput to be able to match the speed provided to the client on the wireless link.[89] As of mid-2005, the typical consumer grade access point can provide wireless connectivity up to 54 Mbit/s using the IEEE 802.11g specifications, while the fastest home broadband connectivity usually offers speeds of around 10 Mbit/s in the U.S and 20 Mbit/s in most of Europe. Therefore, considering both local and backbone connection speed could better inform the user of the capabilities of the network connectivity.

4.4.6.7.Trust

In the general implementation, the infrastructure is represented by only one level of granularity. The infrastructure is in fact presented unified around the network ID (the SSID) even if the network is comprised of several levels. Unless the client is using an advanced and specialized tool, she will be presented with a unique SSID that aggregate one or more access point in the near vicinity. The user can choose to connect to any of the networks bearing different SSID but the user do not usually have choice in regard to which access point to connect within the network matching the SSID name. It becomes therefore difficult for users to distinguish between legitimate access points and rogue access points portraying association to a wireless network by using the same SSID name. This trust problem is also likely to expand with the development of mesh technologies that enables a client to retransmit the signal it receives.

4.4.6.8.Offline decisions systems

Knowing if the network is on or off is not enough. Users will get more and more choices when it comes to high speed wireless connectivity. They will want to be able to make decisions based on accurate and comprehensive information, such as:

- Connection average speed
- Up Time
- Services available
- Service credentials

4.4.7. Interactive Learning

4.4.7.1.Wireless and physical spaces support

Wireless networks are bound to profoundly change the way we live and work. Projects like MIT ISPOTS are looking at identifying "the complex and dispersed individual movement patterns that make up the daily life..." and "how could future physical planning of the campus suit the community's changing needs" [101]. While this project outlines some perspectives on the evolution of wireless networks, it also outlines the current infrastructures weaknesses that require administrative commitment to provide users with interaction opportunities. Sophisticated tools are available to monitor and measure activities on high-speed wireless networks. However, these tools require to be installed on top of the existing infrastructure and require corresponding client applications to generate benefits to the target population of users.

An alternate design could be to provide some of the information at the access point level and use a distributed architecture for the client to retrieve additional information of interest from one or several online data repositories.

4.4.7.2.Community Knowledge

Wireless networks are usually shared resources (see section 4.4.4) that can provide highly different levels of services. The infrastructure could then benefit from community knowledge in supporting its operations such as troubleshooting the network, supporting new users or even recommending the best connection based on the activities to be conducted. The recommendations could help the client find an appropriate connection based, for example, on network restrictions (as explained in section 4.4.1.2). These restrictions could be enforced on the various available wireless networks and the limitations or preferences placed by the client itself. Intelligent agents could be designed to collect and make use of network information in a way that matches closely to the user's activities.

4.4.7.3.Statistics

The access point functions as a gateway between the network and the clients. Therefore, it could collect precious information about the network use. For example, the access point could compile statistics of connections failure based on the client devices, operating systems, number of users on the network, etc.

4.5. Room for improvement

Based on our findings, we can define some design ideas that need to be explored further in order to improve the user experience with Wi-Fi systems.

- **Provide more granularity in the visualization of the network architecture.**

  Wi-Fi networks can be individual access points, can be centered on a common

SSID (BSS) and can also be federated in a larger entity independent of location. The user interface may incorporate some of this information to support better user's activities.

- **Provide additional information at connection time**. Network name and signal strength may not represent the best selection criteria and additional information such as speed, privacy and security level, operator name, cost and access rights may prove more useful.
- **Provide network administrators with tools to manage access to its wireless network and inform user on the selected settings**. Access rights, type of use allowed and restrictions could be communicated to potential users of the connection to limit legal and usability issues.
- **Dynamically maintain the connection**. By providing statistical information about the connections, the user or the device, on his behalf, could make connectivity choices as needs or technical difficulties arise.

4.6. Our design model

4.6.1. Design questions

Table 6. Possible information to be provided by the Wi-Fi infrastructure to the user

Data	Model Component	Need	User / Infrastruc	In Use	Value
Network Name	Choice	Which networks are	Infrastruct	X	OSU_PUB
Network Name (Institution)		Who am I connecting to?	Infrastruct ure		Oregon State
Signal Strength		What is the quality of the	User	X	dBm
Security	Norms	Are there security measures in	Infrastruct	X	WPA
Authentication	Norms, Laws	Can I connect?	Infrastruct ure	X	Browser-based ONID
Type of Access	Choice, Law,	Am I allowed to connect?	Infrastruct		P u b l i c ,
Acceptable Use	Norms, Law	What are the rules in place?	Infrastruct	(X)	
Local Connection	Choice	How fast is my local	User		2.7 Mbps
Distant		How fast is the backbone	Infrastruct		5.3 Mbps
Preferred Networks	User Control, Memory, Filtering	Remember my previous settings and connect to my preferred network	User	(X)	OSU_PUB
Reliability	Filtering,	How reliable is this wireless	Both		Up for X
Connection Status	User Control	Am I connected?	User	X	Connected
Available services	Choice, Filtering	What services and activities are possible on this	Infrastruct ure		VPN,POP,I M
Number of Users		How many people are using the connection	Infrastruct ure		35

Table 6 describes some of the information that our model for improved interactions with Wi-Fi will try to implement based on the results of the analysis of our Wi-Fi study. Our design incorporates three major components: a network facts module, a network stats module and a connect commons license.

4.6.2. Network Facts

The Network Facts module provides general information about the operator of the network connectivity as well as the authentication and security settings. Information provided can be used to determine automatically how to connect by proving the proper credentials and determining if the security mechanisms enforced on the network are compatible with the ones implemented on the device performing the access.

Network Facts	OSU_PUB	
Operated by	**OSU**	EDU-ORST
Name on Certification	Oregon State University	EDU-ORST
Operator Type	University	EDU
Contact Name	John Doe	-
Contact Info	541-555-1000	-
Contact Info	john.doe3(@)oregonstate.edu	-
Authentication/Security	**Authentication-No Security**	-
Authentication	ONID Account Holder	ONID
Authentication Scheme	Browser-based	AUTH-HTTPS
Security	NO	SEC-0
Security Scheme	None	SECTY-0

Figure 22. Network Facts mock up display

This enables the device to select only connectivity options that are compatible and also inform the user of any discrepancies between the network and the device. For example, a portable device that does not support the transmission or security protocol used on one of the Wi-Fi network available can chose an alternate network for the transmission or alerts the user that the transmission is likely to fail because of incompatibilities. As more of the devices support wireless connectivity, gaining information on the wireless network operator can also be useful to make sure that the device is accessing the correct network and also receive support if needed.

4.6.3. Network Stats

A statistical report could contain information like the maximum local and distant transmission rate, current uptime and number of devices or users using a particular network connection. The distinction between the local access capabilities (e.g., speed to connect to a local network) and the distant access (e.g., speed to connect to the Internet) could be important for devices having multiple connectivity options.

Making decisions based on the connection speed of the link between the device and the local network will overlook the fact that access to the Internet may be several times slower than the one afforded through the local network providing the wireless connection.

4.6.4. Connect Commons License

Similarly to the Creative Commons license, a Connect Commons license could be provided by the producers of the connectivity to inform the consumers of the rights and privileges available through a particular connection. It is not uncommon for service providers to restrict or block particular usage of a network connection. For example, a network operator may block unsecured data exchange vulnerable to security exploits (such as File Transfer Protocol (FTP)) or limit services that consume a large amount of the network resources (e.g., peer to peer downloading or video broadcasting). Until now, being informed of these restrictions proved to be difficult. A license, both machine- and user-readable, could facilitate the access to this kind of information.

Licence	CO-FR-ALL-NOL-NOS-USOR	
Connect Commons Licence	Community-Free-AllServices-Nolimit-NoShare	
Access Type	Community	ONID account only
Cost	Free	No Cost
Services Allowed	All	No Restrictions on Services
Time Limitation	No	No Time Limitation
Connection Sharing	No	Retransmission of Signal is prohibited
Jurisdiction	US-OR	USA, Oregon

Figure 23. Connect Commons mock up interface

Also, a home network administrator would no longer have to resort to use security mechanisms to manage the permissions he wishes to associate with sharing the wireless access to his home network and the Internet. Occasional or temporary use could then be permitted to visitors and neighbors while the use as a permanent access could be forbidden.

4.7. Survey design

4.7.1. Choice of instrument and hypothesis testing

Due to the early stage of the design model, we decided to conduct a survey to test some of the ideas expressed. In regard to the legal issues defined earlier, we decided that an online and anonymous survey would provide us with better answers in regard to personal beliefs about the legality of the access to some Wi-Fi connections.

4.7.2. Survey goals

The goal of the survey was to explore some of the issues that were identified earlier in the exploratory Wi-Fi study. As there was no academic study found in the literature on the use of Wi-Fi, we needed to get an overall image on some of the basic uses of the technology before being able to research some of the more advanced issues we identified. Our main goals were:

- Assess the level of experience of users.
- Define the general settings of use both at home and outside the home.
- Determine the behavior and belief in regard to security, privacy and legal issues associated with the use of Wi-Fi.
- Test some of the hypotheses for improvement described in our design model.

4.7.3. Recruitment

As Wi-Fi is often used to obtain connection to the Internet, we believe that Wi-Fi users are a subsection of the general Internet population. Wi-Fi is yet to become as popular as the Internet and its adopters can be classified as ranging from early adopters to early majority of the online population. To target early adopters and early majority users, we selected to target a group with a similar adoption pattern: blog readers. As of early 2006, the blogosphere (also referred to as "blog ecosystem"), counted more than 30 millions blogs and in the US alone, it is believed that one in three Internet users regularly read blogs.

We used postings on Wi-Fi users forums and encouraged persons with a blog to post a link to our online survey. “Boing Boing”, a blog with a readership of 2.2 million subscribers, posted a link to the online survey that stayed on the front page for approximately four hours. While the distribution of responses is closely similar before and after the link was posted on “Boing Boing”, it is worth noted that half of the respondents to our survey took the survey during the time it was linked on the front page of “Boing Boing.”

The survey was taken by 536 people and the distribution of respondents based on self-reported Wi-Fi expertise is shown in Figure 24. A majority of respondents considered themselves as experts (55.1%) or familiar (33.3%) with the Wi-Fi technology. Therefore, the analysis of the survey results took into account the fact that our sample is much more accustomed to the technology that the general population

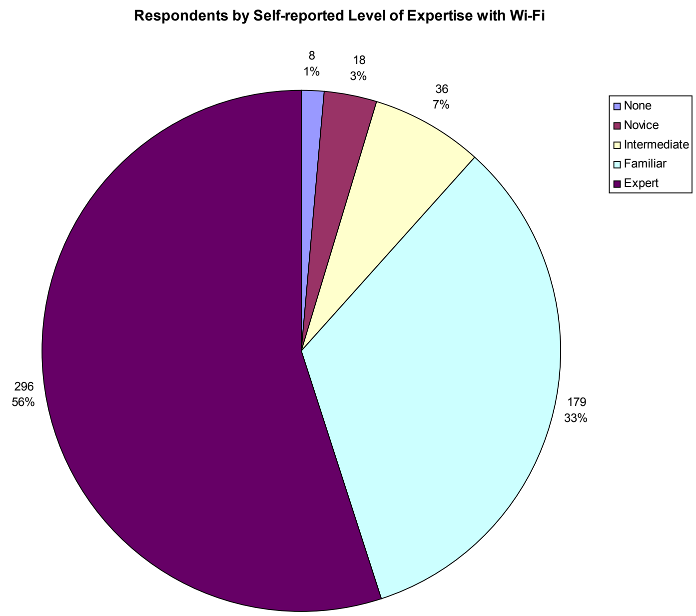


Figure 24. Survey Respondents by Self-Reported Level of Expertise with Wi-Fi

Respondent Type	Number	%
Expert	296	55.1
Familiar	179	33.3
Intermediate	36	6.7
Novice	18	3.4
None	8	1.5

4.7.4. Trends and Hypothesis testing

Based on our previous study and the aggregate results of the survey, we can formulate a series of hypotheses for which we will perform additional statistical analysis:

- There is a strong belief that an association exists between privacy and security mechanisms in Wi-Fi systems.

- The information currently provided to users of Wi-Fi systems for connectivity management is inadequate.
- Additional information not provided to users of Wi-Fi systems is judged necessary.
- Current existing laws are in contradiction with the behavior of most Wi-Fi users,

4.7.4.1.Importance Factors Analyses

In two combined questions of our survey, we asked respondents to rate the importance of 10 different criteria in the process of selecting a Wi-Fi connection in a public space. The results, rated by importance on a scale from 1 to 5 (1 being not important at all and 5 being very important), are shown in Table 7.

Table 7. Importance of Criteria in Selecting Public Wi-Fi Connection by Mean Value of Importance

Criteria	Mean Value
Network Name	1.60
Permission	2.73
Planned Use of the Connection	2.85
Trust / Reputation of the Provider	2.90
Login Required	2.96
Privacy	3.31
Security	3.31
Speed	3.99
Signal Strength	4.31
Cost of Use	4.47

After performing a multiple factor analysis with multiple range tests using Fisher's least significant procedure at a 95% confidence interval, we have identified groups of factors with means showing no statistically significant differences in the confidence interval.

Table 8. Grouping of Factors Based on Multiple Factor Range Tests at 95% least significant difference of means

Group 1	Network Name		
Group 2	Permission	Planned Use of the connection	
Group 3	Planned Use of the	Trust / Reputation of Service	Login
Group 4	Privacy	Security	
Group 5	Speed		
Group 6	Signal Strength	Cost of Use	

After further analysis, we identified that only group 4 shows no statistical difference between its means. Therefore, we looked further at the possible relationship between security and privacy in terms of importance.

4.7.4.2.Security and Privacy hypothesis

Security and privacy settings for Wi-Fi systems are complex. In addition to that, we showed earlier that privacy settings that can be inferred from security mechanisms in a wired space couldn't be expected to be available when using the same security mechanisms in a wireless space. Therefore, we were interested in measuring how people associate security mechanisms with privacy features when using a Wi-Fi connection.

For this purpose, we used a series of questions to measure the importance and satisfaction of several parameters including security and privacy, as well as several questions specific on security and privacy.

Previous studies [25] have shown that people are highly likely to respond to questions related to privacy and security in a way that do not always match their real behavior. Therefore, while we understand that the results of such an analysis would not constitute a strong evidence of respondents' behavior, we also believe that analyzing questions where the central focus was neither the security nor their privacy could still provide us with valuable insights on people's beliefs in this regard.

Based on the previous multiple factors analysis (Table 8) and the observed distribution of Privacy and Security importance (see Figure 25), we can formulate the following hypothesis:

Hypothesis 1: the perceptions of Privacy and Security are strongly related in Wi-Fi

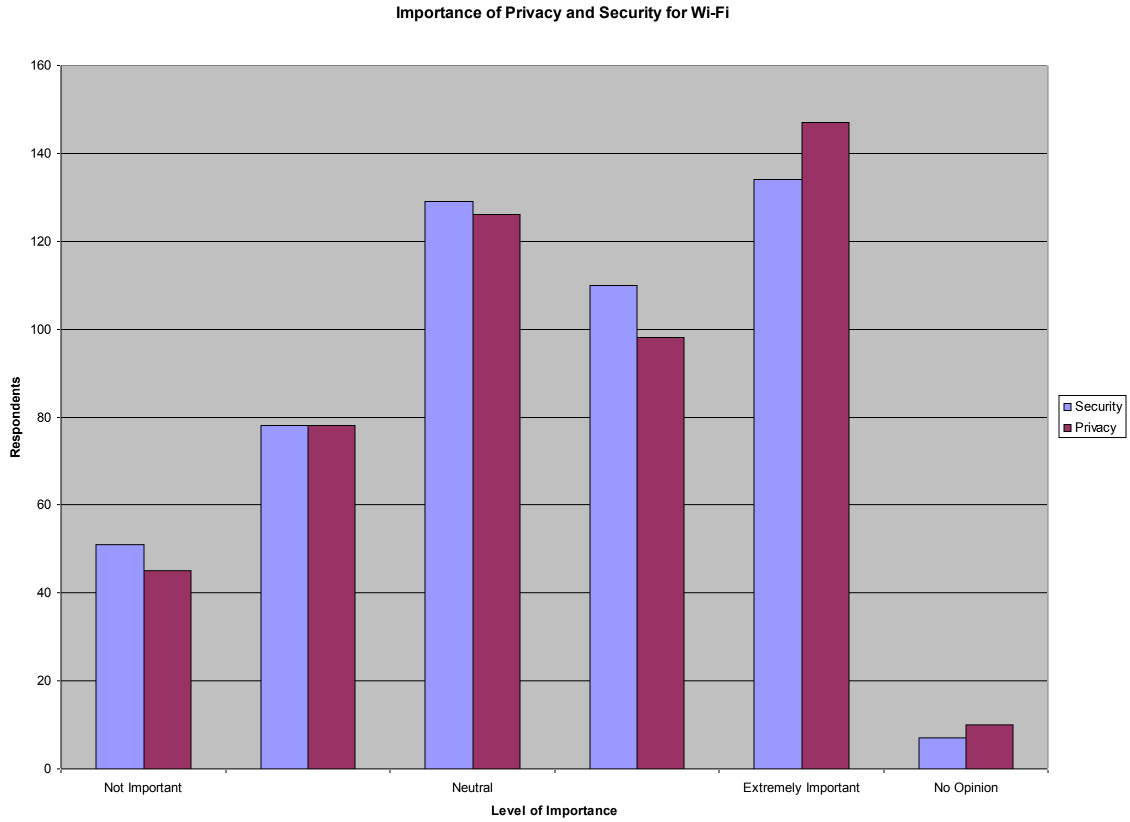


Figure 25 Expressed Importance of Security and Privacy

To test this hypothesis, we conducted a t-test and an ANOVA test on the responses regarding security and privacy in question 3.

The p-value for the t-test on equality of mean of criteria importance for security and privacy is 0.96 and do not enable us to reject hypothesis 1 for a confidence interval of 99%, leading to the conclusion that there is no significant difference in the mean for *importance of security* and *importance of privacy*.

The ANOVA (see Table 9) shows that a linear model accounts for 65% of the variability and that the factor *importance of security* is statistically significant (p-value =

0.0000) to explain the variation of *importance of privacy*. The correlation coefficient of 0.79 indicates a quite strong relationship between *importance of privacy* and *importance of security* in this context.

Table 9. ANOVA Table for Security and Privacy Importance

Source	Sum of Squares	Df	Mean Square	F-Ratio	P-Value
Model	674.114	1	674.116	930.53	0.0000
Residual	386.852	534	0.7244		
Total	1060.97	535			

A similar analysis, performed on both *privacy satisfaction* and *security satisfaction* parameters in regard to user satisfaction as expressed in answers to question 4, provides us with similar results. As shown on Figure 26 and Table 10, privacy and security show a strong relationship in regard to satisfaction (p-value = 0.0000). The ANOVA shows us that a linear model accounts for 44% of the variability. The correlation coefficient of 0.67 indicates a moderately strong relationship between *privacy satisfaction* and *security satisfaction* in this context.

Table 10. ANOVA Table for Security and Privacy Satisfaction

Source	Sum of Squares	Df	Mean Square	F-Ratio	P-Value
Model	318.7	1	318.7	416.04	0.0000
Residual	396.807	534	0.766037		
Total	715.508	535			

In question 16, we asked the following:

Compared to Wi-Fi access that does not request any information from you, do you think that **requesting a username and password in a browser provides data transmission** that is

Our goal was to determine if respondents could identify that the security mechanism described do not provide them with additional privacy. Our results indicate that 16% of the respondents assimilated the security mechanism described with increased privacy, while the question was formulated to provide with no expectation of increased privacy or security.

We also left space for comments and several of the comments we received were stating that be encrypting the username and password using the SSL protocol, they will expect that their data transmission will then become more private while in fact only the exchange of credentials will be more secure and private.

Based on these results, we can determine that security and privacy are strongly associated in regard to Wi-Fi.

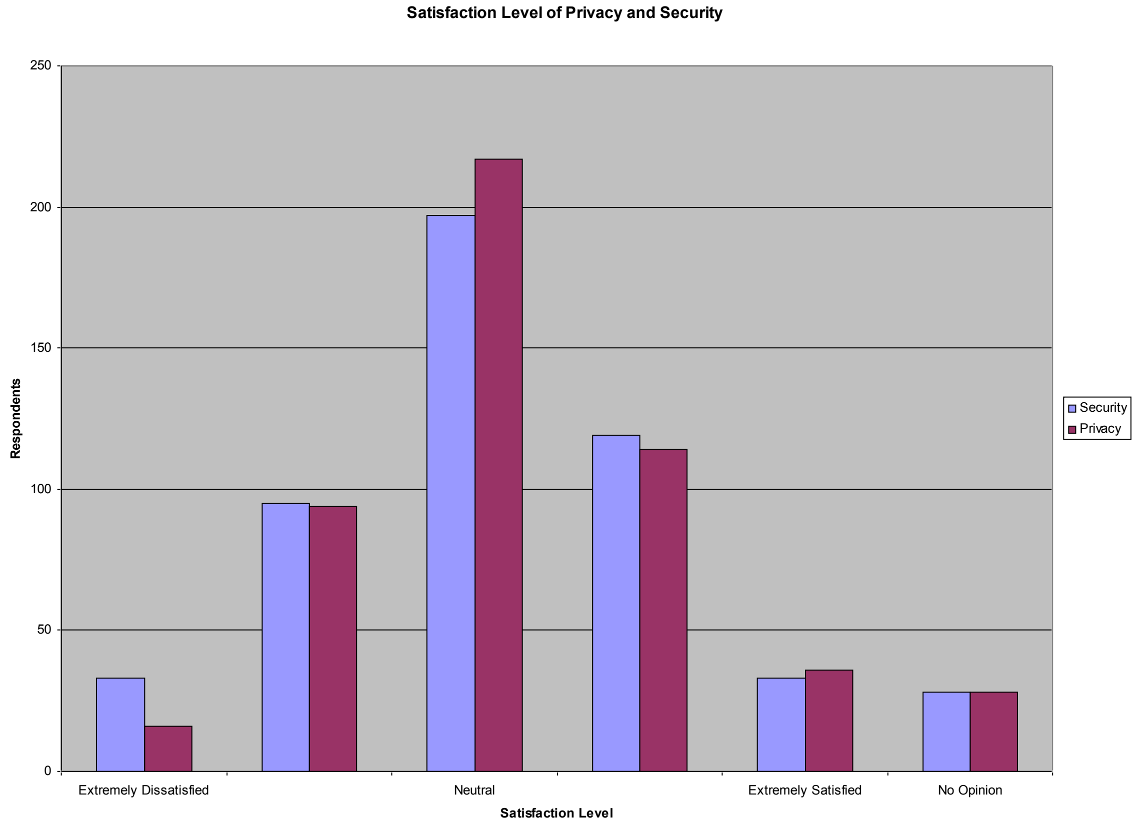


Figure 26 Satisfaction Level Expressed for Privacy and Security

4.7.4.3.Inadequate existing connectivity information

An analysis of the importance and satisfaction level expressed toward network name, signal strength and security information was also conducted. We looked for possible correlation with the self-reported level of experience with Wi-Fi and the education level in a computer related field.

Hypothesis 2: Network name, signal strength and security are not relevant elements in the selection of network connectivity.

We selected 10 factors for which to test relevance in the context of selecting a Wi-Fi connection in a public space. Of these factors, two are explicitly presented to the Wi-Fi user in terms of information during the connection (network name and signal strength) and a third is also partially visible (security). The rest of the information is not directly visible to the user, if available at all.

Table 11. Ratings of Existing Information delivered to Wi-Fi users before connection

	Mean Rating (out of 5)	Rank (out of 10)
Signal Strength	4.31	2
Security	3.31	4
Network Name	1.60	**10**

While both signal strength and security ranked high in terms of importance in the process of selecting a Wi-Fi connection, network name, which is one of the most preeminent information provided by Wi-Fi equipment is ranked last out of the 10 criteria offered for selection to the survey respondents.

A more detailed look at the results shows the distribution of the ratings was as follows.

Table 12. Expressed importance of existing information provided by Wi-Fi equipment (in % of respondents)

	Not Important		Neutral		Extremely Important
Signal Strength	0%	2%	10%	**30%**	**57%**
Security	10%	15%	25%	**21%**	**27%**
Network Name	**55%**	14%	15%	6%	4%

A large majority of respondents (87%) expressed that signal strength was important or extremely important information to have available when selecting a Wi-Fi connection. Similarly, 47% believed that security information was relevant while 25% believed it was not. However, 55% of all respondents stated that network name was not important at all in their selection process and only 10% believed it was important or extremely important.

As shown on Figure 27, among all the selections offered to the survey respondents, network name was by far the one that generates the largest amount of responses categorizing it as non-important. While signal strength and security ranked respectively second and fourth in terms of importance, network name was ranked 10^{th} and last by a significant margin.

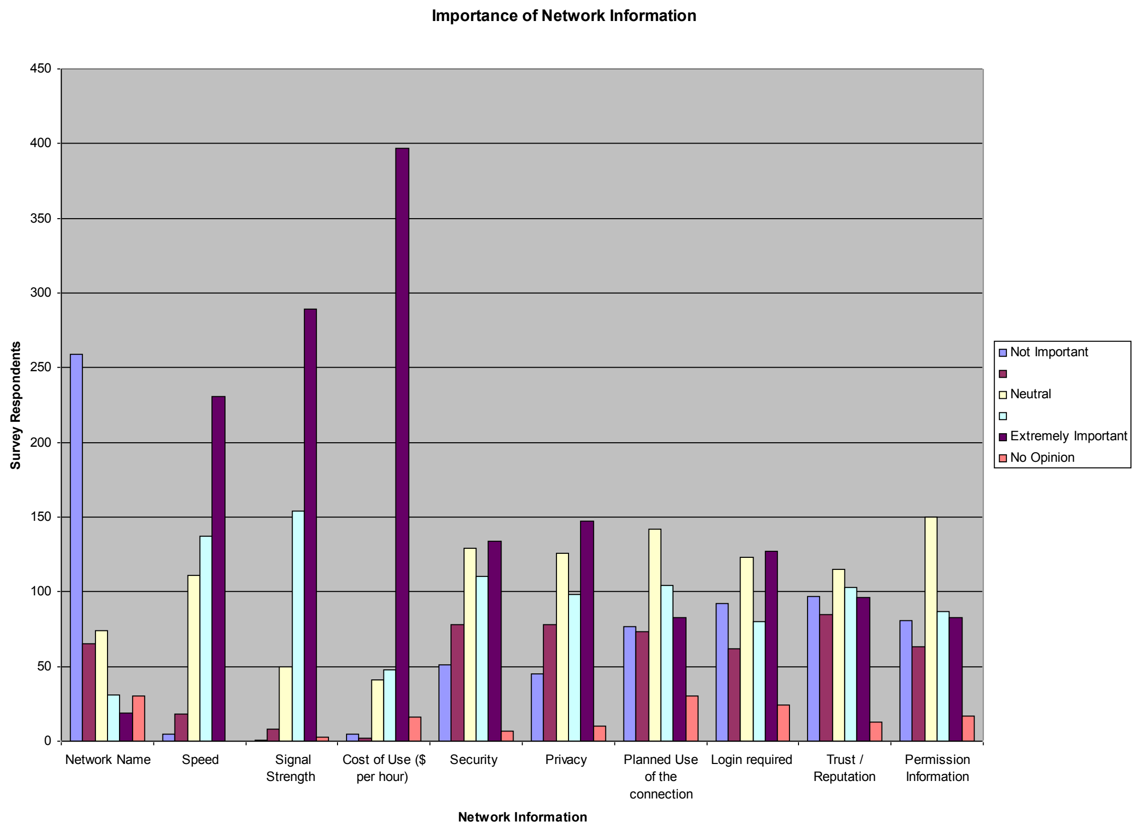


Figure 27. Importance level of various factors in selecting a public connection

This shows that some basic information (or what we called earlier "metadata") about the connection is not judged appropriate while other metadata not currently made available could serve the user better.

4.7.4.4.Adequate non-existing connectivity information

Based on the previous analysis, we have observed that existing metadata provided by Wi-Fi equipment are not judged as relevant as some information not currently provided or difficult to acquire. Therefore we analyzed the importance and satisfaction level expressed toward speed, cost of use, privacy, planned use, login requirement and trust level information. We looked for possible correlation with the self-reported level of experience with Wi-Fi and the education level in a computer related field.

Hypothesis 3: Speed, cost of use and other information are relevant elements in the selection of network connectivity.

Based on Figure 27, we can observe that cost of use and speed, two of the four metadata information the best rated, are not currently available before connection.

Table 13. Ratings of Information non-available from Wi-Fi users before connection

	Mean Rating (out of 5)	Rank (out of 10)
Cost of Use	4.47	1
Speed	4.00	3

Table 14. Expressed importance of information not provided by Wi-Fi equipment (in % of total respondents)

	Not Important		Neutral		Extremely Important
Cost of Use	1%	1%	8%	9%	**78%**
Speed	1%	3%	23%	**25%**	**45%**

Information about cost of use was extremely important for 79% of the survey respondents when selecting a Wi-Fi connection while only 2% of respondents believed in the opposite. Similarly 70% of all respondents stated that connection speed information was in some regard important to them. This is significant since Wi-Fi users are required to try and connect to a particular connection before they can even start to assess either cost of use or speed of the selected connection and of the other ones also available in the neighborhood.

While respondents are split in regard to the other information that could be used to select a particular connection (e.g., permission, trust, privacy or need for login), it is still significant that any of these information ranked higher that one already provided in the form of network name.

4.7.4.5.Legal implications of Wi-Fi

We were also interested in determining the common behavior of users in regard to access to open wireless networks. We asked the following question:

> Have you ever accessed a Wi-Fi network for which you did not expect to have explicit permission?

The majority of survey participants (80%) responded ”YES” to this question. This shows that connecting to a Wi-Fi network without explicit permission is a common behavior among respondents to our survey. This goes against the general interpretation of US federal law and helps justify the need for a permission disclosure system as described in our design.

Here are some of the comments left by survey respondents:

> In the 1800's there was a thing in the western US called "Free-Graze". It basically stated that if you owned land and you chose not to fence (or secure) that land, then it was open to anyone to graze their livestock on. The burden was on the landowner to secure his property. If he did not fence it then it was open for anyone to use. Wi-Fi is no different. If you're going to broadcast a signal into a public area and you don't secure it, then it's

I'm concerned about making my WiFi connection publicly available because of what someone may use my connection for. Inept law enforcement would _not_ understand that a connection from your house (WiFi) was not necessarily you.

If the wifi network is unencrypted and does not require a log-in or expressly require payment or registration/authentication or expressly limit how the connection may be used it should be perfectly legal to use the connection freely without seeking permission to use it.

Most of the comments left in the open part of the survey were related to the legal implications of using or sharing an open Wi-Fi access. This clearly indicates that the legal aspects of the use of Wi-Fi

4.8. Conclusions of Wi-Fi Study

Based on the results of both our analysis and our survey, we can recognize that systems using Wi-Fi connectivity could be improved in terms of user experience by implementing some of the concepts described in our design described in section 4.6. Providing more and different information to the user to support connection choices in the form of some descriptive metadata has been validated by the survey results. While survey respondents have described network name as not helpful, they have expressed strong interests for knowing the cost and speed of the different connections available, information that is not currently provided.

The difficulty for survey respondents to differentiate between security and privacy also confirms some of the issues identified in our case study and the need for improvement in this area.

Finally, the inadequacy of the law with common social norms in regard to access to open Wi-Fi network has been demonstrated and supports the need for better policy management and permission disclosure.

5. Contribution

Ubicomp is becoming more of a reality every day. Nevertheless, past and current research has looked at Ubicomp from a limited perspective especially in terms of integration [33]. Gellersen and Davies's research highlighted that most of the system components are readily available but that there were conceived and managed without the overview required to make them work easily in a ubiquitous environment.

Our research took a multidisciplinary approach at defining the design requirements for the user in a ubiquitous. By isolating and characterizing common requirements and methodologies that made each of the Ubicomp research projects successful, we were able to define a framework of design questions to be answered in order to build an environment as close as possible to the vision of Mark Weiser.

One challenge faced in this endeavor was be to integrate the different needs and aspirations unveiled from research as various as human-computer interaction, social sciences, business, ethics, privacy, new media communication or engineering. As shown in an overview of the past research in ubiquitous computing [2], evaluating the impact of our research on an Ubicomp environment is too complex to be done globally. Our approach was to define major components that were more likely to be affected in regard to managing and deploying an Ubicomp environment. While limited, this approach gave us insight on how the selected components and requirements associated have an impact on the design of an Ubicomp environment and help us shape a framework of design implications.

This work provides insight to system application designers and IT administrators on how to improve the information flow within an ubiquitous information system through the use of the design framework defined in this document. The description of some appropriate evaluation techniques, with their advantages and drawbacks, could also help information systems designers in defining evaluation plans for their system design. The review of current technology options could also prove valuable in helping designers define the technological infrastructure of their system.

6. Future Work

The main objective of this research was to provide an overview of the design requirements of an Ubicomp system in regard to improving user experience. To achieve this goal, an extensive review of the literature and evaluation techniques was established, a framework of design questions was compiled and current and appropriate technology options were identified.

While the Wi-Fi study helped us demonstrate the benefit of our approach, we believe that using the framework and the associated information described in this document on Ubicomp system different from the Wi-Fi infrastructure could help us significantly improve our framework. Also, the Wi-Fi study could be complemented by a system implementation of some of the design concepts described to provide with a better overall validation of this research.

7. Bibliography

1. New Hampshire HB0495.An act relative to unauthorized access to a wireless computer network. *State of New Hampshire*, 2004.

2. Abowd, G.D. and Mynatt, E.D. Charting past, present, and future research in ubiquitous computing. *ACM Trans. Comput.-Hum. Interact.*, *7* (1). 29-58.

3. Abowd, G.D., Mynatt, E.D. and Rodden, T. The human experience [of ubiquitous computing]. *Pervasive Computing, IEEE*, *1* (1). 48-57.

4. Ackerman, M., Darrell, T. and Weitzner, D.J. Privacy in Context. *Human-Computer Interaction*, *16* (2, 3 & 4). 167-176.

5. ARABASZ, P., AND PIRANI, J. . Wireless networking at Carnegie Mellon University, ECAR, EDUCAUSE, 2002.

6. Arbaugh, W.A. Wireless Security Is Different. *Computer*, *36* (8). 99-101.

7. Arnstein, L., Grimm, R., Hung, C.-Y., Kang, J.H., LaMarca, A., Look, G., Sigurdsson, S.B., Su, J. and Borriello, G. Systems Support for Ubiquitous Computing: A Case Study of Two Implementations of Labscape in *Proceedings of the First International Conference on Pervasive Computing* Springer-Verlag, 2002 30-44

8. Arnstein, L., Hung, C.-Y., Franza, R., Zhou, Q.H., Borriello, G., Consolvo, S. and Su, J. Labscape: a smart environment for the cell biology laboratory. *Pervasive Computing, IEEE*, *1* (3). 13-21.

9. Barkhuus, L. and Dey, A. *Is Context-Aware Computing Taking Control away from the User? Three Levels of Interactivity Examined*, 2003.

10. Barkhuus, L. and Dourish, P. Everyday Encounters with Context-Aware Computing in a Campus Environment. in *Proceedings of the Sixth International Conference on Ubiquitous Computing Ubicomp 2004*, Nottingham, United Kingdom, 2004, 232-249.

11. Battiti, R., Cigno, R.L., Sabel, M., Orava, F. and Pehrson, B. Wireless LANs: From WarChalking to Open Access Networks. *Mobile Networks and Applications*, *10* (3). 275-287.

12. Bausch, P. *We blog : publishing online with weblogs*. Wiley Pub., Indianapolis, IN, 2002.

13. Beckwith, R. Designing for Ubiquity: The Perception of Privacy. *IEEE Pervasive Computing*, *2* (2). 40-46.

14. Bell, G., Blythe, M., Gaver, B., Sengers, P. and Wright, P. Designing culturally situated technologies for the home. in *CHI '03 extended abstracts on Human factors in computing systems*, ACM Press, Ft. Lauderdale, Florida, USA, 2003, 1062-1063.

15. Bellotti, V. and Sellen, A., Design for Privacy in Ubiquitous Computing Environments. in *Proceedings of the Third European Conference on Computer Supported Cooperative Work ({ECSCW}'93)*, (1993), 77-92 PU - Kluwer.

16. Bellotti, V. and Smith, I., Informing the design of an information management system with iterative fieldwork. in *DIS '00: Proceedings of the conference on Designing interactive systems*, (2000), 227-237 PU - ACM Press.

17. Bernard, J.B. and Charles, R.B. Wireless Andrew: building a high speed, campus-wide wireless data network. *Mob. Netw. Appl.*, *6* (1). 9-22.

18. Berners-Lee, T., Cailliau, R., Luotonen, A., Nielsen, H.F. and Secret, A. The World-Wide Web. *Commun. ACM*, *37* (8). 76-82.

19. Bible, J.D. and McWhirter, D.A. *Privacy in the workplace : a guide for human resource managers*. Quorum Books, New York, 1990.

20. Bill, N.S., Anthony, L., Gaetano, B., William, G.G., David, M., Edward, L., Anand, B., Jason, H. and Vaughn, I. Challenge: ubiquitous location-aware computing and the "place lab" initiative *Proceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots*, ACM Press, San Diego, CA, USA, 2003.

21. Billsus, D., Brunk, C.A., Evans, C., Gladish, B. and Pazzani, M. Adaptive interfaces for ubiquitous web access. *Commun. ACM*, *45* (5). 34-38.

22. Borriello, G. Key challenges in communication for ubiquitous computing. *Communications Magazine, IEEE*, *40* (5). 16-18.

23. Brown, B., Green, N. and Harper, R. *Wireless world : social and interactional aspects of the mobile age*. Springer, London ; New York, 2002.

24. Cairncross, F. *The Death of Distance: How the Communications Revolution Will Change Our Lives*. Harvard Business School Press, 1997.

25. Carlos, J., Colin, P. and Christian, J. Privacy practices of Internet users: self-reports versus observed behavior. *Int. J. Hum.-Comput. Stud. %@ 1071-5819*, *63* (1-2). 203-227.

26. Carr, N.G. *Does IT matter? : information technology and the corrosion of competitive advantage*. Harvard Business School Press, Boston, 2004.

27. Christensen, C.M. *The innovator's dilemma : when new technologies cause great firms to fail*. Harvard Business School Press, Boston, Mass., 1997.

28. Congress, U.S. Computer Fraud and Abuse Act, 1986.

29. Cranor, L.F. and Brian, A.L. Spam! *Commun. ACM*, *41* (8). 74-83.

30. Cummings, J. and Kraut, R. Domesticating computers and the Internet. *Information Society*, *18* (3). 221-232.

31. Dahlbäck, N., Jönsson, A. and Ahrenberg, L. Wizard of Oz studies: why and how. in *Proceedings of the 1st international conference on Intelligent user interfaces*, ACM Press, Orlando, Florida, United States, 1993, 193-200.

32. Dahlen, B.J., Konstan, J. A., Herlocker, J. L., Good, N., Borchers, A., and Riedl, J. Jump-starting movielens: User benefits of starting a collaborative filtering system with "dead data", University of Minnesota, 1998.

33. Davies, N. and Gellersen, H.-W. Beyond prototypes: challenges in deploying ubiquitous systems. *Pervasive Computing, IEEE*, *1* (1). 26-35.

34. Davis, M., Simon, K., Nathan, G. and Risto, S. From context to content: leveraging context to infer media metadata *Proceedings of the 12th annual ACM international conference on Multimedia* ACM Press, New York, NY, USA, 2004, 188-195.

35. Dey, A.K., Evaluation of Ubiquitous Computing Systems: Evaluating the Predictability of Systems. in *Proceedings of Evaluation Methods for Ubiquitous Computing Workshop*, (2001), Springer-Verlag.

36. Dey, A.K. Understanding and Using Context. *Personal Ubiquitous Comput.*, *5* (1). 4-7.

37. Dourish, P. *Where the action is : the foundations of embodied interaction*. MIT Press, Cambridge, Mass., 2001.

38. Dourish, P. and Edwards, W.K. A Tale of Two Toolkits: Relating Infrastructure and Use in Flexible CSCW Toolkits. *Comput. Supported Coop. Work*, *9* (1). 33-51.

39. ECPA. ELECTRONIC COMMUNICATIONS PRIVACY ACT *ECPA*, 1986.

40. Edwards, W., Policies and roles in collaborative applications. in *CSCW '96: Proceedings of the 1996 ACM conference on Computer supported cooperative work*, (1996), 11-20 PU - ACM Press.

41. Edwards, W.K., Bellotti, V., Dey, A.K. and Newman, M.W. The challenges of user-centered design and evaluation for infrastructure. in *Proceedings of the SIGCHI conference on Human factors in computing systems*, ACM Press, Ft. Lauderdale, Florida, USA, 2003, 297-304.

42. Edwards, W.K., Newman, M.W., Sedivy, J. and Izadi, S. Challenge:: recombinant computing and the speakeasy approach in *Proceedings of the 8th annual international conference on Mobile computing and networking* ACM Press, Atlanta, Georgia, USA 2002 279-286

43. FCC. Over-the-Air Reception Devices Rule, Federal Communications Commission, 2005.

44. FCC. Title 47 PART 15 : RADIO FREQUENCY DEVICES, Federal Communications Commission, 2004.

45. Finkin, M. *Privacy in Employment Law*. BNA Books, 1995.

46. Fischer, K. Agent-based design of holonic manufacturing systems. *Journal of Robotics and Autonomous Systems*.

47. Francisco, C.o.S. San Francisco TechConnect, 2005.

48. Franklin, M. and Stan, Z. “Data in your face”: push technology in perspective. *SIGMOD Rec.*, *27* (2). 516-519.

49. Goffman, E. *The presentation of self in everyday life*. University of Edinburgh, Social Sciences Research Centre, Edinburgh,, 1956.

50. Goldstine, H. *The Computer from Pascal to von Neumann*. Princeton United Press, 1972.

51. Grudin, J. The computer reaches out: the historical continuity of interface design. in *Proceedings of the SIGCHI conference on Human factors in*

computing systems: Empowering people, ACM Press, Seattle, Washington, United States, 1990.

52. Gupta, P. and Moitra, D. Evolving a pervasive IT infrastructure: a technology integration approach. *Personal Ubiquitous Comput.*, *8* (1). 31-41.

53. Haartsen, J.C. The Bluetooth radio system. *Personal Communications, IEEE [see also IEEE Wireless Communications]*, *7* (1). 28-36.

54. Herlocker, J.L., Konstan, J.A. and Riedl, J. Explaining collaborative filtering recommendations. in *Proceedings of the 2000 ACM conference on Computer supported cooperative work*, ACM Press, Philadelphia, Pennsylvania, United States, 2000.

55. Hong, J.I., G. Boriello, J.A. Landay, D.W. McDonald, B.N. Schilit, and J.D. Tygar, Privacy and Security in the Location-enhanced World Wide Web. in *Fifth International Conference on Ubiquitous Computing: Ubicomp 2003 (Workshop on Ubicomp Communities: Privacy as Boundary Negotiation)*, (Seattle, WA, 2003), Springer.

56. ITU. The Internet of Things. ITU ed. *ITU Internet Reports*, International Telecommunication Union, 2005.

57. IWS. WORLD INTERNET USAGE AND POPULATION STATISTICS, International World Stats, 2005.

58. Jiajun, Z. and Lie, L., Perceptual Visualization of a Music Collection. in *IEEE International Conference on Multimedia and Expo, 2005. ICME 2005.*, (2005), 1058-1061.

59. Jiwire. Jiwire Wi-Fi Service, 2006.

60. Kindberg, T., Barton, J., Morgan, J., Becker, G., Caswell, D., Debaty, P., Gopal, G., Frid, M., Krishnan, V., Morris, H., Schettino, J., Serra, B. and Spasojevic, M. People, Places, Things: Web Presence for the Real World. *Mobile Networks and Applications*, *7* (5). 365-376.

61. Kindberg, T. and Fox, A. System software for ubiquitous computing. *Pervasive Computing, IEEE*, *1* (1). 70-81.

62. Kleinrock, L. Nomadic computing—an opportunity. *SIGCOMM Comput. Commun. Rev.*, *25* (1). 36-40.

63. Kling, R. *Computerization and controversy : value conflicts and social choices*. Academic Press, San Diego, 1996.

64. Kobsa, A. Tailoring Privacy to Users' Needs. in *Proceedings of the 8th International Conference on User Modeling 2001*, Springer-Verlag, 2001, 303-313.

65. Lederer, S. Designing Disclosure: Interactive Personal privacy at the Dawn of ubiquitous computing *Computer Science Division*, University of California, Berkeley, Berkeley, 2003.

66. Lederer, S., Mankoff, J. and Dey, A.K. Who wants to know what when? privacy preference determinants in ubiquitous computing. in *CHI '03 extended abstracts on Human factors in computing systems*, ACM Press, Ft. Lauderdale, Florida, USA, 2003, 724-725.

67. Lee, Y. The CAN-SPAM Act: a silver bullet solution? *Commun. ACM*, *48* (6). 131-132.

68. Lemhachheche, R., Porter, J.D. and Puthpongsiriporn, T., Methodology for the Deployment of Effective Campus Wireless Environment Infrastructures. in *14th Industrial Engineering Research Conference*, (Atlanta, Georgia, 2005).

69. Lessig, L. *Code and other laws of cyberspace*. Basic Books, New York, 1999.

70. Manber, U., Patel, A. and Robison, J. Experience with personalization of Yahoo! *Commun. ACM*, *43* (8). 35-39.

71. Mantei, M.M. and Teorey, T.J. Cost/benefit analysis for incorporating human factors in the software lifecycle. *Commun. ACM*, *31* (4). 428-439.

72. McDaniel, T. Magneto-optical data storage. *Commun. ACM*, *43* (11). 56-63.

73. Mick, D.G. and Fournier, S. Paradoxes of Technology: Consumer Cognizance, Emotions and Coping Strategies. *Journal of Consumer Research*, *25* (2). 123-143.

74. Microsoft. To set up automatic wireless network configuration, 2005.

75. MIT. Project Oxygen, Pervasive, Human-centered Computing, 2000.

76. Molnar, D. and Wagner, D., Privacy and security in library RFID: issues, practices, and architectures. in *CCS '04: Proceedings of the 11th ACM conference on Computer and communications security*, (2004), 210-219.

77. Moore, G.E. Cramming more components onto integrated circuits. *Electronics*, *38* (8). 56-59.

78. Newman, M.W., Izadi, S., Edwards, W.K., Sedivy, J.Z. and Smith, T.F. User interfaces when and where they are needed: an infrastructure for recombinant computing. in *Proceedings of the 15th annual ACM symposium on User interface software and technology*, ACM Press, Paris, France, 2002, 171-180.

79. Nielsen, J. Heuristic evaluation. in *Usability inspection methods*, John Wiley \& Sons, Inc., 1994, 25-62.

80. Norman, D.A. Design principles for human-computer interfaces *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, ACM Press, Boston, Massachusetts, United States, 1983.

81. Norman, D.A. *The invisible computer*. MIT Press, 1998.

82. Norman, D.A. and Draper, S.W. *User centered system design : new perspectives on human-computer interaction*. L. Erlbaum Associates, Hillsdale, N.J., 1986.

83. O'Hara, B. and Petrick, A. *The IEEE 802.11 Handbook: A Designer's Companion*. Standards Information Network IEEE Press, 1999.

84. Osborne, A. *An introduction to microcomputers*. McGraw-Hill, 1976.

85. Palen, L. and Marilyn, S. Welcome to the wireless world: problems using and understanding mobile telephony. in *Wireless world: social and interactional aspects of the mobile age*, Springer-Verlag New York, Inc., 2002, 135-153.

86. Pankoke-Babatz, U., Klockner, K. and Jeffrey, P. Norms and conventions in collaborative systems *Proceedings of the HCI International '99 (the 8th International Conference on Human-Computer Interaction) on Human-Computer Interaction: Communication, Cooperation, and Application Design-Volume 2 - Volume 2*, Lawrence Erlbaum Associates, Inc., 1999.

87. Philadelphia, C.o. Wireless Philadelphia, 2005.

88. Plazes Plazes Wi-Fi Location service.

89. Rao, B. and Parikh, M.A. Wireless broadband drivers and their social implications. *Technology in Society*, *25* (5). 477-489.

90. Rivero, J., Porter, J.D., Puthpongsiriporn, T., Layton, W.M. and Lemhachheche, R. Campus Wireless Environment Deployment Guide, Intel Corporation - Oregon State University, 2005.

91. Rogers, E.M. *Diffusion of innovations*. Free Press, New York, 2003.

92. Russ, H. and William, A. Security problems in 802.11-based networks. *Commun. ACM*, *46* (5). 31-34.

93. Salber, D., Dey, A.K. and Abowd, G.D. The context toolkit: aiding the development of context-enabled applications. in *Proceedings of the SIGCHI conference on Human factors in computing systems: the CHI is the limit*, ACM Press, Pittsburgh, Pennsylvania, United States, 1999, 434-441.

94. Satyanarayanan, M. Pervasive computing: vision and challenges. *Personal Communications, IEEE [see also IEEE Wireless Communications]*, *8* (4). 10-17.

95. Schachter, J. Del.icio.us, 2003.

96. Schilit, B., Adams, N. and Want, R., Context-aware computing applications. in *Mobile Computing Systems and Applications, 1994. Proceedings., Workshop on*, (1994), 85-90.

97. Schmidt, A. Ubiquitous Computing – Computing in Context., PhD thesis - Lancaster University, 2002.

98. Schmidt, A., Beigl, M. and Gellersen, H. There is more to context than location. *Computers and Graphics*, *23* (6). 893-901.

99. Scholtz, J. and Consolvo, S. Towards a Discipline for Evaluating Ubiquitous Computing Applications, Intel Research, Seattle, Washington, 2004.

100. Semacode. Semacode, 2002.

101. SEVTSUK A., R.C., iSpot: describing the use of space on the mit campus through the analysis of wifi networks. in *CUPUM '05: The Ninth International Conference on Computers in Urban Planning and Urban Management*, (London, 2005).

102. Sharples, M., Corlett, D. and Westmancott, O. The Design and Implementation of a Mobile Learning Resource. *Personal and Ubiquitous Computing*, *6* (3). 220-234.

103. Shneiderman, B. *Designing the user interface : strategies for effective human--computer interaction*. Addison-Wesley, Reading, Mass., 1992.

104. Smart, L. Making Sense of RFID. *Library Journal*, *129* (Fall 2004). 4-11.

105. Smetters, D.K. and Grinter, R.E., Moving from the design of usable security technologies to the design of useful secure applications. in *Workshop on New security paradigms*, (Virginia Beach, Virginia, 2002), ACM Press, 82-89.

106. Tatarinov, I., Ives, Z.G., Halevy, A.Y. and Weld, D.S. Updating XML. in *Proceedings of the 2001 ACM SIGMOD international conference on Management of data*, ACM Press, Santa Barbara, California, United States, 2001.

107. Toyama, K., Ron, L. and Asta, R. Geographic location tags on digital images *Proceedings of the eleventh ACM international conference on Multimedia*, ACM Press, Berkeley, CA, USA, 2003.

108. Union, E. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 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*, 1995.

109. Vanderwal. Folksonomy, 2005, http://www.vanderwal.net/random/entrysel.php?blog=1750.

110. Want, R., Hopper, A., Falcão, V. and Gibbons, J. The active badge location system. *ACM Trans. Inf. Syst.*, *10* (1). 91-102.

111. Weiser, M. The computer for the 21st century. *Scientific American*, *265* (3). 94-104.

112. Weiser, M. The major trends in computing, 1996.

113. Weiser, M. Some computer science issues in ubiquitous computing. *SIGMOBILE Mob. Comput. Commun. Rev.*, *3* (3). 12.

114. Westin, A.F. *Privacy and freedom*. Atheneum, New York,, 1967.

115. Wheatley, M. ERP Training Stinks *CIO Magazine*, 2000.

116. Wikipedia Network Neutrality.

117. Winer, D. RSS 2.0 Specification http://blogs.law.harvard.edu/tech/rss, Harvard Law School, 2003.

118. Wixon, D., Holtzblatt, K. and Knox, S. Contextual design: an emergent view of system design. in *Proceedings of the SIGCHI conference on Human factors in computing systems: Empowering people*, ACM Press, Seattle, Washington, United States, 1990.

119. Yin, R.K. *Case study research : design and methods*. Sage Publications, Thousand Oaks, Calif., 2003.

8. Appendix

The Wi-Fi online survey is attached as a PDF file