Association for Information Systems
AIS Electronic Library (AISeL)

UK Academy for Information Systems Conference Proceedings 2010

UK Academy for Information Systems

Spring 3-23-2010

Ubiquitous Information Systems – Understanding privacy concerns

David Bell
Brunel University, david.bell@brunel.ac.uk

Samuel Odofin
Brunel University

Ubiquitous Information Systems – Understanding privacy concerns

Samuel Odofin and David Bell
School of Information Systems, Computing and Mathematics
Brunel University, Uxbridge, United Kingdom.

Email: david.bell@brunel.ac.uk

Abstract

Ubiquitous information systems (UBIS) adapt current Information System thinking to explicitly differentiate technology between hardware devices and software components. An unfolding vision of vast numbers of computing devices becoming a pervasive part of our everyday lives in underway as more routine activities move into the realm of information and communication technology (ICT). Customer loyalty smart card tracking, mobile and smart phone application, wireless MP3 players, intelligent key cards, close circuit television cameras, motion sensors, electronic passports and RFID cards are some of the frequently used ubiquitous devices that handle personal information about their owners and of which a typical average consumer could own more than one of them. This research paper investigates personal privacy issues confronting ubiquitous system users with the aim of constructing a framework that can help designers of such systems to better protect the personal privacy of the users of these systems through the integration of certain design concepts suggested by the framework into their design processes. Ten selected users of ubiquitous devices were interviewed, focusing on issue around the misunderstanding of some personal privacy concepts relating to their ubiquitous devices and locations of use. Interview responses were transcribed into electronic format and analyzed using grounded theory analysis and micro-coding techniques. The grounded theory analysis led to the identification of five concepts: Scope of potential disclosure of information, Scope of actual disclosure of information, Complexity of configuration, Top level control mechanism and integration of existing practices.

Keywords: Ubiquitous/Pervasive Computing, Privacy, Grounded Theory

1.0 Introduction

Mark Weiser (1991) described the term ubiquitous computing as the seamless interaction between various computer systems and people without restrictions on location or time. The field of ubiquitous computing envisages an era when the typical consumer owns hundreds or thousands of mobile and embedded computing devices (Weiser, 2001). These devices will perform actions based on the context of their users, and therefore ubiquitous systems will gather, collate and distribute much more personal information about individuals than computers do today (Beresford, 2005).

Each day, every one of us leaves some individually identifiable information behind (as recently highlighted by Channel 4 news in the UK 2009). All the information that is sent and received via mobile phones, Web browsers and other ubiquitous devices are traceable, in such a way that credit or customer loyalty card use leaves residual information about what is consumed by the card owner.

It is generally recognised that the use of ubiquitous computers, networks and intelligent sensors make it possible to record consumers behaviour in more detail. Coupled with the use of sophisticated analysis techniques and their adoption in sectors with sensitive data raise privacy concerns and poses a threat on the safety of the information such as shopping history, internet sites browsed, current location of device etc. collected by these systems. In relation to the first trend, it is important that users are aware of the nature and privacy implications of information they are disclosing when interacting with ubiquitous devices. In order for users to understand these privacy implications it is necessary that designers of these ubiquitous devices and applications endeavour to provide effective privacy protection frameworks within the ubiquitous systems, one that is able to support the intended user straightforward and meaningful way.

Despite many concerns with these ubiquitous issues, there have been little analytical or systematic attempts to enable understanding of the relationship between privacy and the ubiquitous technology. It is obvious that users try to note whenever this system introduces ‘privacy issues’, but with the present lack of analytical tools, users are unable to understand what exactly these issues are (Palen and Dourish, 2003). This research hopes to provide designers of ubiquitous systems a better understanding of what ‘Privacy’ means in relation to the users of the ubiquitous devices and further present recommendations aimed at forming a meaningful privacy protection framework that can be applied during the ubiquitous systems/application design process. This study presents a preliminary investigation into personal privacy issues concerning ubiquitous technology users, their view on privacy and then concludes with suggestions for possible ways of extending the research for further works.

This paper is structured as follows. Section 2 covers some of the characteristics of privacy in general and with respect to ubiquitous systems. Section 3 covers the interview design and Section 4 presents the grounded theory research method deployed in this research and the data collection mechanisms. Section 5 discusses this early research and identifies a number of possible avenues for helping the designer to better support the privacy concerns of the user.

2.0 Privacy in Ubiquitous Systems

2.1 Privacy

The importance of privacy in the conduct of human affairs is rightly significant and is agreed upon by researchers of various disciplines (Grabner-Kräuter and Kaluscha, 2003). However agreement on a suitable definition of the concept is still lacking (Hosmer, 1995; Rousseau et al., 1998; Husted, 1998; Michael, 1994). In the 1890s, future United States Supreme Court Justice Louis Brandeis articulated a concept of privacy that urged that it was the individual's “right to be left alone” (Warren and Brandeis, 1890). According to Bloustein (1964) privacy protects the inviolate personality, independence and an individual's dignity, highlighting the importance of ensuring maximum privacy protection for user’s of ubiquitous devices since most ubiquitous devices handles very sensitive information (typically schedules, movement and even payment) which could be used in an unwanted way to uncover details about a users activity. The Calcutt Committee (1990) said that, nowhere had they found a wholly satisfactory statutory definition of privacy, though were satisfied to implement the following definition legally: “privacy is the right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information”.

The debate on privacy has been a major issue as early as the 19th century, when Samuel Warren and Louis Brandeis (1890, p.193 – 220) wrote a paper titled “The Right to Privacy” which comprehensively explains and analyzes the various rights of users to the protection of their privacy, which was largely motivated by the advent of modern photography and the printing press. Many people nowadays think of privacy more as “the right to select what personal information about me is known to what people” (Westin, 1967). Researchers Goecks and Mynatt (2002) emphasized that privacy is a vital social issue confronting ubiquitous computing and the emerging ubiquitous society today because ubiquitous computing promises a world where computational artifacts embedded in the environment will continuously sense our activities and provide services based on what is sensed (Weiser, 1991). However, such a world presents significant privacy dilemmas (Bellotti and Sellen, 1993; Langheinrich, 2001); for instance, these embedded (ubiquitous) artifacts may collect personal data about users (such as their location, contact details etc.) and transmit this without the user's intentional consent.

One of the most common examples of a ubiquitous device is the mobile phone. Taking off in Europe by mid 1990's, the mobile phone has been universally seen as intruding on the individual's control over time and space as well as redefining public and private time and space (Christian and Jean-Philippe, 2002; R. Ling, 2004;Leysia and Paul, 2003). With the mobile phone, the risk of data getting into the wrong hands is quite high as it possesses simple security mechanism which the users are sometimes ignorant about and privacy frameworks that does not fully explains the implications of the decisions made when operating it. This, among other issues, constitutes a serious privacy risk for users of the ubiquitous systems.

2.2 Privacy Characteristics

Researchers have looked at the interactional, process nature of privacy in human communications and how it should be supported by technology (Palen and Dourish, 2003; Warren and Brandeis 1890). Various approaches which look at privacy from different perspectives were proposed by these researchers, which could be synthesized into the following categories:

- Individual-to-State (the information a government has about her citizens)
- Individual-to-Organizations (what we disclose to different organizations and what we get in return)
- Public (what anybody may know about someone)
- Groups (how we present ourselves to different reference groups).

Since this research is built around the concept of personal privacy it is more focused on privacy related to groups and Individual-to-Organizations, with some linkages to that of the public sectors.

2.3 Ubicomp Privacy

Ubiquitous Computing promises a world where computational artifacts embedded in the environment will continuously sense our activities and provide services based on what is sensed (Weiser, 1991). However, such a world presents significant privacy dilemmas (Bellotti and Sellen, 1993; Langheinrich, 2001); if not addressed, Goecks and Mynatt (2002) suggested these dilemmas have the potential to turn the vision of ubiquitous computing into a world where “Big Brother” is always watching us and personal privacy is near nonexistent. Alan (1967) highlighted that one of the most important aspects of privacy protection is the control of personal information. The goal of personal privacy protection is to empower users with authority over data collected from them by any (ubiquitous) system.

Personal information may take on many forms in the ubiquitous environment. For example, Harrison et al.(1993) illustrated this in media spaces which use audio and video recording devices to capture and share what a user says or is doing. Similarly, Futakawa et al.(1999) explained that some mobile ubiquitous applications are capable of identifying and sharing a user’s location thereby exposing its user to serious privacy risk, should such information fall into the wrong hands. In order to achieve the ultimate vision of the ubiquitous computing world, it is paramount that designers of ubiquitous systems employ a privacy framework when developing and deploying into ubiquitous devices, applications and environments in order to protect the privacy of the users and gain their trust at some level. A preliminary study is undertaken in order to explore the concerns of user in this arena.

3.0 Research Approach

3.1 Interviews

Interview questions were derived from the issues identified from the outcomes of the literature review, it focuses on addressing user’s misunderstanding on the issues of personal privacy concerned with the usage of (their) ubiquitous devices; the research adopted an interview development framework which was previously suggested by Moore (2000). The process was carried out in four stages: a) Purpose of interview established, b) Subject areas to be covered outlined, c) Key interviewees determined and d) the Interview approach identified.

3.2 Interview purpose established

The purpose of the interview was to discover the user's appreciation of security when interacting with ubiquitous devices. Identification of the privacy gaps in relation to the ubiquitous systems with the ultimate objective of uncovering privacy issues, causes of the issue and possible solutions to the issue; as such the following areas are to be addressed by the interview:

- Identify the factors that affect actions taken by users of ubiquitous systems when operating the device
- Identify various protective measures that ubiquitous device users initiate to enable the protection of their privacy
- Identify how the users are expecting the system to function

In achieving its objectives, the interview was divided into two parts the first part seeks understand the interviewee characteristics (such as gender, age group, level of involvement in ubiquitous system usage est.) of the interviewee. The second part of the interview will examine the theoretical areas of vulnerability proposed in the literature review, the analysis of which will assist in the identification of generalized planning and contingency steps.

3.3 Areas of interest

The interview aims to cover various ubiquitous devices based on some general characteristics of ubiquitous systems, these characteristics being: 1) Availability of user interface (Visual and Non-Visual), 2) Mobility and 3) Context awareness. With a diversified selection, it is more likely to uncover specific issues and direct associated solutions. Alternatively, a more specific approach with limited responses about a single ubiquitous device would not provide an opportunity to examine the expansive nature of privacy in this area. Three ubiquitous devices: 1) Mobile phones (Ubiquitous device with UI and mobile), 2) Oyster cards (Ubiquitous devices without UI, but mobile) and 3) Ambient displays for example intelligent advertisement billboard (ubiquitous device that is static, but affected by contextual surroundings).

3.4 Interviewees and Approach

Since these preliminary interviews focus on identifying user opinions on privacy affecting ubiquitous systems, an ideal participant for this interview will be someone who is familiar with the usage of an ubiquitous system such as mobile phones, oyster cards or personal computer; these are the most common example of ubiquitous systems that exhibits characteristics (such as the availability of a visual user interface) that are of interest to the purpose of the research. It is important that the people selected for the interview already posses some experience and have the relevant knowledge on ubiquitous systems operation in order that the data provided would have the required depth. The participants also span through various genders, professions and age groups, this was intentionally done to help the research in achieving a diversified set of responses.

Data was captured during the interview using note-taking and audio-recording equipment; the latter subject to the interviewee's permission some of the participants in the interview were university students, IT professionals, medical workers and other unskilled professions (detailed analysis of participants is found in the next section on data presentation). On approaching a potential participant, there is a brief verbal introduction, and then the research information sheet was first handed to the participant to read through, although some of the participants requested the information sheet be read out to them and this was willingly done by the researcher. Once the participants agrees to continue with the interview the consent form was given to them to tick as appropriate and sign, after this the interview questioning started.

Prior to conducting the interviews a pilot interview took place to allow for adjustments and changes to be made to the interview structure, questions and format before the actual interviews take place.

3.4 Interview summary

It would be beneficial to quickly present a breakdown of the audience that participated in this research in order to relate the various demographics of the participants to the outcome of the research. There were a total of ten interviewees for this research and the constituents of the audience are as follows:

Gender	Participants
Male	6
Female	4

Table 1a: Gender of participants

Age Group	Participants
18 – 24	6
25 – 35	2
36- 45	1
Over 45	1

Table 1b: Age groups of participants

In order to have a clearer understanding of the content of the interview and how it relates to the actual purpose intended, a brief segmentation of the interview questions and their relationship to the research subject is presented in the following table:

Areas covered	Questions
Background	1) Age 2) Gender 3) Make and model of mobile phone 4) Do you use an oyster card or club card?
Ubiquitous device usage profile	5) Please select activities you carry out using your mobile phone • Mobile Internet • SMS • Keypad lock • Alarm / Scheduler • Address book • Bluetooth • Music player • Email • Instant messaging • Alert profiles 6) Which of the following activities that you carry out on your computer can you also perform on your mobile phone? • Checking email • Apple ITunes shopping • Amazon/Ebay shopping • Watching videos • Social networking • News websites • Using other web services
Perceptions to privacy on	7) How do you protect your personal information (such as contacts, text messages and pictures if applicable) from being accessed by people you do not

ubiquitous device	want to show? 8) Do you make payments using your credit card/debit card through the mobile phone? Why? What are the factors the influences your decision? 9) Do you protect your voicemail with a password or PIN no? Why? What are the factors the influences your decision? 10) What action do you take when you do not wish to receive mobile phone calls? Why? What are the factors the influences your decision? 11) Did you register your oyster card/shopping club cards with your correct personal information? Why/Why not? 12) How often do you check your journey details/shopping activities on your oyster/shopping club cards? What are the reasons for this?
Perception to privacy in ubiquitous location	13) Would you be comfortable viewing your email, dairy on large display screens in a public place? Why/Why not?

Table 2: Interview Structure

4. Data Analysis – Grounded Theory

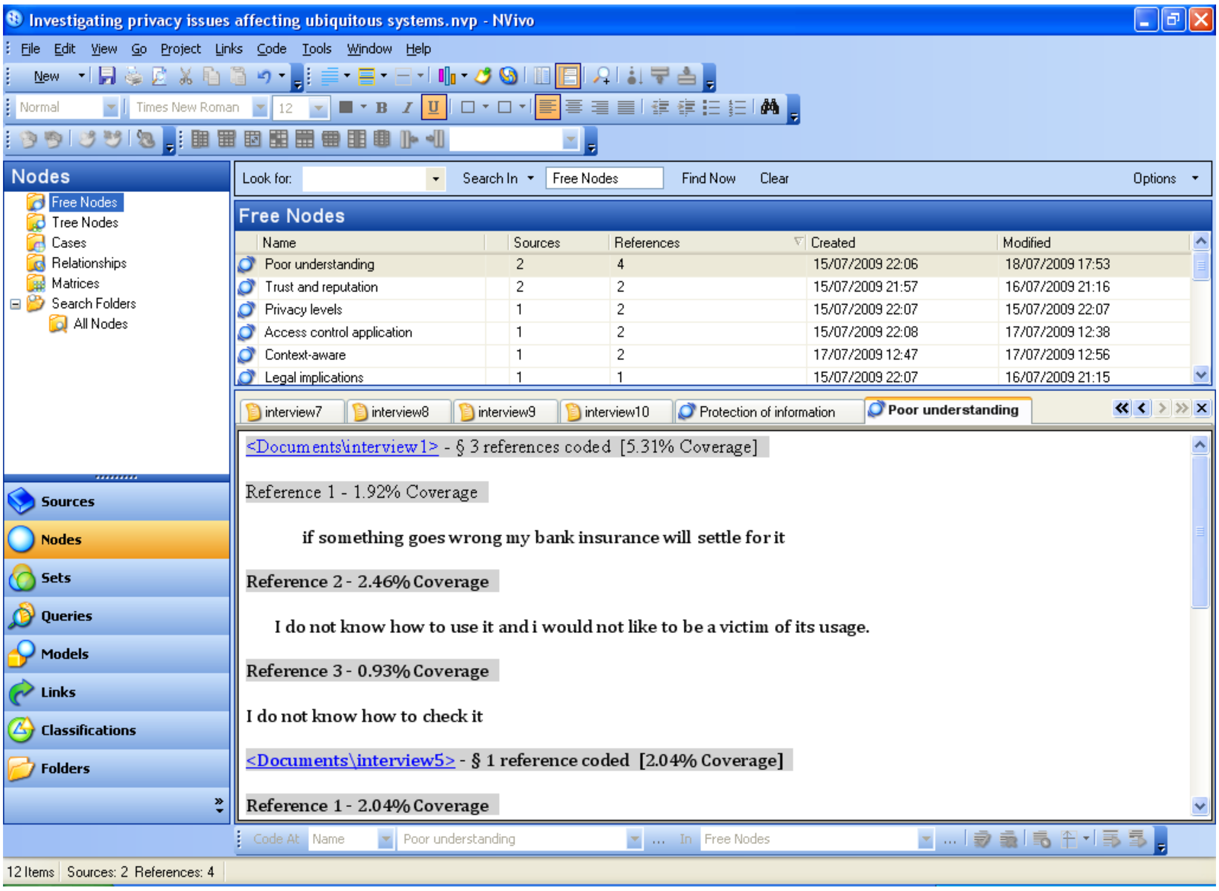
A qualitative data analysis methodology was used for this research - grounded theory. This framework was chosen because of the open nature of the research (with no initial hypothesis), its applicability to the data being collected and its popularity in qualitative research (Bryman and Bell, 2007). Grounded theory provides a framework allowing the researcher to systematically categorize transcribed qualitative data, using a coding system that allows for identification of themes within the data (Easterby-smith, Thorpe and Jackson, 2008). Traditional research designs usually rely on a literature review leading to the formation of a hypothesis. This hypothesis is then put to the test by experimentation in the real world. On the other hand, grounded theory investigates the actualities in the real world and analyses the data with no preconceived hypothesis (Glaser and Strauss, 1967).

4.1 Grounded Theory Analysis Process

For the purpose of clarity, a brief overview of the tasks carried out from data collection to analysis of research data using grounded theory is provided (Table 3):

Task	Task details
Data Collection	Record the interview with each participant.
Transcription	Transcribe each completed interview into electronic format (Using Microsoft word) in preparation for analysis
Creation of Nvivo project	Create new Nvivo project and import the transcribed documents into the new project in Nvivo
Analysis in Nvivo	All imported documents where opened in Nvivo, Codes and concepts where identified using the micro-coding technique of the grounded theory (See Figure 1 below).
Coding	Where a code appears more than once it is added to the already existing node and this increases the “References” to that node (represented as frequency during presentation) and similar codes where groups together into a new concept.
Categorization	Concepts with similar top-level attributes were classified into same category, thus identification of categories.
Summary and result export	Summary of the results was exported back to a tabular format in Microsoft word (See table 4.2)

Table 3: Research Steps



Free Nodes

Name	Sources	References	Created	Modified
Poor understanding	2	4	15/07/2009 22:06	18/07/2009 17:53
Trust and reputation	2	2	15/07/2009 21:57	16/07/2009 21:16
Privacy levels	1	2	15/07/2009 22:07	15/07/2009 22:07
Access control application	1	2	15/07/2009 22:08	17/07/2009 12:38
Context-aware	1	2	17/07/2009 12:47	17/07/2009 12:56
Legal implications	1	1	15/07/2009 22:07	16/07/2009 21:15

<Documents\interview1> - § 3 references coded [5.31% Coverage]

Reference 1 - 1.92% Coverage

if something goes wrong my bank insurance will settle for it

Reference 2 - 2.46% Coverage

I do not know how to use it and i would not like to be a victim of its usage.

Reference 3 - 0.93% Coverage

I do not know how to check it

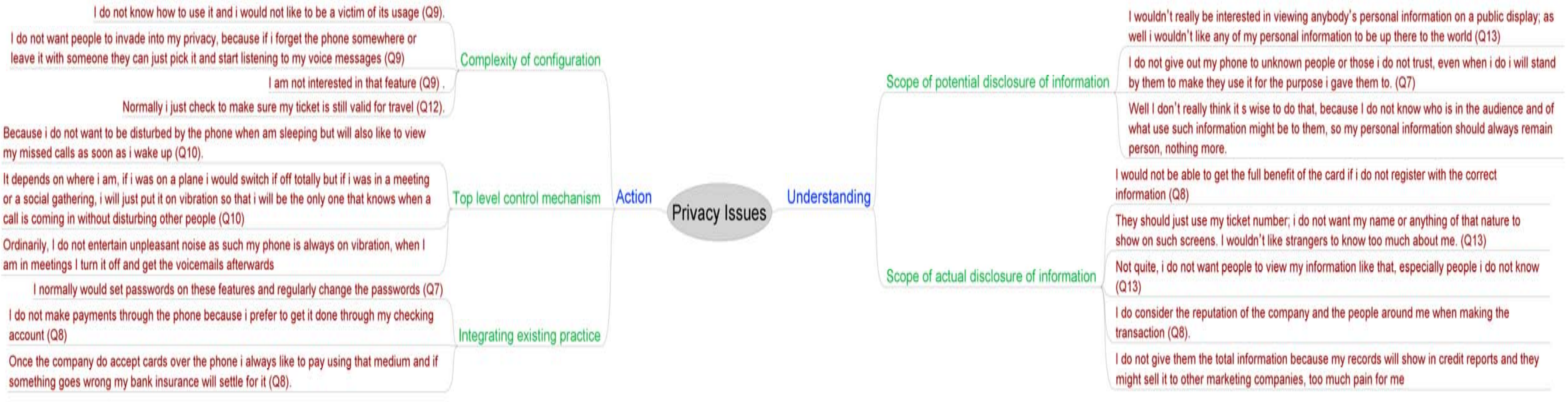
<Documents\interview5> - § 1 reference coded [2.04% Coverage]

Reference 1 - 2.04% Coverage

Figure 1: Screenshot showing the process of coding Nvivo

When analyzing the interview data, each of the completed interviews were first recorded then transcribed into electronic format using Microsoft word 2007 because this format made it easier to work flexibly with the actual interview data during the actual analysis process. The electronic transcripts were then put through a coding process, this involved the identification, breakdown, and comparison of key concepts common in the interview data collected until clearly defined patterns are formed which gives an insight into understanding the research question (Strauss and Corbin, 1998), to assist with the coding and analysis the use of a computer aided qualitative data analysis software tool (CAQDAS) called NVivo was adopted.

NVivo assists in speeding up the often cumbersome task associated with coding and retrieving large amounts of data by providing a global view of the transcribed documents making it easy to go back and forth within the transcripts. The coding was done using the micro-analysis coding method of the grounded theory; meaning each interview response in the transcript was critically scrutinized such that more than one code could emerge from the same data (Allan, 2003). A concept map relating the identified concepts to the raw data collected from the interview was created in order to demonstrate the relationship of the analysis output to the raw data collected from the interviews, this would also give a sense of wholesome understanding about the how the codes were created and how it relates to the various research areas.


Privacy Issues
Action
Complexity of configuration
Top level control mechanism
Integrating existing practice
Understanding
Scope of potential disclosure of information
Scope of actual disclosure of information

I do not know how to use it and i would not like to be a victim of its usage (Q9).

I do not want people to invade into my privacy, because if i forget the phone somewhere or leave it with someone they can just pick it and start listening to my voice messages (Q9)

I am not interested in that feature (Q9) .

Normally i just check to make sure my ticket is still valid for travel (Q12).

Because i do not want to be disturbed by the phone when am sleeping but will also like to view my missed calls as soon as i wake up (Q10).

It depends on where i am, if i was on a plane i would switch if off totally but if i was in a meeting or a social gathering, i will just put it on vibration so that i will be the only one that knows when a call is coming in without disturbing other people (Q10)

Ordinarily, I do not entertain unpleasant noise as such my phone is always on vibration, when I am in meetings I turn it off and get the voicemails afterwards

I normally would set passwords on these features and regularly change the passwords (Q7)

I do not make payments through the phone because i prefer to get it done through my checking account (Q8)

Once the company do accept cards over the phone i always like to pay using that medium and if something goes wrong my bank insurance will settle for it (Q8).

I wouldn't really be interested in viewing anybody's personal information on a public display; as well i wouldn't like any of my personal information to be up there to the world (Q13)

I do not give out my phone to unknown people or those i do not trust, even when i do i will stand by them to make they use it for the purpose i gave them to. (Q7)

Well I don't really think it s wise to do that, because I do not know who is in the audience and of what use such information might be to them, so my personal information should always remain person, nothing more.

I would not be able to get the full benefit of the card if i do not register with the correct information (Q8)

They should just use my ticket number; i do not want my name or anything of that nature to show on such screens. I wouldn't like strangers to know too much about me. (Q13)

Not quite, i do not want people to view my information like that, especially people i do not know (Q13)

I do consider the reputation of the company and the people around me when making the transaction (Q8).

I do not give them the total information because my records will show in credit reports and they might sell it to other marketing companies, too much pain for me

Figure 2: A Concept map that links discovered concepts to the interview responses

5.0 Discussion

The research presented in this paper is still at an early stage. The five concerns identified can be classified under two major categories which are those that primarily affect users' understanding of a system's privacy implications and those that primarily affect their ability to conduct meaningful action through the system.

Understanding	Action
Scope of potential disclosure of information	Top level control mechanism
Scope of actual disclosure of information	Complexity of configuration
	Integration of existing practice

Table 3: Privacy Concerns

Each concern is now detailed, with suggestions of how designers of ubiquitous systems could overcome them with examples of applications in real life.

5.1 Concern DI: Scope of Potential Disclosure of Information

Users might sometimes have difficulty appropriating a system into their privacy practice if the scope of its privacy implications is not explicitly clear. This scope includes the types of information the system conveys, the kinds of observers it conveys to, the media through which it is conveyed, the length of retention, the potential for unintentional disclosure, the presence of third-party observers, and the collection of Meta information. Clarifying a system's potential for conveying personal information is vital to users' ability to predict the social consequences of its use. Among the conveyable information types are identifiable personae (e.g., true names, login names, email addresses, credit card numbers) and monitorable activities (broadly, any of the user's interpretable actions and/or the contexts in which they are performed, e.g., locations, purchases, social relations, correspondences, audio/video records). Boyd (2002) revealed that this dichotomy of personae and activities, though imperfect and coarse, can be useful shorthand for conceptualizing a user's identity space, with personae serving as indices to dynamically intersecting subspaces and activities serving as the contents of those subspaces.

5.1.1 Research Evidence: Scope of Potential Disclosure of Information

One of the easiest ways that ubiquitous system designers obscure a system's privacy scope is by presenting certain functions ambiguously. An obvious example of this flaw is the power off button available on most mobile phone devices. Sometimes when mobile phone users want to switch their mobile phone off they simply apply the "power off" button in anticipation of completely powering down the entire device. The field study revealed that about 70% of ubiquitous device users switch off their devices in anticipation of avoiding alerts and disturbances (7 out of the 10 respondents to the interview demonstrated this in their responses). This is evident in one of the responses by the users quoted below:

> *"Ordinarily, I do not entertain unpleasant noise as such my phone is always on vibration, when I am in meetings I turn it off and get the voicemails afterwards" (Appendix 10, Question 10b)*

However completely switching off a mobile phone from the power button might not completely disable the device in some situations, as certain utilities such as the alarm and scheduler still continue to run even when the phone is powered down. If an alarm had been previously set on the mobile device, at the scheduled time the alarm would still go off and could create some unsolicited alert and possibly pass a lot of information about the user (such as been at an appointment at the time the alarm went off) to the people around; this is totally unintended as the mobile phone user would have assume to have completely turned off the device.

A similar example of this flaw was illustrated in Beckwith's (2003) report of an eldercare facility that uses worn transponder badges to monitor the locations of residents and staff (Beckwith, 2003). Many residents perceived the badge only as a call-button (which it was) but not as a persistent location tracker (which it also was). They did not understand the disclosures it was capable of facilitating. In another similar piece of research by Reang, he reveals that some hospitals use badges to track the location of nurses for efficiency and accountability purposes but neglect to clarify what kind of information the system conveys. Erroneously thinking the device was also a microphone, one concerned nurse wrote, "They've placed it in the nurses' lounge and kitchen. Somebody can click it on and listen to the conversation. You don't need a Big Brother overlooking your shoulder” (Reang, 2002).

5.1.2 Proposed Solution: Scope of Potential Disclosure of Information

Ubiquitous systems should provide clear indications of the scope and limitations of actions carried out on the system, for instance providing an easy option for user to completely “power down” their mobile phones including all applications (such as alarm and scheduler) while switching off their phones will help them realize how their actions has actually affected the potential scope of information flow on the mobile phone. More so, many web sites that require an email address for creating an account should give clear notice on their sign-up forms that they do not share email addresses with third parties or use them for extraneous communication with the user. Clear, concise statements like these help clarify scope, and they are becoming more common, as well as being demanded by law in certain circumstances by the information commissioner’s office (http://www.ico.gov.uk, 2009).

5.2 Concern AD: Scope of Actual Disclosure of Information

Having highlighted the user’s need to understand a system’s potential privacy implications, the next level is the instances of actual disclosure of personal information. To whatever degree is reasonable, designers should make clear the actual disclosure of information through the system. Users should understand which of their information is being conveyed to whom and for what purpose. The disclosure should be obvious to the user as it occurs; if this is impractical, notice should be provided within a reasonable delay. Feedback should sufficiently inform but not overwhelm the user. This can help users understand the consequences of their use of the system thus far and predict the consequences of future use.

5.2.1 Research Evidence: Scope of Actual Disclosure of Information

During the interviews, some of the participants indicated their willingness to divulge their financial information over phone only if the company has a reputable public image and accept payment over the phone, an interviewee response is quoted as follows:

> *"Once the company do accept cards over the phone I always like to pay using that medium and if something goes wrong my bank insurance will settle for it"*

Around 50% of ubiquitous device users who showed their willingness to divulge their financial information vocally over their mobile devices (5 out of the 10 respondents to the interview demonstrated this in their responses). Although the motive of payment itself might be justified however; it is at sometimes done without the consideration of those who are around the user that may be acquire the information being conversed thereby compromising the information being transferred. In another similar work, Felten et. al (2001) illustrated an example of this in web browser support for cookies. Most browsers do not, by default, indicate when a site sets a cookie or what information is disclosed through its use. The prevalence of third-party cookies and web bugs (tiny web page images that facilitate tracking) exacerbates users' ignorance of who is observing their browsing activities. Beckwith (2003) yet again illustrated this in the locator badges which generally do not inform their wearers about who is locating them.

5.2.2 Proposed Solution: Scope of Actual Disclosure of Information

Mobile phone payment systems should be designed in such a way that coarse information are required from end users when requesting for sensitive information such as passwords and memorable information, for instance it could just require some random characters from the memorable information instead of the entire word, when complete information such as credit card number are required users should only be allowed to enter it using their phone keypad instead of reading it out, assuming they are not alone. Friedman et al's (2002) redesign of cookie management reveals what information is disclosed to whom. They extended the Mozilla web browser to provide prominent visual feedback about the real-time placement and characteristics of cookies, thereby showing users what information is being disclosed to what web sites (Friedman et al., 2002).

5.3 Concern TOP: Top Level Control Mechanism

Designers should offer an obvious, top-level mechanism for halting and resuming the transmission of information in ubiquitous systems. Users are accustomed to turning a device off when they want its operation to stop. Often a single power button or exit button will do the trick. Beyond binary control, a simple ordinal control may also be appropriate in some cases (such as audio devices' volume and mute controls). In the general case, users can become remarkably adept at wielding coarse grained controls to yield nuanced results (*e.g.*, driving a car requires use of a wheel, a stick, and two or three pedals, but their manipulation yields tremendous results). Plus, coarse-grained controls often reflect their state, providing direct feedback and freeing the user from having to remember whether she set a preference properly. This helps users accommodate the controls and even co-opt them in ways the designer may not have intended. Examples specific to privacy include: setting a door ajar, covering up or repositioning cameras (Janke et. al, 2001), turning off a phone or using its invisible mode rather than navigating its privacy-related options, and removing a worn locator badge. While some fine-grained controls may be unavoidable, the flexibility they are intended to provide is often lost to their neglect, which is then compensated for by the nuanced manipulation of coarse-grained controls across devices, applications, and time.

5.3.1 Research Evidence: Top Level Control Mechanism

Most users take the "switch off" button on devices literally and when they intend achieve this through the easiest possible means they can. One of the interviewees asserted that:

> *"Mainly because when i do not want to receive calls, I do not want disturbance, I just switch it off. "*

Almost all users of ubiquitous devices use one form of top level switching mechanism such as mute, turn off and profiling functions on their ubiquitous devices (all of the 10 respondents to the interview demonstrated this fact in their responses). This reflects the user's intension to completely disable their devices through the switch off button, however this might not be the situation in some cases as to whereby the switch off button is not been placed somewhere it can be quickly accessed or some devices that just do not switch off completely even when its visual display has been turned off. Similarly, most web browsers still bury their privacy controls under two or three layers of configuration panels (Felten et. al, 2001). While excessive configuration may itself be a problem, the issue here is that there is typically no top-level control for switching between one's normal cookie policy and a "block all cookies" policy.

In another similar research, wearable locator-badges like those described in (Harper et. al, 1992) and (Beckwith, 2003) do not have power buttons. One could remove the badge and leave it somewhere else, but simply turning it off would at times be more practical or preferable.

5.3.2 Proposed Solution: Top Level Control Mechanism

Systems that expose simple, obvious ways of halting and resuming disclosure include easily coverable cameras (Sellen and Bellotti, 1993), mobile phones with obvious power buttons, instant messaging systems with invisible modes and stealth controls (Abowd et. al, 2001). Designers should learn to adopt obvious top level controls and buttons such as these ones at locations that are easy to find in the ubiquitous device.

5.4 Concern IP: Integration of Existing Practice

Designers should be aware of inhibiting existing social practice. People manage privacy through a range of established, often nuanced, practices. While early designs might lack elegant support for emergent practices—since, obviously, substantive practice cannot evolve around a system until after deployment—designers can at least take care to avoid inhibiting established ones. This is effectively a call to employ privacy design patterns. In particular, it is important to emphasize the broad applicability of plausible deniability (whereby the potential observer cannot determine whether a lack of disclosure was intentional) (Woodruff and Aoki, 2003; Nardi et al., 2000) and disclosing ambiguous information (*e.g.*, pseudonyms, imprecise location).

These common, broadly applicable techniques allow people to finesse disclosure through technical systems to achieve nuanced social ends. Systems that rigidly contradict meta-practices like plausible deniability and ambiguous disclosure may encounter significant resistance during deployment (Suchman, 1997). Technical systems are notoriously awkward at supporting social nuance (Ackerman, 2004). Interestingly, however, systems that survive long enough in the field often contribute to the emergence of new practice even if they suffer from socially awkward design in the first place (*e.g.*, see [Wakeford et. al, 2001, Boyd, 2004]). In other words, emergent nuance happens. But being intrinsically difficult to predict, seed, and design for, it generally doesn't happen as optimally as we might like it to. Designers will continue to struggle to support these emergent practices, but by identifying existing genres of disclosure and successful privacy design patterns, they can at least help users transfer established skills to new technologies and domains.

5.4.1 Research Evidence: Integration of Existing Practice

Some mobile phone users simply do not bother about chosen a secured personal identification number (PIN) for their voicemails, simply because they dim the process not too suitable for their usage, as it reflects a huge learning curve for the users. One of the responders gave reason for not using the PIN service as:

> *"I do not know how to use it and I would not like to be a victim of its usage."*

About 80% of ubiquitous device users will not interact with distinctively new features that have not been effectively bonded to the existing operational culture they are used to (8 out of the 10 respondents to the interview demonstrated their unwillingness to protect their voicemails due to insufficient understanding of how the protection system functions, in their responses). Some researchers envision context-aware mobile phones that disclose the user's activity to the caller to help explain why their call was not answered (Wong et. al, 2003). However, this prohibits users from exploiting plausible deniability. There can be value in keeping the caller ignorant of the reason for not answering. Location-tracking systems like those described by Newman et. Al. (1992) and Beckwith (2003) constrain users' ability to incorporate ambiguity into their location disclosures. Users can only convey their concise location or—when permitted—nothing at all.

5.4.2 Proposed Solution: Integration of Existing Practice

Mobile phones, push-to-talk phones (Aoki and Woodruff, 2003), and instant messaging systems (Bradner et. al, 2000) let users exploit plausible deniability by not responding to hails and not having to explain why. Although privacy on the web is a common concern, a basic function of HTML allows users to practice ambiguous disclosure. Forms that let users enter false data facilitate anonymous account creation and service provision.

5.5 Concern CC: Complexity of Configuration

Designs should not require excessive configuration to create and maintain privacy. They should enable users to practice privacy management as a natural consequence of their ordinary use of the system. Palen and Dourish (2003) argued that standardising on explicit parameters and requiring people to live by them simply does not work, and yet this is often what information technology requires… Instead, a fine and shifting line between privacy and publicity exists, and is dependent on social context, intention, and the fine-grained coordination between action and the disclosure of that action". But because configuration has become a universal user interface design pattern, many systems fall for this configuration flaw. Configured privacy breaks down for at least two reasons.

First, in real settings users manage privacy semi-intuitively; they do not spell out their privacy needs in an auxiliary, focused effort (Whitten and Tygar, 1999). Configuration imposes an awkward requirement on users, one they will often forsake in favour of default settings (Adams, 2000; Beckwith, 2003). If users are to manage their privacy at all, it needs to be done in an intuitive fashion, as a predictable outcome of their situated actions involving the system. People generally do not set out to explicitly protect their privacy. Rather, they participate in some activity, with privacy regulation being an embedded component of that activity. Designs should take care not to extract the privacy regulation process from the activity within which it is normally conducted.

5.5.1 Research Evidence: Integration of Existing Practice

Some mobile ubiquitous devices provide frustrating processes in the configuration of privacy and this affects and discourages users to use them. About 70% of ubiquitous device users will not check their emails or buy items from the internet on their mobile devices because of the complexity of the interaction interface made available for this process. (7 out of the 10 respondents to the interview demonstrated their unwillingness to protect their voicemails due to insufficient understanding of how the protection system functions, in their responses). One of the responses was quoted thus:

"I do not know how to use it and I would not like to be a victim of its usage."

5.5.2 Proposed Solution: Complexity of Configuration

When someone is aware of a camera's presence, they tend to adjust their behaviour to present alignment with the perceived expectations of their ostensible observers (Foucault, 1977). They do not step outside to reconfigure their representation. They simply act, albeit with "appropriate" intuition and/or intention. Cadiz and Gupta (2001) proposed a smart card that one could hand to a receptionist to grant him limited access to one's calendar to schedule an appointment; he would hand it back right afterwards without much hassle of searches and configuration and no one would have to fumble with setting permissions (Cadiz and Gupta, 2001). Similar practices were proposed by Cadiz and Gupta (2001) above could be integrated into the design of new ubiquitous systems to simplify the processes involved in carrying out operations on ubiquitous systems. Two identified categories of concern are those that primarily affect users' understanding of a system's privacy implications and those that primarily affect their ability to conduct meaningful action through the system.

6.0 Conclusion

This paper reports on a preliminary study that uncovers privacy concerns associated with everyday digital interaction with recognised devices (termed Ubiquitous devices as they play an active part in our everyday lives). The focus on devices used in our everyday lives allows the research to investigate privacy in a ubiquitous world, moving the lens from a single device to everyday activities on a range of devices. Ten interviews are carried out and the transcribed data is analysed using grounded theory to code the responses into a number of categories. The categories are brought together (with literature) to form a design framework that aims to support the designer of ubiquitous applications or ubiquitous information systems. Two major categories are found – those that affect user understanding of a system’s privacy implications and those that primarily affect their ability to conduct meaningful action through the system.

References

Ackerman, M. S. (2004). *Privacy in pervasive environments: next generation labeling protocols*. Personal Ubiquitous Comput. 8, 6 (Nov. 2004)

Adams A (2000). *Multimedia Information Changes the Whole Privacy Ballgame.* Proceedings of the Conference on Computers, Freedom, and Privacy (CFP 2000), ACM Press, Toronto, Ontario, Canada, pp 25-32.

Alan F. Westin (1967). Privacy and Freedom. Atheneum, New York NY.

Allan G. (2003). *A critique of using grounded theory as a research method*. Department of Information Systems and Computer Applications, Portsmouth University, UK

Beckwith R. (2003). *Designing for Ubiquity: The Perception of Privacy*. IEEE Pervasive 2(2):40-46.

Bellotti V. and Sellen A. (1993). *Design for Privacy in Ubiquitous Computing environments*. Proceedings of ECSCW ’93, Milan, Italy, p. 77-92.

Bloustein, E. (1964) Privacy as an Aspect of Human Dignity, 39 New York University Law Review 971`.

Boyd d (2002). Faceted Id/Entity: Managing representation in a digital world (M.S. Thesis). Massachusetts Institute of Technology, Cambridge, MA, USA.

Boyd d (2004). *Friendster and Publicly Articulated Social Networks*. Extended Abstracts of the Conference on Human Factors in Computing Systems, ACM Press, Vienna, Austria, in press.

Bryman, A. and Bell, E. (2007). Business research methods, 2nd Edition, Oxford University press Inc., New York.

Cadiz J and Gupta A (2001) *Privacy Interfaces for Collaboration*, Technical Report MSR-TR-2001-82. Microsoft Corp., Redmond, WA, USA.

Calcutt QC, D. (1990) *Report of the Committee on Privacy and Related Matters,* Cmnd. 1102, London: HMSO

Channel4 News (2009). Privacy warning over mobile phones. Available online at http://www.channel4.com/news/articles/science_technology/privacy+warning+over+mobile+phones/3149777 [accessed 02/09/09]

Christian Licoppe and Jean-Philippe Heurtin (2002). *France: preserving the image*. In J. Katz and M. Aakhus, editors, Perpetual Contact: Mobile communication, private talk, public performance, pages 94–109. Cambridge University Press, Cambridge, MA.

Corbin, J and Strauss, A. (1996). *Analytic Ordering for Theoretical Purposes*. Qualitative inquiry, Vol. 2 (2), pp. 139-150.

Dey AK, Salber D and Abowd GD (2001). *A Conceptual Framework and a Toolkit for Supporting the Rapid Prototyping of Context-Aware Applications*. Human-Computer Interaction 16(2-4):97-166.

Dey, A., Futakawa, M., Salber, D., and Abowd, G (1999). *The Conference Assistant: Combining Context-Awareness with Wearable Computing*. Proceedings of the 3rd International Symposium on Wearable Computers, San Francisco, CA,

1999. p. 21-28.

Easterby-smith, M., Thorpe, R., and Jackson, P. (2008) Management research‘, 3rd Edition, Sage publications Inc, London

Foucault M (1977). Discipline and Punish. Vintage Books, New York, NY, USA.

Friedman B, Howe DC and Felten EW (2002). *Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design*. Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS 02), Hawaii, USA.

Glaser, B.G. and Strauss, A.L. (1967) The Discovery of Grounded Theory, New York, Aldine

Grabner-Kräuter, S. and Kaluscha E. A. (2003). *Empirical research in on-line trust: a review and critical assessment*, International Journal of Human-Computer Studies, 58 (6), pp 783 – 812

Green N, Lachoee H and Wakeford N (2001). *Rethinking Queer Communications: Mobile Phones and beyond. Proceedings of the Sexualities*, Medias and Technologies Conference, University of Surrey, Guildford, UK.

Harper RHR, Lamming MG and Newman WH (1992). *Locating Systems at Work: Implications for the Development of Active Badge Applications*. Interacting with Computers 4(3):343-363.

Harrison, S., Bly, S., Anderson, S., and Minneman, S. *The Media Space* In K.E. Finn, A. J. Sellen, and S.B. Wilbur (eds.) (1993). Video-Mediated Communication. Lawrence Erlbaum Associates, NJ, 1993, p. 273-300.

Hosmer, L.T. (1995). *Trust: the connecting link between organizational theory and philosophical ethics*. Academy of Management Review, 20 (2) pp. 379–403

Husted, B.W. (1998). The ethical limits of trust in business relations. Business Ethics Quarterly, 8 (2) pp. 233–248

Information commisioner’s office ICO (2009), know your rights. Available online at http://www.ico.gov.uk/what_we_cover/privacy_and_electronic_communications/your_rights.aspx [Accessed 02/09/09]

Jancke G, Venolia GD, Grudin J, Cadiz J.J. and Gupta A. (2001). *Linking public spaces: technical and social issues*. Proceedings of the Conference on Human Factors in Computing Systems (CHI 01), ACM Press, Seattle, WA, USA, pp 530-537

Jeremy Goecks and Elizabeth Mynatt (2002), *Enabling Privacy Management in Ubiquitous Computing Environments through Trust and Reputation Systems*, College of Computing, Georgia Tech.

Langheinrich M (2001). *Privacy by Design – Principles of Privacy Aware Ubiquitous Systems*. Proceedings of Ubicomp 2001, Atlanta, GA, p. 273-291.

Lawrence Lessig (1999). Code and other laws of cyberspace, Basic Books, New York NY.

Michael, J. (1994). *Privacy and Human Rights*. The International and Comparative Law Quarterly, 44 (4).

Millett L.I., Friedman B and Felten E (2001). *Cookies and Web browser design: toward realizing informed consent online*. Proceedings of the Conference on Human Factors in Computing Systems (CHI 2001), ACM Press, Seattle, WA, USA, pp 46-52.

Moore, N. (2000). How to do research. Third edition. Library Association publishing

Nardi BA, Whittaker S and Bradner E (2000). *Interaction and Outeraction: Instant Messaging in Action*. Proceedings of the Conference on Computer Supported Cooperative Work (CSCW 00), ACM Press, New York, NY, USA, pp 79-88.

Palen L. and Dourish P. (2003). *Unpacking “privacy” for a networked world*. In CHI ’03: Proceedings of the SIGCHI conference on Human factors in computing systems, pages 129–136, New York, NY, USA, ACM Press.

R. Ling (2004). The Mobile Connection: The Cell Phones Impact on Society. Morgan Kaufmann.

Reang P (2002). Dozens of nurses in Castro Valley balk at wearing locators. Mercury News, San Jose, CA, Sept. 6, 2002.

Rousseau, D.M., Sitkin, S.B., Butt, R.S. and Camerer, C. (1998). *Not so different after all: a cross-discipline view of trust*. Academy of Management Review, 23 (3) pp. 393–404

Suchman L (1997). Do Categories have Politics? The language/action perspective reconsidered. In Friedman B (eds). Human Values and the Design of Computer Technology, Center for the Study of Language and Information, Stanford, CA, USA, pp 91-106.

Warren S. and Brandeis L. (1890). *The right to privacy*. Harvard Law Review, 4:193 – 220.

Weiser M. (1993). *Some computer science issues in ubiquitous computing*, Communications of the ACM, 36(7) 75-84

Weiser M. (1995), *The PARCTab Ubiquitous Computing Experiment*, technical report CSL-95-1, XEROX Palo Alto Research Center.

Weiser, M. (1991). *The Computer for the Twenty-first Century*. Scientific American, 265, 3 (September 1991), p. 94-104.

Whitten A and Tygar JD (1999). *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*. Proceedings of the 8th USENIX Security Symposium, Washington, DC, USA.

Woodruff A and Aoki PM (2003). *How Push-to-Talk Makes Talk Less Pushy*. Proceedings of the International Conference on Supporting Group Work (GROUP 03), ACM Press, Sanibel Island, FL, USA, pp 170-179.