Configurable Dynamic Privacy for Pervasive Sensor Networks

by

Nan-Wei Gong

Submitted to the Program in Media Arts and Sciences,
School of Architecture and Planning,
in partial fulfillment of the requirements for the degree of

Master of Science in Media Arts and Sciences

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

August 2009

Author____

Program in Media Arts and Sciences
August 7, 2009

Certified by____

Joseph A. Paradiso
Associate Professor of Media Arts and Sciences
MIT Media Laboratory
Thesis Supervisor

Accepted by____

Deb Roy
Chair, Department Committee on Graduate Students
Program in Media Arts and Sciences
MIT Media Laboratory

Configurable Dynamic Privacy for Pervasive Sensor Networks

by

Nan-Wei Gong

Submitted to the Program in Media Arts and Sciences,
School of Architecture and Planning,
on August 7th, in partial fulfillment of the
requirements for the degree of
Master of Science in Media Arts and Sciences

Abstract

Ubiquitous computing sensor networks have greatly augmented the functionality of interactive media systems by adding the ability to capture and store activity-related information. Analyzing the information recorded from pervasive sensor networks can provide insight about human behavior for better personalized system services, as well as richer media content and social communication. With these increased capabilities, serious concerns which create obstacles to the deployment of such networks are raised with regard to privacy and boundaries. However, there currently exists no real data about privacy in pervasive media networks and most studies that have been made so far are speculative. This thesis presents the design and implementation of a configurable infrastructure that can protect users' dynamic levels of privacy in a pervasive sensor network. Through an active badge system, users have different options to disable each type of data transmission and collection. This work evaluates approaches for privacy protection through conducting an extensive user study in an actual ubiquitous invasive sensing environment to obtain feedback via sensor system data and questionnaires and correlates that information for future reference in the design of privacy-protected ubiquitous sensor networks. Results from the user study indicate that an active badge for on-site control, especially periodically broadcast RF beacon for privacy control, is the most effective and acceptable method. It also suggested that if every occupant in the building used this approach to constantly block all data transmission, significant system blinding (on the order of 30 % or more) would be incurred. These results allow a better understanding of what value is assessed to privacy versus capabilities/awareness beyond the current assumptions.

Thesis Supervisor: Joseph A. Paradiso
Title: Associate Professor of Media Arts and Sciences, MIT Media Lab

Configurable Dynamic Privacy for Pervasive Sensor Networks

by

Nan-Wei Gong

The following people served as readers for this thesis:

Thesis Reader____

Deb Roy
Associate Professor of Media Arts and Sciences
Program in Media Arts and Sciences

Thesis Reader____

Alex (Sandy) Pentland
Toshiba Professor of Media Arts and Sciences
Program in Media Arts and Sciences

Acknowledgments

I would like to thank Professor Joe Paradiso for giving me the chance to work with him and being the best advisor that anyone could ever hope for. Coming to the Media Lab for my graduate study was a life-changing decision and I could have never done it without the support from Professors Samuel C.C. Ting and Peter Fisher. Also, I would like to thank my thesis readers, Professors Alex (Sandy) Pentland and Deb Roy for their constructive feedbacks during my thesis writing process.

I would like to thank everyone in the Responsive Environments Group. Without them, I could not have completed this project.

To Mat Laibowitz: for teaching me literally everything I know and providing extermly valuable advice on my projects and life.

To Bo Morgan: for helping with coding and being the best user study subject on this planet.

To Mark Feldmeier: for offering his generous help on everyone's electronics project.

To Michael Lapinski: for always explaining things in a way that I can understand.

To Manas Mittal: for his patience in answering all my ridiculous questions.

To Behram Mistree: for the great inspiration and knowledge he provided on my thesis topic.

To Alex Reben: for being a great officemate and slapping my troubles away.

To Matt Aldrich: for fixing CargoNet.

To everyone who has participated in my user study: for wearing a blinking gizmo avidly.

To Lisa Lieberson: for being always helpful and supportive.

To Pamela Siska: for working with me on my writing.

To Linda Peterson and Aaron Solle: for their support and timely reminders.

I would also like to thank all my friends for their help and support along the way especially

To Amit Zoran: for always making things perfect.

To Dori Lin: for being my debugger and always showing up magically when I stumbled.

To Cati Vaucelle: for giving me great advice and insight.

To Chiu-Yen, Yu Chen, Liang-Yi, Flora, Aithne, Wu-Hsi, Anna, Annina, Quinn, Ana, Andrea, Santiago, Wei, Noah, Dale: for being great friends.

To Chia-Wei Lin: for always being caring and understanding.

Finally, I would like to thank my family for all the support and love.

Table of Contents

List of Figures and Tables

Chapter 1

Introduction

Whenever a conflict arises between privacy and accountability, people demand the former for themselves and the latter for everybody else. *–David Brin*

We live in a world where advanced technology has made the production of extremely cheap, small yet powerful wireless sensor networks possible. The clusters of this electronic nervous system, unlike security surveillance systems on the street, have begun to invade our dwellings under the guise of household appliances and communication/media interaction devices. With the great capability of capturing high quality video and audio plus the current facial recognition technology, we might soon be living in the Orwellian nightmare without knowing it [1]. As researchers develop smarter, faster and more complex ubiquitous computing sensor networks, privacy issues are still yet to be solved. It will only become worse as invasive media capture eventually becomes an intrinsic property of devices scattered all over our environments.

In this research, we have constructed a system that allows users to control and configure their privacy within a ubiquitous sensor network from both online (pre- and post- processing) via a web interface and onsite via a privacy badge.

The construction of this system started from developing a multimodal sensor and display network, the Ubiquitous Sensor Portals [2-4]. This sensor network can communicate with wearable privacy badges through a ZigBee radio network and change the sensing parameters onsite, i.e. turn on or off different sensors according to the settings of each individual badge user. Users can setup their privacy preference online by editing the sensor settings of each node and post process their recorded data from a web interface. The privacy level can also be dependent on the group status of the client browsing the sensor network—the badge user can assign different levels of privacy to different groups of people (e.g. taking an analogy to UNIX file system permission: “user/group/world”). Physical means of providing immediate privacy are also afforded (e.g., physically obstructing the sensors). Also, users can also scrub (or selectively "blur") any archived data.

Unlike other systems designed for enhanced privacy protection (see Chapter 2.1), our system leaves all the control to the users with our active privacy badge. The experimental design for our user study focuses on changing different parameters of this sensor network, for example, the default settings (opt in or out), and the processing of information (broadcasting or recording). Therefore, our major contribution to the research of privacy will be providing a user-centric privacy platform for ubiquitous computing and, for the first time, using this platform to obtain real-time experience with user feedback towards privacy within different scenarios, and default settings in a distributed dense sensor network.

1.1 Theory

For years, the study of privacy in ubiquitous computing has focused on designing privacy protocols. System designers construct their own privacy protocols either based on assumptions from their own education, religion, and social background or a survey about privacy concerns from a limited number of users. They either define “private zone’s” in a building, or use a context aware system to identify a possible “private scenario” [5-6]. After deciding on the complicated sensing algorithm, they declare their system to be privacy enhanced and able to protect any private scenario. However, a simple question one may ask is: “What situation should be considered private?” Does two people talking softly in a café, which is identified by the sensor network via a low audio signal with multiple motion sensor readings and the facial recognition system from the image snap shot, indicate a 100percent private conversation? The answer is as simple as the question itself: “We don’t really know.”

“Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively.” [7]

Admittedly, we system designers have overlooked one very important aspect of privacy for a long time – the dynamic nature of privacy. From the above definition of privacy, we can see that privacy is the ability of individuals to reveal themselves selectively. However, the existing systems only allow a fixed parameter that will define everyone’s privacy opinion regardless of the difference between time, space and individuals. Our brain is a very sophisticated machine plus, as the definition for privacy is in an ambiguous gray zone, it is extremely difficult to conclude a general rule for privacy that can suit all ages, genders, cultural backgrounds, and education levels. Rather then trying to automatically deduce a desired level of privacy for everyone, it is much more trackable to allow users to change their settings and control the sensors on site instantly – through user-centric control over sensor-related privacy that exploits pre-established privacy preferences.

The problem does not end there. On the users’ ends, there is almost no way for the users to access the information gathered by those sensor networks, not to mention having control over their personal information flow and customized privacy settings. The only option for the users is to trust the system and think that they are safe because of the accountability of system designers. Meanwhile, they try to stay away from the sensors as far as possible to protect their privacy making it impossible to realize the original goal of having a smart sensing and media interacting infrastructure in a modern building.

For example, Figure 1.1 is a series of pictures taken from the common area at the MIT Media Laboratory. Each red circle indicates a connected sensor node. There are at least 5 different sensor networks involved, including MITes [8], foodcam [9], Sociometric badges [10], G-speak [11] and Ubiquitous Sensor Portals [4]. Undoubtedly, it is an environment with dense sensor networks. It is also a very confusing space, since people have no control and almost no knowledge about the technologies around them. Although we trust our colleagues’ administrative accountability and believe that those systems are well-designed for privacy protection, there is still no interaction between users and sensor systems provided. N. Aharony [12] suggests that networked devices should be able to act on our behalf to other people and devices around us in a manner analogous to the way humans naturally interact with one another. In the same way, any privacy system should be configurable, allowing users to dynamically change the resolution of personal information exposed to and by the system differently for different groups of users. Thus, from this approach, ubiquitous computing’s goal of rich interactions in context aware environments will be gracefully balanced against the dynamic and varied concerns of privacy. Therefore, in this research, we focus on what we will call the logical layer of privacy control (Fig. 1.2).

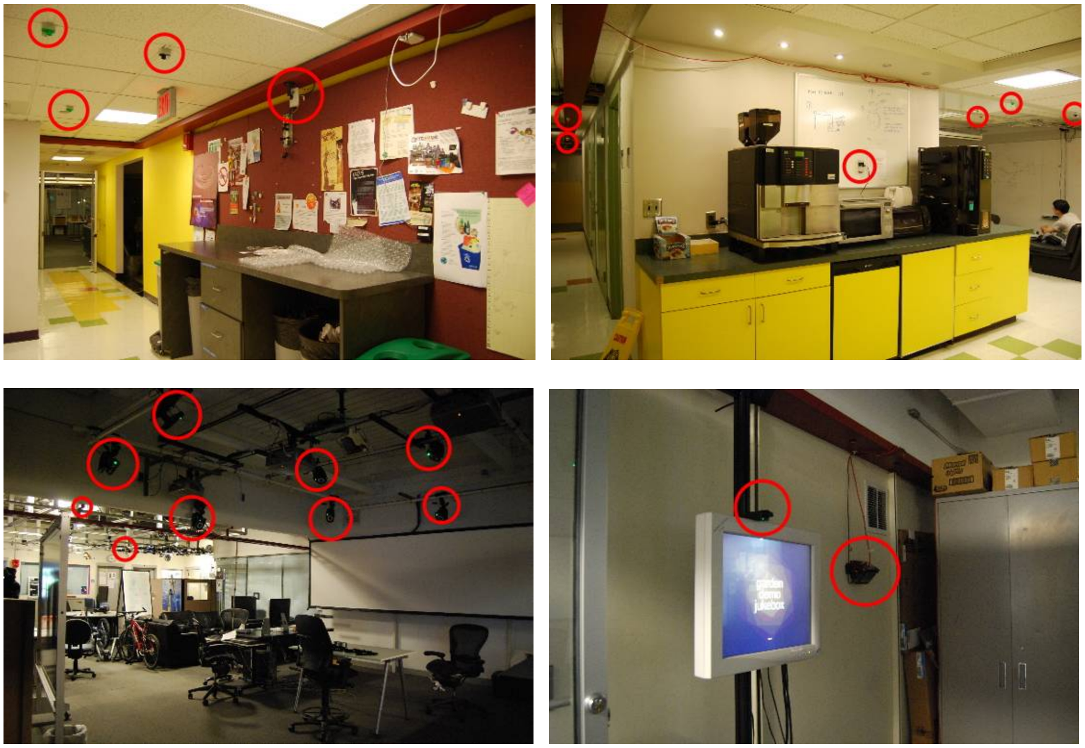


Figure 1.1 A series of pictures taken from common areas in the Media Lab. Each red circle indicates a sensing device.

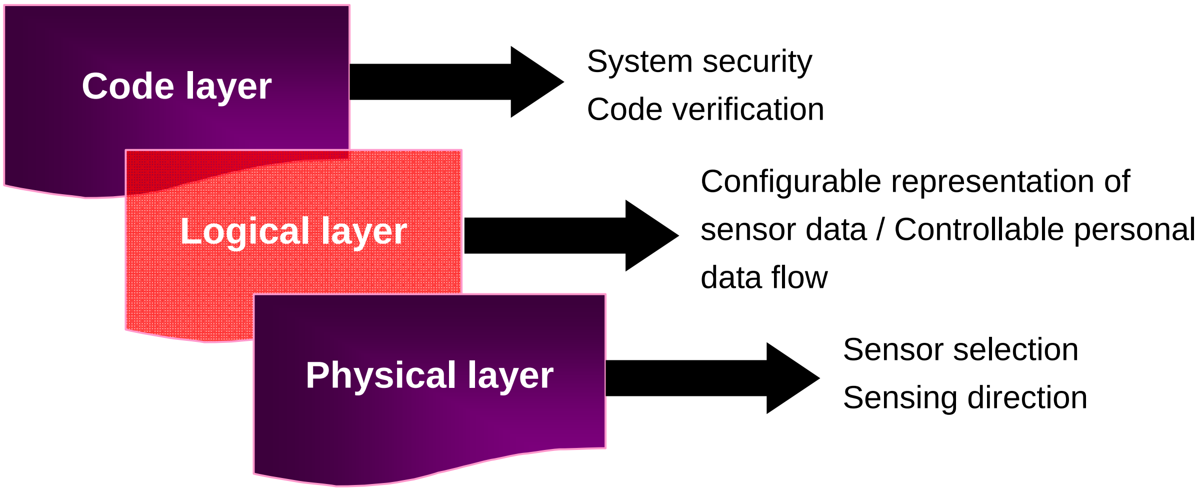


Figure 1.2 Three layers of privacy aspect in the design of ubiquitous sensor networks.

Instead of focusing on the code layer and basic system vulnerability (network security and code or hardware verification, which are active areas of research in practice [13]) or the physical layer (sensor selection or sensing region), we create a new approach which aims at giving each user dynamic privacy control for various sensing modalities with the configurable wearable device – an active privacy badge. In a ubiquitous sensor network environment, there will be too many nodes in the environment to be able to manually mask or deactivate and granting access on each sensor node isn't a feasible task to explicitly do. Consumers will not accept devices into their environment unless they feel some control over the information leakage – the market will dictate the need for standards and verifications to maintain the knowledge of controllable privacy. Therefore, with an active badge system broadcasting privacy preferences to the local vicinity, the environment can automatically throttle data to maintain appropriate privacy levels.

Furthermore, an accessible server for sensor data display will enable users to post-process their information flow, delete or restrict any recorded data and adjust their privacy resolution to different groups. This approach, unlike the previous privacy protection work, aim at giving users a measure of control over and peaceful coexistence with the massive, dense, ubiquitous computing sensor networks coming in the future. Therefore, instead of developing rules for system designers, the focus of this research is about managing privacy in various ways at a logical level – how people manage their own privacy rather than secure it from the system designers' end.

Chapter 2

Background

"Conscience is the inner voice which warns us that someone may be looking."

–H.L. Mencken

2.1 Previous Work

2.1.1 Privacy Research in Ubiquitous Computing

Substantial research has been devoted to the design strategies and policies for approaching privacy issues in a ubiquitous computing environment. The major approach for controlling the privacy status within sensor networks is through constructing secure protocols and code verification mechanisms for system developers to follow and examine as they construct the infrastructure for data acquisition and post data processing. Bellotti and Sellen were pioneers with their work on privacy in the context of video media spaces based on the experience of the RAVE media space at EuroPARC. They first proposed a framework in 1993 [14] for designing the feedback and control in ubiquitous computing environments and described the ideal state of affairs with respect to feedback or control of each of four types of behavior – Capture (What kind of information is being picked up?), Construction (What happens to information?), Accessibility (Is information public, available to particular groups, certain persons only, or just to one'self?) and Purposes (To what uses is information put?). The argument is that "feedback and control" over information in a ubiquitous computing environment can help preserve privacy.

Drawing upon Bellotti and Sellen's work, many toolkits and infrastructures have been developed to provide programming support and abstractions for protecting privacy in a ubiquitous computing environment. Confab [15], for example, is a personal ubiquitous computing system where data starts with the end-user (from a customized instant messenger) and can optionally be disclosed to others in a limited manner. It provides basic support for building ubiquitous computing applications with customizable privacy mechanisms. Campbell [16] and collaborators introduced Mist, a privacy control communication protocol, to separate location from identity from a privacy-preserving hierarchy of routers that form an overlay network.

Researchers also tried to use pseudonym and dummy users to blur users' information, especially location-specific data [17]. Recently, the research of privacy protection in context-aware pervasive systems moves further to the design of self-configuring privacy management infrastructures. Ortmann et al. proposed a self-configuring privacy management architecture for pervasive systems [4]. Further, Moncrieff and coworkers [5] presented a dynamic method for altering the level of privacy in the environment based on the context and the situation within the environment. Besides the research on dynamic privacy configuration in a building, the concept of automatically inferring privacy settings is also used in personal electronic devices such as a cell phone [18-19]. All of the above examples demonstrate the idea of creating a smarter and sophisticated system that could better suit users' need of privacy within the environment. However, without direct user control, the construction of an ideal system that can suit everyone's needs is almost impossible.

Another major method for improving the design of privacy protection in sensor networks is through the physical approach — different choice of sensors and location/direction for the sensing elements. In the technical report from MERL (Mitsubishi Electric Research Laboratories), "Worse is Better for Ambient Sensing", Reynolds and Wren [20-21] examined the ethical implications of choosing camera networks vs. infrared motion detector networks. Their results indicate that for most participants, infrared sensors (Fig. 2.1) were significantly less invasive than pan-tilt-zoom cameras. The design was later adapted and further developed by the House_n group at the MIT Media Laboratory [8], and implemented as a demonstration of a portable kit of wireless sensors for less invasive naturalistic data collection. The problematic part about this direction, sacrificing the sensing modalities to meet privacy needs, is that in order to provide better feedback and functions for users in a context-aware building infrastructure, merely motion sensor data might be insufficient. Although it is proven that data collected from motion sensing can indirectly lead to approximate personnel identification and localization, a motion sensor network still can not provide the full function of a modern ubiquitous network. Therefore, we try not to compromise our sensor system design, but rather to control a dynamic privacy level from the users' end with a privacy badge.

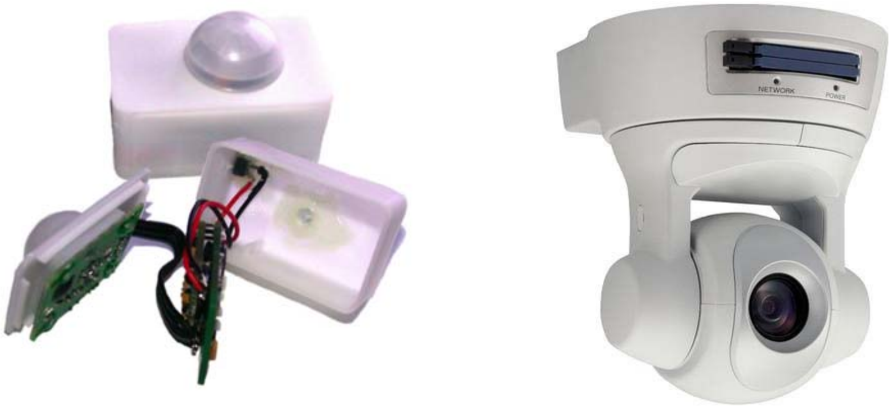


Figure 2.1 Left: a MERL motion detector node [8]. Right: the pan-tilt-zoom camera system the MERL team used to compare with the motion detection system.

2.2 Wearable Badge Systems

Wearable devices are by far the most effective method for connecting individuals with ubiquitous sensor networks. There are two major types of badge systems: active badges and passive badges. Active badge systems interact with the environmental sensors and observe how their actions affect them. Examples of technologies that are used in active badge systems include infrared (IR) transceivers, RFID (Radio Frequency Identification) tags, Bluetooth, and ZigBee networks. Passive badge systems sense the signal from ambient environments and receive or send the information passively, for example, exploiting the Global Positioning Systems (GPS) or RFID tags. Passive systems reveal no information about the user to a sensor network. Therefore, users can have full control over their privacy in a passive badge system. Because of the nature of its low privacy threat, we will focus this review on active badge systems.

2.2.1 Active Badge Systems

In a context-aware sensor network, active badges with the addition of multiple sensing modalities allow those network systems to adapt their functions to better suit the behavior and preferences of badge wearers. One of the first attempts to augment name tags with electronics and enhanced interaction was the active badge developed at Xerox PARC in 1991[22]. The badge (Figure 2.2) broadcasts the identity of its wearer and so can trigger automatic doors, automatic telephone forwarding and computer displays customized to each person reading them.

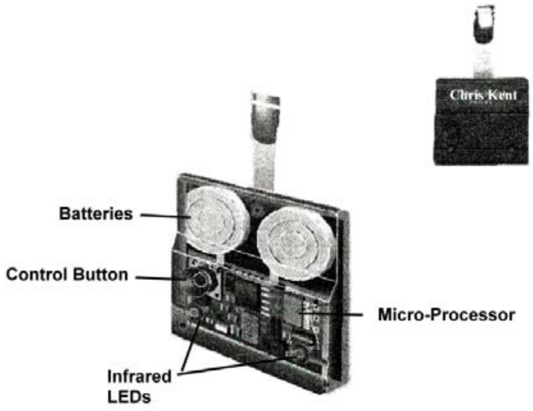


Figure 2.2 The design of active badge developed at Xerox PARC in 1991.

In 1992, Hopper et al. from Olivetti Research developed a simple platform that periodically transmits a modulated infrared (IR) ID to the vicinity, enabling people to be located by the IR receiver network in their facility [23]. Besides simply tracking the location of badge users, an active badge could be used to interact with the building system and provides better control over heating, ventilation, air-conditioning (such as HVAC system) and lighting base on the arrival, departure and routine movement of each individual [24]. One recent example is demonstrated by Mark Feldmeier [25] at MIT Media Laboratory, exploiting dense sensor networks for building comfort control. He built short range RF active badges (Fig 2.3) for building occupants that infer their comfort level in terms of temperature, humidity and lighting. Users wear the badge and train this system to adapt their comfort settings from pressing the "too hot" or "too cold" button on the badge during the testing period. With the information, this sensor networks can adjust the building's HVAC system automatically based on users' comfort preferences and minimize energy consumption while best maintaining the satisfaction of the occupants.

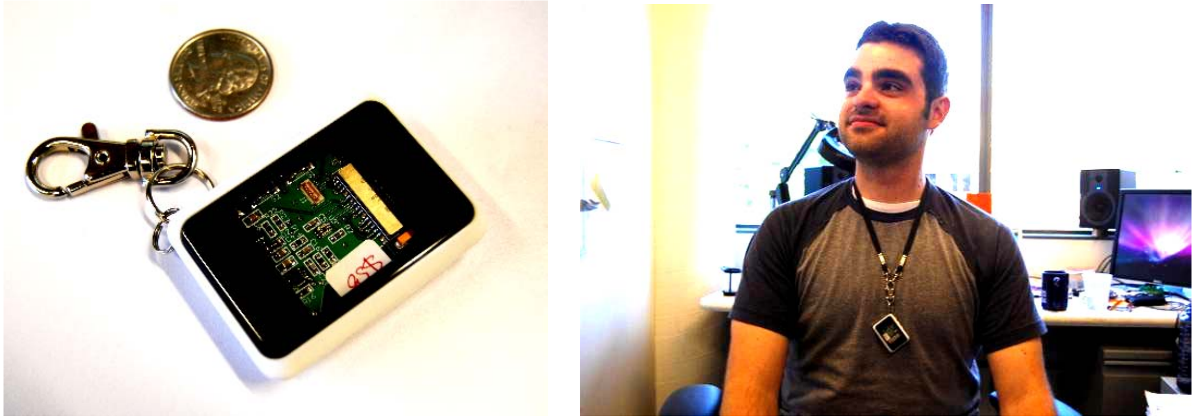


Figure 2.3 The active badge for building comfort control.

2.2.2 Active Badge Systems for Group Interaction

An active badge can also serve as a dynamic display for facilitating person-person interaction at large events. This direction started at the MIT Media Lab from the "Thinking Tag" project [26] that flashes LEDs according to agreement of wearers on a series of provocative questions, and the "Meme Tag"[27] which enabled users to selectively exchange brief catch phrases that can be tracked as they propagated through large groups (Figure 2.3 a,b). The idea of using active badge for group interaction was carried further by Mat Laibowitz with the design of UbER-Badge (Figure 2.3 c,d), a versatile platform at the juncture between wearable and social computing[28-29]. This platform was the first badge prototype that facilitates a variety of group interaction such as viral message passing, analysis of social networking, formation of affinity groups, real time display of social interaction and storing contacts for later retrieval.

The system was later adapted by the Sociometric badge, a wearable computing platform for measuring and analyzing human behavior in organizational settings [30]. The project proposed that through the use of active wearable badges, users' face-to-face interaction, conversational time and physical activity levels can be captured and analyzed to obtain their pattern of behavior. The developers believe the interaction and dynamics between organizations and individuals can be analyzed and understood through this wearable computing platform.

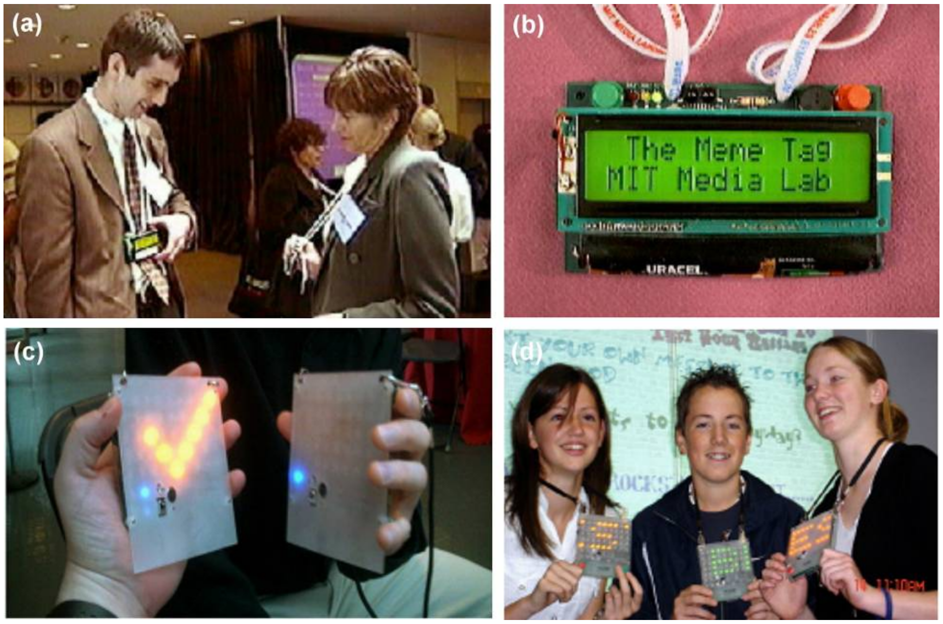


Figure 2.4 (a) Two people interacting through their Meme Tag. (b) Close up image of one Meme Tag. (c) Interaction between two UbER-Badges. (d) UbER-Badge users demonstrating the ability of scrolling text and showing simple animations from the LED array on their UbER-Badges.

2.3 Ubiquitous Sensor Portals

In order to study privacy from the viewpoint of actual users, the first step for this research is to build a highly visible lab-wide sensor network that potentially creates enough awareness for people working in this environment. We call it the Ubiquitous Sensor Portals (USPs). This sensor network was originally designed by Mat Laibowitz to support his SPINNER project [2-3] which will be described in the next section. The 45 portals comprise a sensor network that was distributed throughout the real world Media Lab (Fig. 2.4). Each portal, mounted on pan/tilt platform, has an array of sensors, as well as audio and video capabilities. Video is acquired via a 3 Mega Pixel camera above a touch screen display. The video board is driven by a TI DaVinci processor (an ARM9 running Linux paired with a C64x+ DSP core for video processing), and features a touch-screen LCD display and speaker.

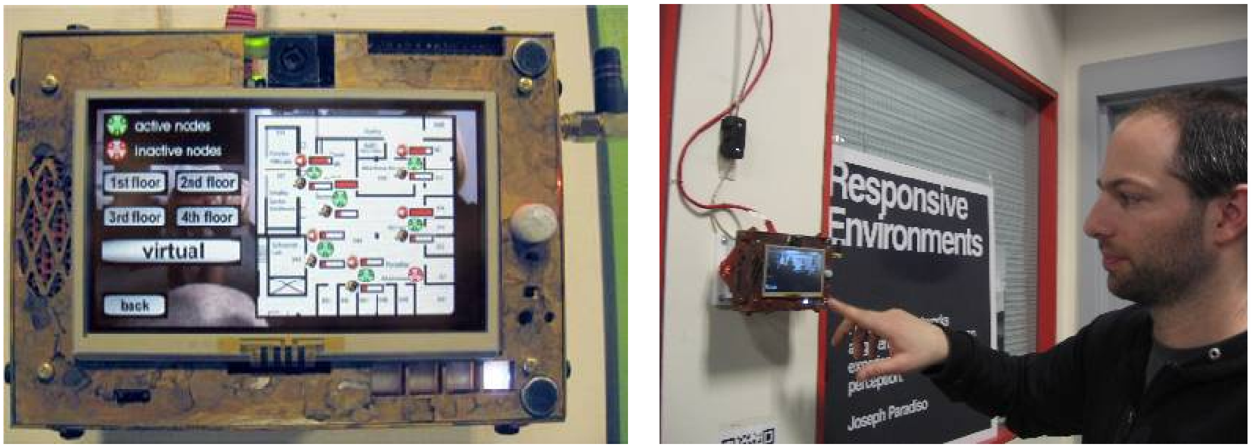


Figure 2.4 Left: USP with an interactive application for sensor data browsing and real time video streaming from other portals. Right: A user interacting via the USP’s touch screen interface.

The sensors and an 802.15.4 radio are mounted on a daughter card, which can be connected directly to a wired network for standalone operation or run as a slave to the video board. The sensor board runs off an AVR32 microcomputer (AV32UC3A1256) and features stereo microphone’s, PIR motion sensor, humidity/temperature sensor, light sensor, and 2 protocols of IR communication so it can detect and talk to any of the Media Lab's badges (For example, the Sociometric badge, the Privacy badge and the wearable badge for SPINNER applications) that are in the line of sight. The daughter card also supports several status LED's, and the radio communicates with and coarsely localizes many of the wearable sensors that several groups in the Media Lab are developing. The ubiquitous sensor portals are capable of streaming real time sensor data over the network and initiate interactions between different portals.

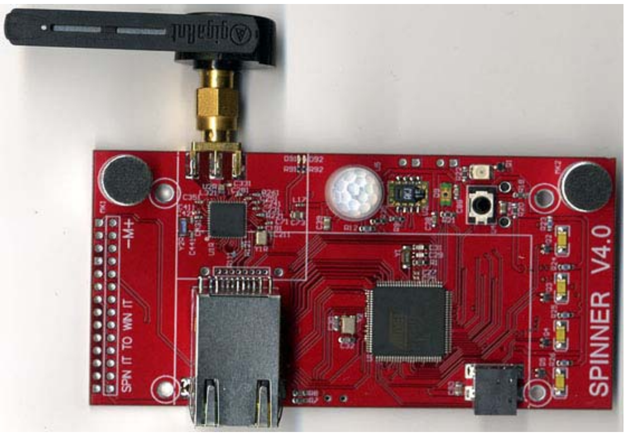


Figure 2.5 The environmental SPINNER sensor board.

2.3.1 SPINNER

SPINNER [3] (Sensate Pervasive Imaging Network for Narrative Extraction from Reality) is a novel sensor network system designed to detect and capture fragmented events of human behavior. SPINNER exploits the dense imaging sensor network formed by the USPs that cover 45 different places in the Media Laboratory. The network can collect and sequence the events through a sensor for narrative query and generate videos according to SPINNER's behavior model. The SPINNER network is comprised of wearable sensors (active badge and wristband, Figure 2.6), environmental sensors (Figure 2.5), and video sensors (Figure 2.6) that can identify and record events that fit specific narratives from the high resolution camera. Alternatively, the system can capture all events along with narrative data for cataloging and browsing. It is a platform for studying narratology in order to develop an effective narrative model that can be mapped onto sensor-detectable elements of human behavior.

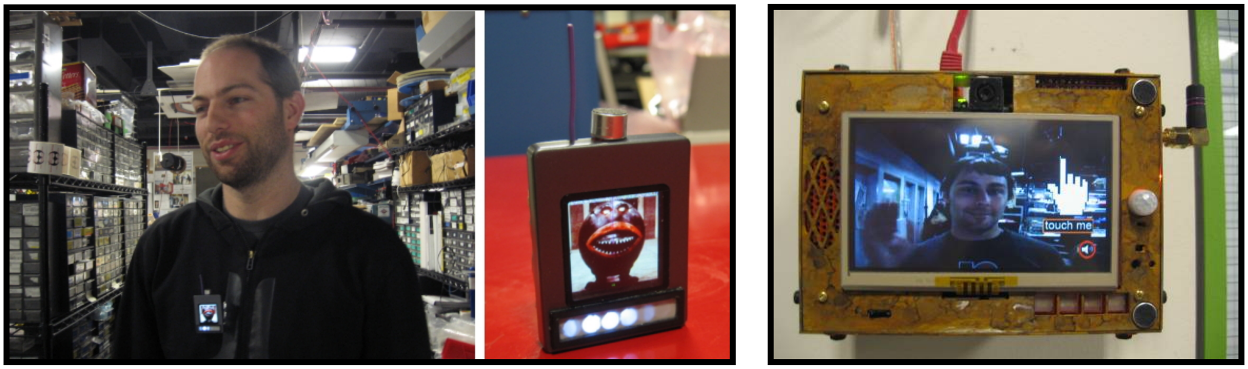


Figure 2.6 Left: an active badge for dynamic management of dense ubiquitous media. Right: a portal that is collecting video of an active badge user.

2.3.2 Cross Reality Application

The portal platform also supports another application called Cross Reality that involves possible privacy risks. Cross Reality, sometimes referred to as X-Reality, is a framework where events in the real world drive phenomena in a virtual environment that is unconstrained by time, space, or the constraints of physics [31]. Unlike traditional sensors or surveillance systems that record information and store data in a secure server that can only be accessed by system administrator, X-Reality applications broadcast the information to the virtual environment. The problem is that when information is broadcast, it becomes harder to manage the information flow afterwards and track personnel or agencies that obtain the information. Therefore, a Cross Reality event can instigate even more privacy concern than a simple recording. Hence, it is crucial for us to find a solution for privacy protection before ubiquitous media and Cross Reality events become substantial in our everyday lives.

In our Ubiquitous Sensor Portal system, we used Second Life from Linden Labs to demonstrate the Cross Reality concept. Created by Drew Harry, this virtual Media Lab on Second Life allows visitors to see live video from any of the portals in the real world by touching the screen of the portal with their avatar (Fig 2.7). They can also communicate with the real-world portal by touching a "Talk” button on the portal - initially, communication from Second Life to the real world is through text, but if the request to talk is granted in the real world, audio from the sensor board will also stream from the real world to the virtual portal, enabling 2-way communication.

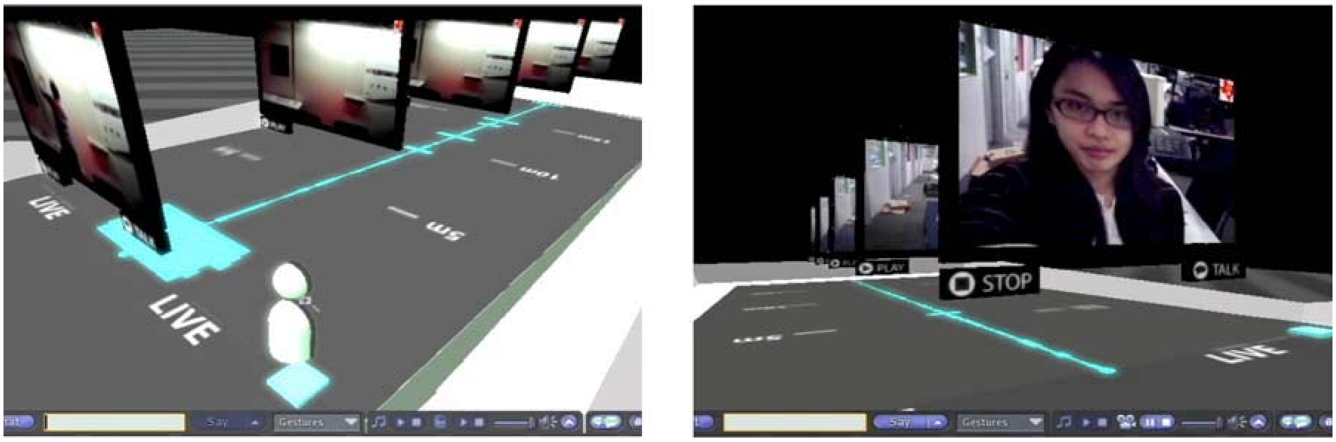


Figure 2.7 The virtual extension of a portal from Second Life. Left: One portal view over time, showing current and past images. Second Life visitors can look at video in the past by touching on the screens that are further back in the virtual portal view. Right: A real world user interacting with the virtual world through USP.

From the previous work about privacy research in ubiquitous computing, we have learned that it is important to create a flexible and configurable system that can protect users’ dynamic privacy needs. The research on active badge systems further provides a good method for sending individual signals that allow users to provide immediate feedback to the sensor portals and control the sensor systems around them in any locations and scenarios. Therefore, by combining the concept of dynamic privacy adjustment with the work on active wearable badge systems, we designed an active badge system that can be more efficient and effective for privacy protection. More details about the design and implementation of the privacy badge will be discussed in the following chapter.

Chapter 3

Design and Implementation

Sacrificing anonymity may be the next generation's price for keeping precious liberty, as prior generations paid in blood. ***–Hal Norby***

3.1 System Overview

There are four basic elements in this system — active privacy badges, Ubiquitous Sensor Portals, a data server, and web browsers (Figure 3.1). In this chapter, we describe the design principles of each element. Also, information about experimental setup and user study protocols are provided. In Chapter 4 and 5, we will go though more details on the hardware and software design of each element.

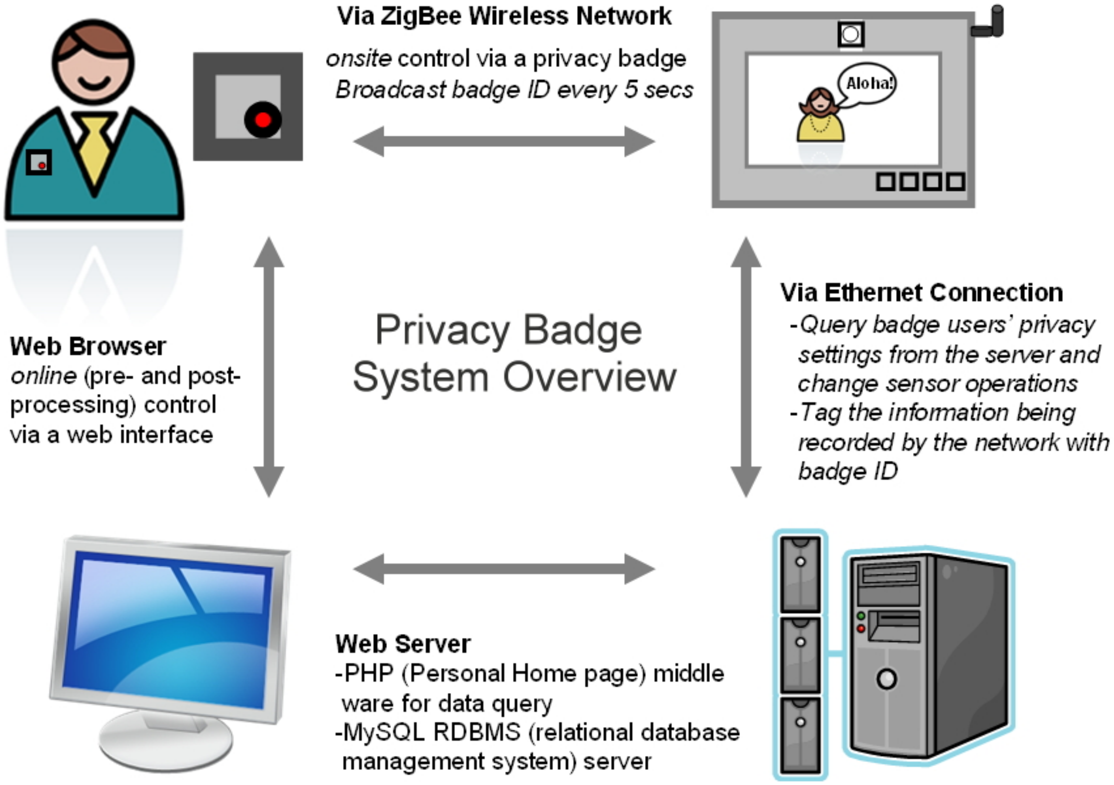

Via ZigBee Wireless Network
onsite control via a privacy badge
Broadcast badge ID every 5 secs
Aloha!
Privacy Badge System Overview
Web Browser
online (pre- and post-processing) control via a web interface
Via Ethernet Connection
-*Query badge users' privacy settings from the server and change sensor operations*
-*Tag the information being recorded by the network with badge ID*
Web Server
-PHP (Personal Home page) middle ware for data query
-MySQL RDBMS (relational database management system) server

Figure 3.1 System block diagram.

3.2 Privacy Badge

In order to provide active control, people in the sensor network environment are given active wearable privacy badges that broadcast a unique node ID through ZigBee radio every 10 seconds. The badge can also communicate with the portals via an IR transceiver. Users can register on the web interface with this unique set of 4 digits hex ID and edit their privacy preferences on each node (pre-processed privacy). Also, any information recorded (video, audio, motion sensor and the environmental sensor data) will be tagged with this ID so that users are able to post process their own information on the web interface (post-processed privacy).

While the users are wearing their badges within the coverage of our RF signal receiving range, this RF beacon can change the USPs' sensor settings accordingly. If a sudden privacy risk took place, users could block all sensor data recording for 10 seconds with the red panic button (Figure 3.2). After 10 minutes count down, the system goes back to its previous state.

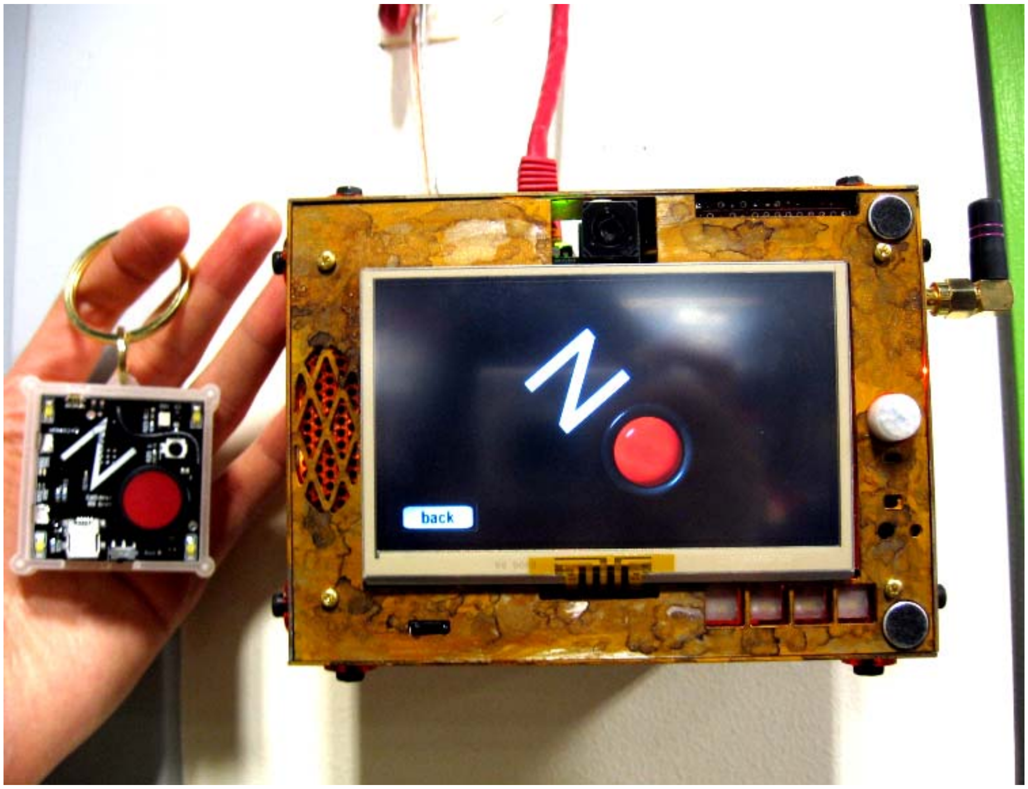
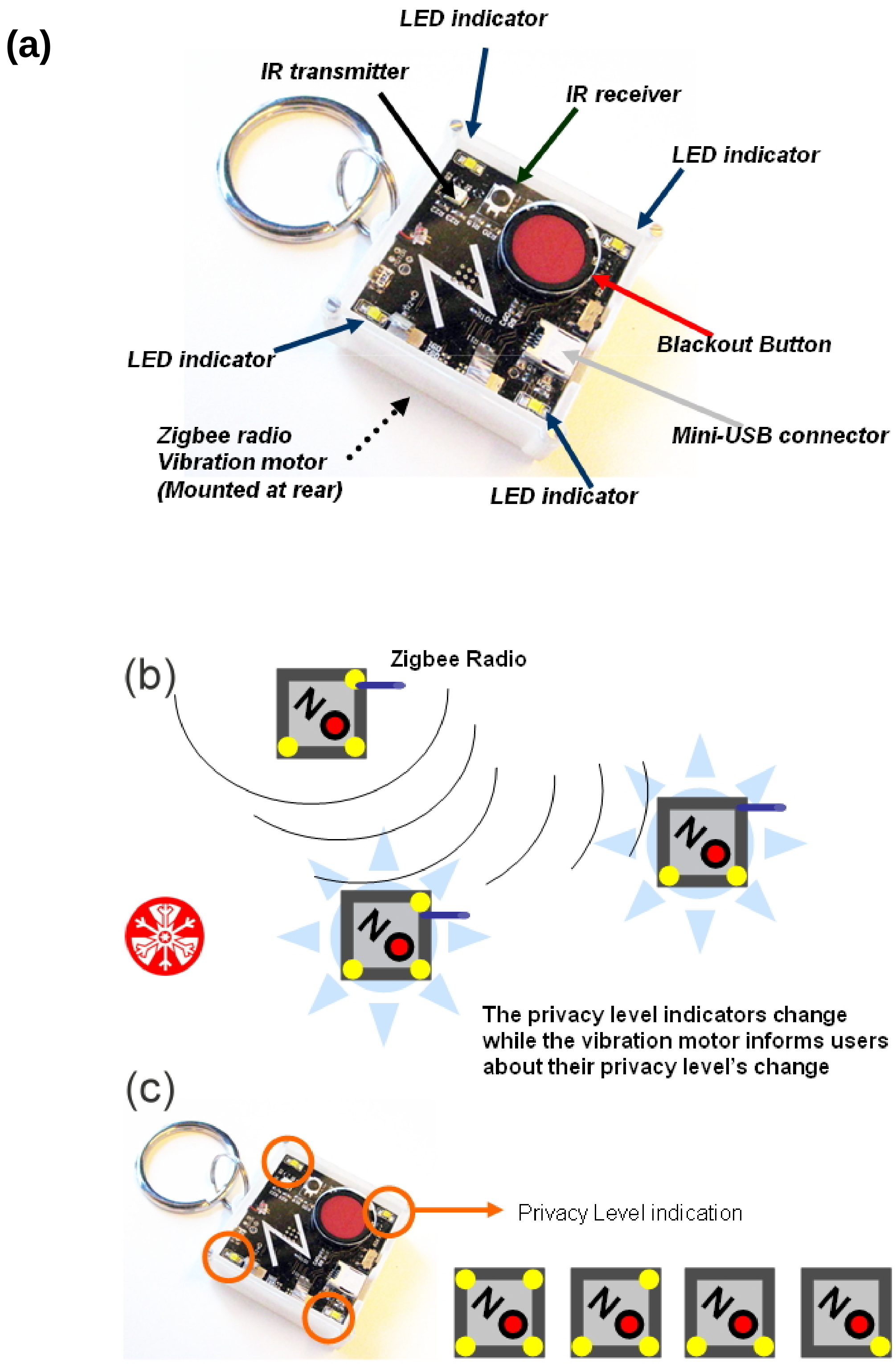


Figure 3.2 After pressing the “NO” button on a privacy badge, the USP blocks all data transmission and start the 10 seconds count down. The badge also counts down and informs the users with blinking from the four LEDs and buzzing from the vibration motor.

In Figure 3.3, we demonstrate one possibility of integrating the electronics into our everyday accessories by assembling the electronics in a case and making it a key chain. The output devices from this design are the four LEDs and the vibration motor mounted at rear. LEDs on the front panel indicate the privacy setting of four privacy levels – video off, audio off, motion sensor off, out of sensing area/total blocking (Figure 3.3(c)). The LEDs can be integrated into illuminated icons with different colored pulses for better indication or even replaced with an LCD. For a user with higher priority (higher privacy criteria), a change of privacy level will trigger the change of other users’ sensor settings in the environment. The vibration motor on the badge can inform users of any sudden privacy level changes such as settings being overwritten by someone nearby or the approach of another sensing device (Figure 3.3(b)).



The privacy level indicators change while the vibration motor informs users about their privacy level's change

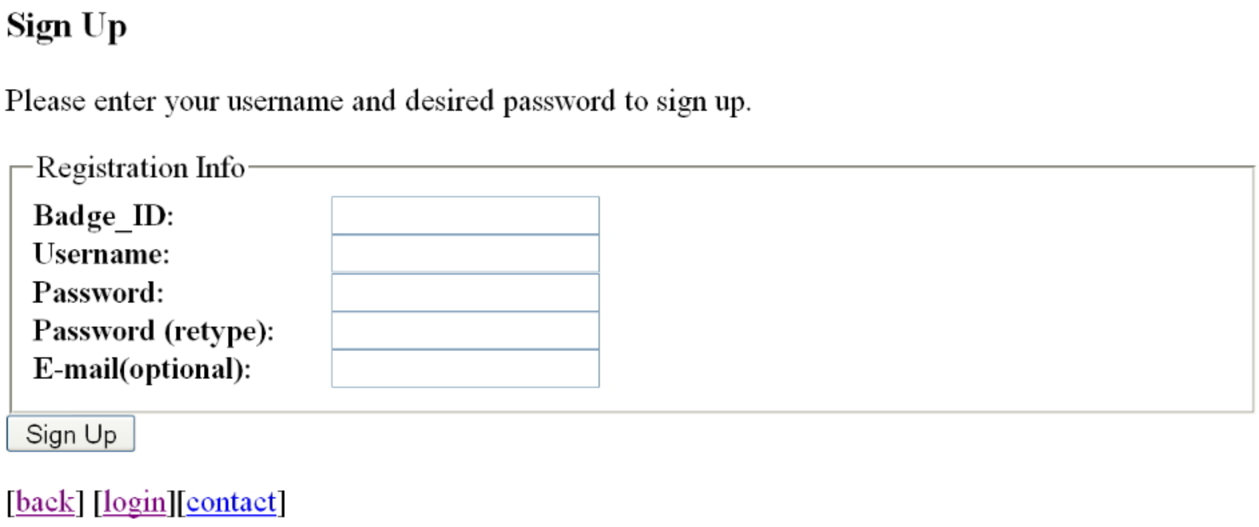
Figure 3.3 (a) A fully assembled Privacy Badge. (b)(c) Privacy level indication and notification through the output of light and vibration.

3.3 Applications on USPs

The role USPs play in this system is to adjust sensors' settings (e.g. on / off of each sensor in different locations) according to each user's preferences. They receive badge ZigBee packets from the sensor board's ZigBee chip and forward this information via Ethernet to the data server. Meanwhile, through the touch screen display, users in the system can get immediate feedback and control over the network (the "NO" image on the screen in figure 3.2 for example). After USPs receive ZigBee beacon packets from a user on IR line of sight signal (when the users stand in front of the portals), they query the badge user's settings from the server via Ethernet connection and change sensor operations, such as turning off video recording but leaving the motion sensor on. They also encode users' ID into the information recorded. This allows users to post process their data by sorting through the ownership of the information.

3.4 Data Server and Web Interface

As mentioned in previous chapters, users can register on the web interface with this unique 4-digit hex ID and edit their privacy preferences on each node. The random badge IDs are assigned from the MAC address of each ZigBee chip (detailed codes are listed in chapter 4.5). The sign up page is designed to keep the anonymity of each user. Moreover, anyone can swap their badge and use a different badge ID to remain anonymous (Figure 3.4).

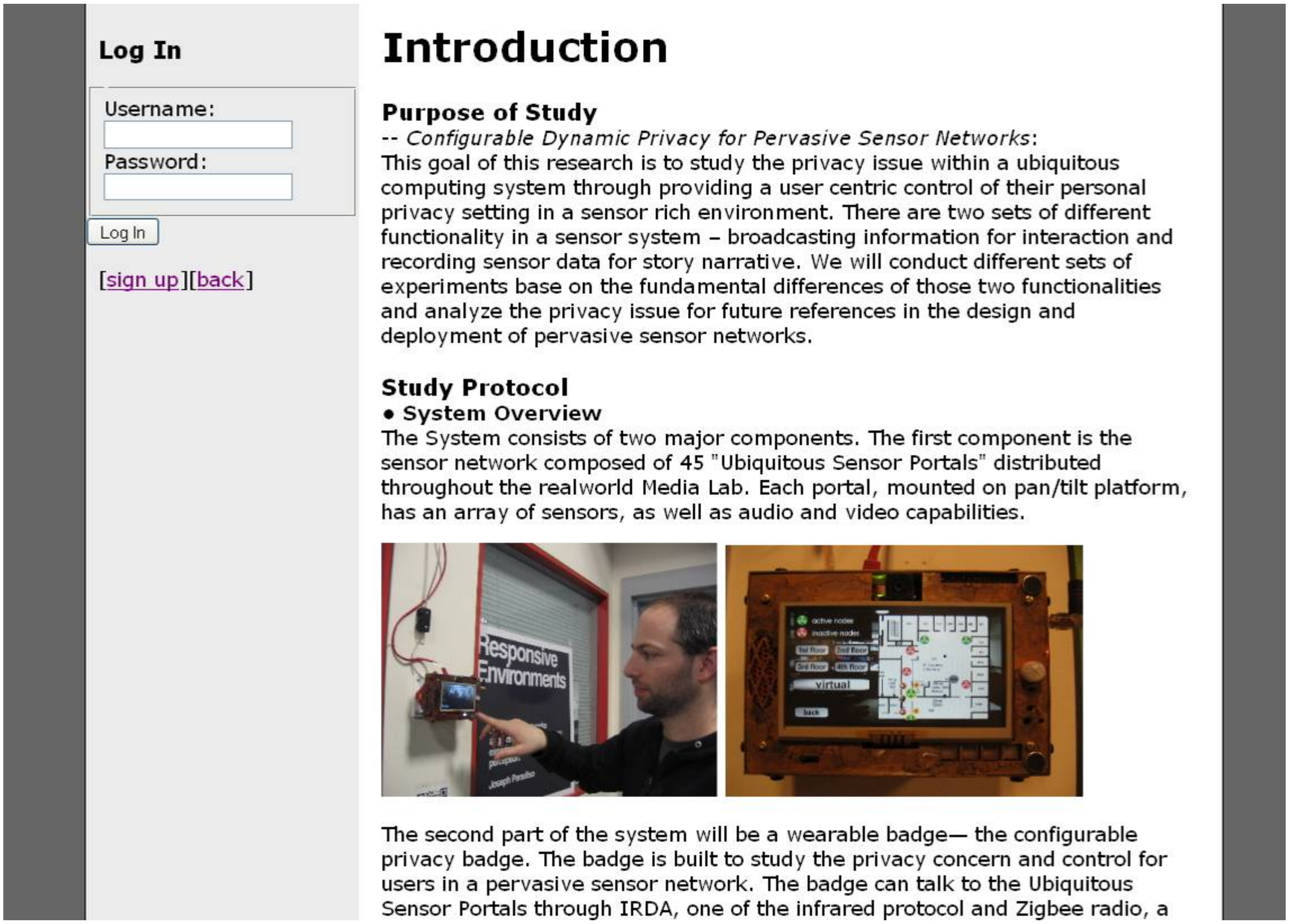


Sign Up

Please enter your username and desired password to sign up.

Figure 3.4 Sign up page of the web interface. The only information collected by the data server is users' randomly assigned badge ID.

In the login page, users can read instructions about protocols of this study (Figure 3.5). Massive amounts of video, audio files, motion sensor data, environmental sensor data, as well as users' privacy settings are processed and stored in log files and then written to a data server. Developed by our fellow Research Assistant from the Responsive Environments Group, Bo Morgan, this server gets registration from all the SPINNER nodes and updates all sensor data and badge packets in to a log file. With a relational database management system (RDBMS), such as SQL or MySQL, we can store the data and query with middleware (such as PHP) and access or edit through a web interface, allowing badge users to control their privacy both online — pre-processing with sensor settings and post-processing from editing/deleting the information recorded and onsite — via immediate feedback from pressing the blocking button.



Introduction

Purpose of Study

-- *Configurable Dynamic Privacy for Pervasive Sensor Networks*:

This goal of this research is to study the privacy issue within a ubiquitous computing system through providing a user centric control of their personal privacy setting in a sensor rich environment. There are two sets of different functionality in a sensor system – broadcasting information for interaction and recording sensor data for story narrative. We will conduct different sets of experiments base on the fundamental differences of those two functionalities and analyze the privacy issue for future references in the design and deployment of pervasive sensor networks.

Study Protocol

- System Overview

The System consists of two major components. The first component is the sensor network composed of 45 "Ubiquitous Sensor Portals" distributed throughout the realworld Media Lab. Each portal, mounted on pan/tilt platform, has an array of sensors, as well as audio and video capabilities.

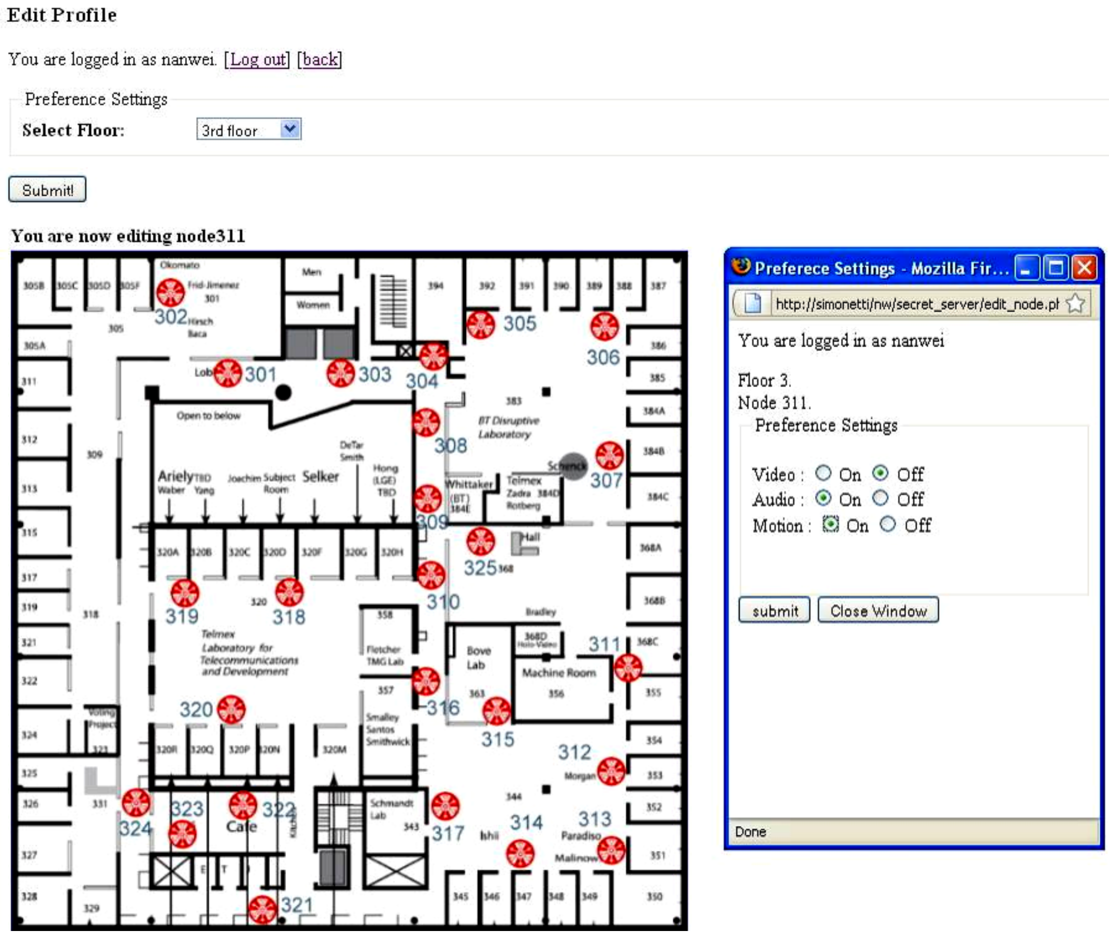
The second part of the system will be a wearable badge— the configurable privacy badge. The badge is built to study the privacy concern and control for users in a pervasive sensor network. The badge can talk to the Ubiquitous Sensor Portals through IRDA, one of the infrared protocol and Zigbee radio, a

Figure 3.5 The login page of our web interface.

3.4.1 Privacy Settings

On the users' end, they can edit sensor preferences on a location basis from the "edit sensor" page. For example, in Figure 3.6, the user is editing node 311 and turns off the video recording at this location. The design aims at getting information to adjust the privacy level of each location with users' sensor settings. We also provide an "edit all sensors" page (Figure 3.7) for people who do not feel like clicking on each node. Results from the data collection on this page can give us more insight about whether specific locations or the nature of different sensors is the greatest privacy threat for most people. In our first experiment, the default setting for all sensors is on (an opt out system that can generalize to higher-level sensor-derived features).

Besides allowing badge users to control the sensors around them, this web interface also provides a means to share your information recorded by the USPs with your friends. In the "edit group page", users can profile their group permission to customize how they appear to who is looking.



Edit Profile

You are logged in as nanwei. [Log out] [back]

Preference Settings

Select Floor: 3rd floor

Submit!

You are now editing node311

Preferece Settings - Mozilla Fir...

http://simonetti/nw/secret_server/edit_node.pl

You are logged in as nanwei

Floor 3.
Node 311.

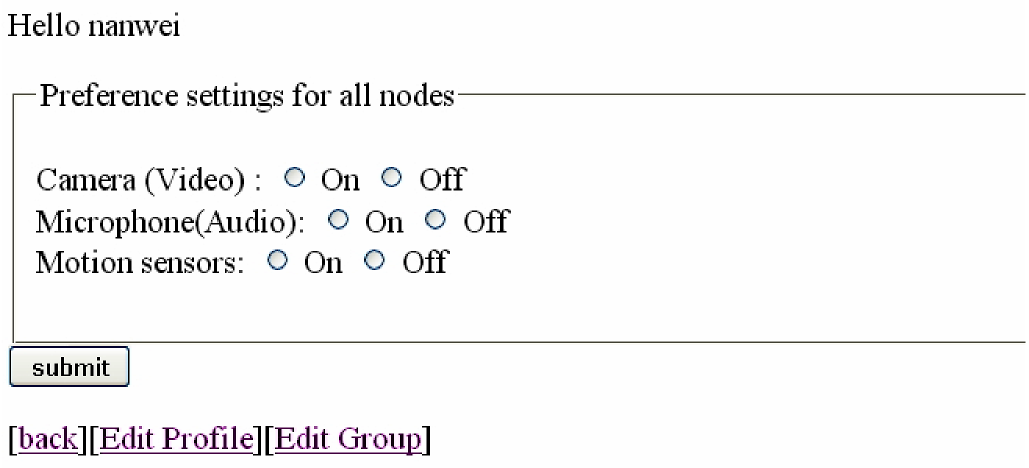
Preference Settings

Video : ○ On ● Off
Audio : ● On ○ Off
Motion : ● On ○ Off

submit Close Window

Done

Figure 3.6 The "edit sensor" page allows users to click on each nodes from a map and edit sensor setting on a location basis.



Hello nanwei

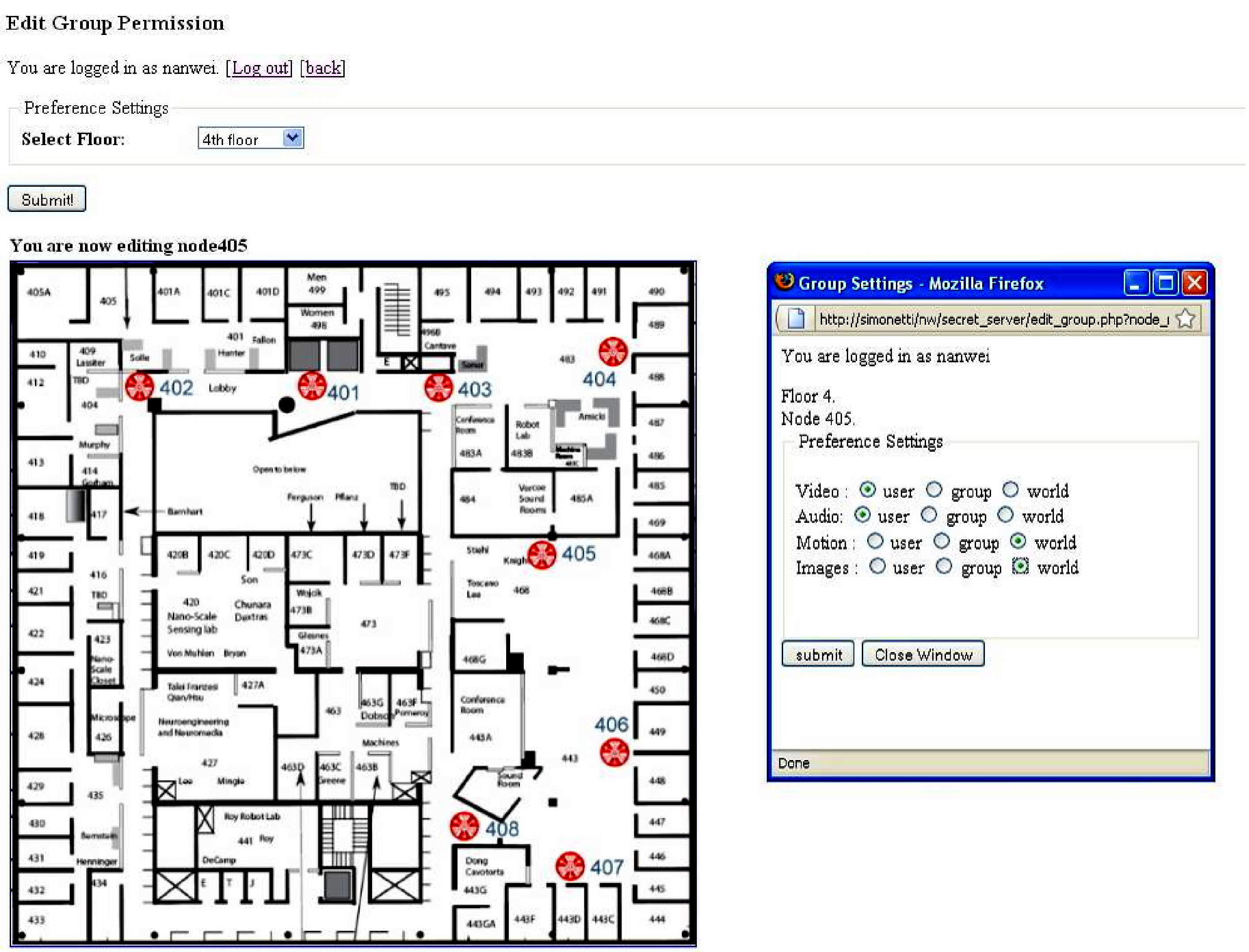
Preference settings for all nodes

Camera (Video) : ○ On ○ Off
Microphone(Audio): ○ On ○ Off
Motion sensors: ○ On ○ Off

Figure 3.7 The “edit all sensors” page allows users to set up all sensor preferences regardless of their location.

3.4.2 Group Dynamics

One of the most important things for users' privacy protection in a ubiquitous computing sensor network is having the ability to post process our personal information flow. While our system has the ability to collect video, audio and images and display that information recorded for each user individually, it could also be tailored to share users' information with others. In the edit group permission page, the users are allowed to reveal their information according to the hierarchy -- user / group / world, like a UNIX file permission system (e.g. family, friends, and world in real life). Further, the users are able to create their own group and send out invitations for other users to join their group. This framework can not only allow the users to customize how they appear to who is looking, but also can be used as a social networking tool similar to Google tracker, which let you follow your friends’ or families’ locations in real-time [32].



Edit Group Permission

You are logged in as nanwei. [Log out] [back]

Preference Settings

Select Floor: 4th floor

Submit!

You are now editing node405

Group Settings - Mozilla Firefox

http://simonetti/nw/secret_server/edit_group.php?node_i

You are logged in as nanwei

Floor 4.
Node 405.

Preference Settings

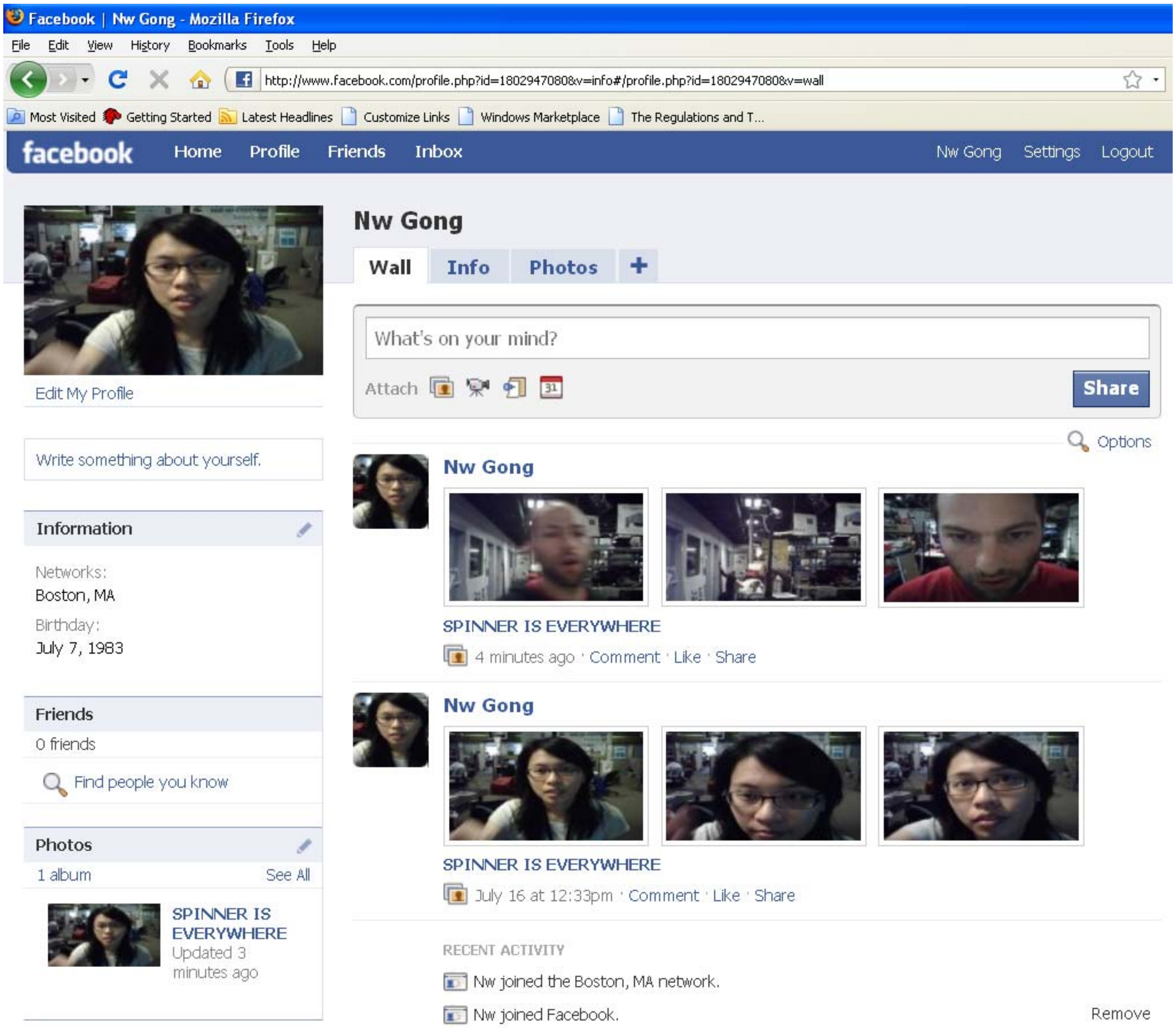
Video : ● user ○ group ○ world
Audio: ● user ○ group ○ world
Motion : ○ user ○ group ● world
Images : ○ user ○ group ● world

submit Close Window

Done

Figure 3.8 The "Edit Group" page allows users to reveal and share information such as images and videos taken by the USPs with different group of people.

Another possibility of group sharing and social networking that we are currently developing is to share our information through Facebook. Facebook is a very popular free-access social networking website that is operated and privately owned by Facebook, Inc.[33] Users can join networks organized by city, workplace, school, and region to connect and interact with other people. It is a widely used social networking platform with more than 30 million active users accessing it everyday. Here, we demonstrate a new concept of using our privacy badge to selectively reveal your location-sensitive information to your social networks. Users can select and invite people to view and comment on the pictures, video and audio regarding you. Figure 3.9 is a demonstration of location-based photo sharing on Facebook. Every picture is automatically captured from the USPs. In our future system, this photo/video sharing mechanism will enable one to automatically link his/her Facebook account to our web interface that will send friend requests and allow users to join groups from this location-specific social network.



http://www.facebook.com/profile.php?id=1802947080&v=info#/profile.php?id=1802947080&v=wall

Nw Gong

What's on your mind?

Edit My Profile

Write something about yourself.

Information

Networks:
Boston, MA

Birthday:
July 7, 1983

Friends

0 friends

Find people you know

Photos

1 album See All

SPINNER IS EVERYWHERE
Updated 3 minutes ago

Nw Gong

SPINNER IS EVERYWHERE

4 minutes ago · Comment · Like · Share

Nw Gong

SPINNER IS EVERYWHERE

July 16 at 12:33pm · Comment · Like · Share

RECENT ACTIVITY

Nw joined the Boston, MA network.

Nw joined Facebook.

Figure 3.9 Example of photo sharing on the Facebook platform.

In conclusion, we have built and implemented a privacy-aware social networking and interactive media system throughout the MIT Media Laboratory. Users' anonymity and privacy are carefully protected during the process of data acquisition. The following chapter will cover details about the hardware design of privacy badges.

Chapter 4

System Design

"When a man assumes a public trust, he should consider himself as public property."

–Thomas Jefferson

4.1 Hardware System

To implement the concept of using wearable active badges for privacy control, we built a hardware system comprised of 30 privacy badges that can communicate with the Ubiquitous Sensor Portals via ZigBee radio and Infrared transmitter. This wearable badge design aims to be as simple and small as could be in order to maintain light weight and be used as an everyday accessory, such as a keychain or a necklace. Another important aspect of badge design – the user interface for wearable badges — is also considered and discussed in the later chapters.

The system block diagram is shown below (Figure 4.1). Each node requires processing (microcontroller), communication (ZigBee radio and IR transceiver), and power management (rechargeable power source) capabilities as well as output devices, such as a vibration motor and LEDs to indicate current privacy status.

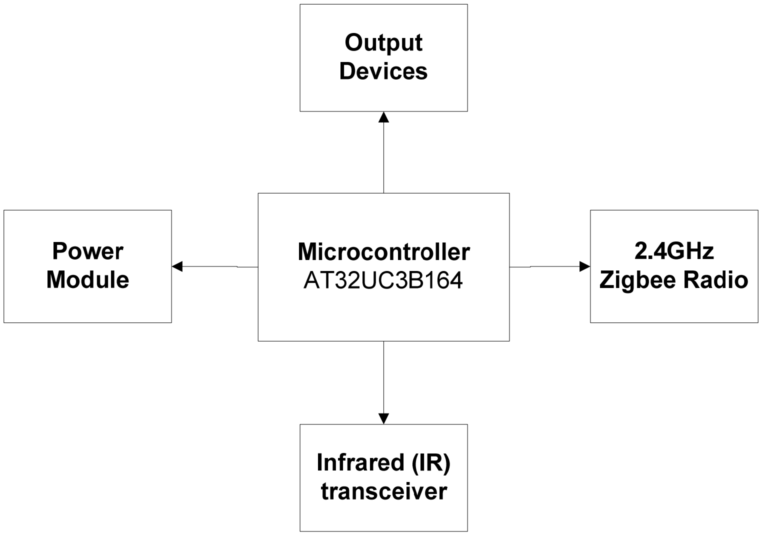


Figure 4.1 Block diagram of the active privacy badge's hardware system.

Figure 4.2 is the picture of our printed circuit board (PCB) layout. Each badge is powered by a 3.7V, 540mAh rechargeable lithium polymer battery. The top side of this board includes a MINI USB connector for charging the battery with a USB cable, 4 LEDs, IR LED, IR receiver, power switch and a big red button for ease of pressing.

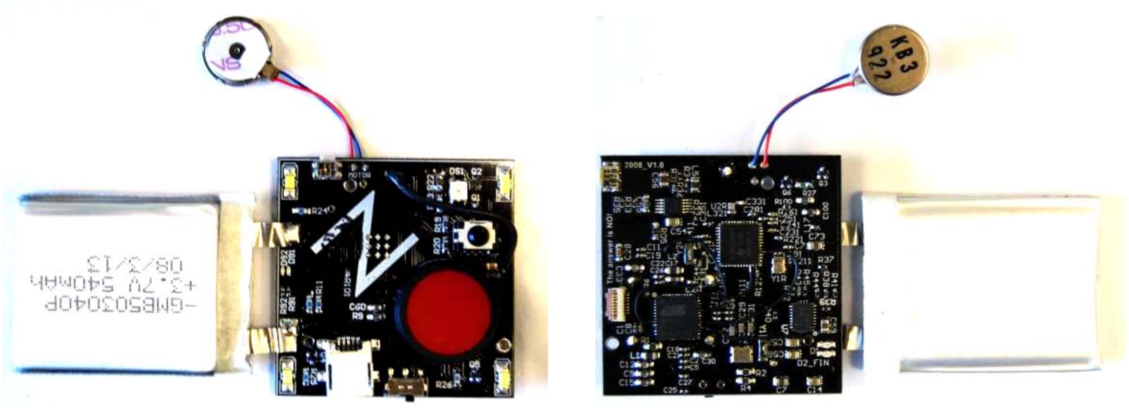


Figure 4.2 Badge hardware top (left picture) and buttom (right picture).

On the bottom of this board, we can see the MCU (AT32UC3B164), ZigBee network processor (CC2480), the power management ICs – step-down converter (TPS62050) and a single chip charge and system power-path management IC (BQ24030). The complete schematics, printed circuit board layouts, bill of materials are listed in Appendix A.

4.1.1 Processing

Each of the battery-powered nodes is controlled by an AVR32 32-bit microcontroller (MCU, here we use AT32UC3B164). The AT32UC3B is a complete System-On-Chip microcontroller based on the AVR32 UC RISC processor running at frequencies up to 60 MHz. It has 16K of SRAM and 64KB of flash for program storage. The power supply is a single 3.3V from the regulated battery power. The AVR32UC is a high-performance 32-bit RISC microprocessor core, designed for cost-sensitive embedded applications, with particular emphasis on low power consumption, high code density and high performance [34]. Two external oscillators are used in the processing circuit. One is an ultra small surface mount type 12 MHz crystal oscillator (NX3225SA, 3.2 x 2.5 x 0.55 mm, 17mg). Another external 32 kHz oscillator (FC-135, 3.2 x 1.5 x 0.8 mm) is also included in the processing module for power and clock management. This ultra-low power oscillator is used when the processor goes into a low power mode. In the low power mode we chose, all synchronous clocks are stopped, but oscillators and the Phase-Lock-Loop (PLL) are running, allowing quick wake-up to normal mode from RTC (Real Time Clock) or external interrupt (EIC) sources. This processor also features 7-Channel 16-bit Pulse Width Modulation Controller (PWM) and one Master/Slave Serial Peripheral Interfaces (SPI) with Chip Select Signals. In order to minimize the size of this board, we choose the smallest 48-pin QFN packaging.

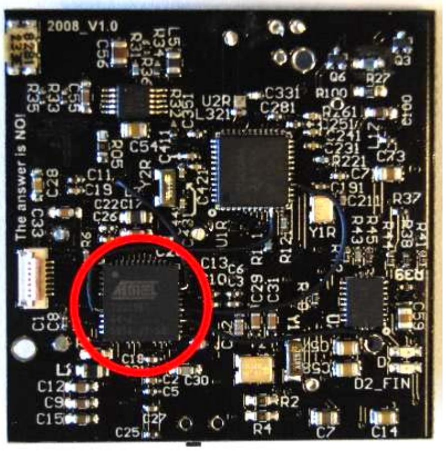


Figure 4.3 Microprocessor on the PCB design.

4.1.2 Communication

Two communication methods were chosen in this design to provide long and short range data transmission. For the long range communication, a ZigBee radio network was chosen to provide a 10m-75m signal range in the building. For the short range communication, an IR Receiver Module and IR LED were selected.

- **ZigBee Radio**

ZigBee technology is a low data rate (250kbps at 2.4GHz), low power consumption, low cost, and wireless networking protocol targeted towards automation and remote control applications build around the IEEE 802.15.4 standard. The specific module used there is Z-Accel 2.4 GHz ZigBee chip (CC2480) from Texas Instruments [35]. The CC2480 is an IEEE 802.15.4-compliant 2.4 GHz DSSS RF transceiver which provides wide supply voltage range (2.0V –3.6V) low current consumption (RX: 27mA, TX: 27 mA) and fast transition times. The 7x7mm QLP48 package chip is shown in Figure 4.4. A single-ended monopole antenna with a Balun network between the trace wire differential output and the antenna is designed for our short range application. Monopole antennas are resonant antennas with a length corresponding to one quarter of the RF electrical wavelength (λ/4). The length of the λ/4-monopole antenna is given by:

$$\boldsymbol{4 * L = c / f}$$

Where f is 2.451GHz (for ZigBee channel 11) and c is 2.998x10^8 m/s, a λ/4-monopole antenna should be 30.59 mm (Figure 4.4).

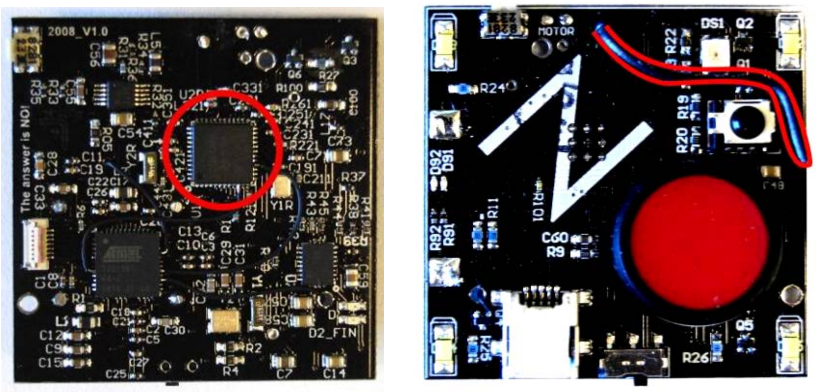


Figure 4.4 Left: The red circle indicates the CC2480 ZigBee processor. Right: Antenna extended from the front of PCB.

The CC2480 interfaces to any microcontroller through an SPI (Serial Peripheral Interface

Bus) or UART (Universal asynchronous receiver/transmitter) interface. In this design, the SPI interface was selected, allowing the microprocessor to control the ZigBee radio through TI's Simple API commands. Figure 4.5 shows the interfacing between a processor and the CC2480 chip.

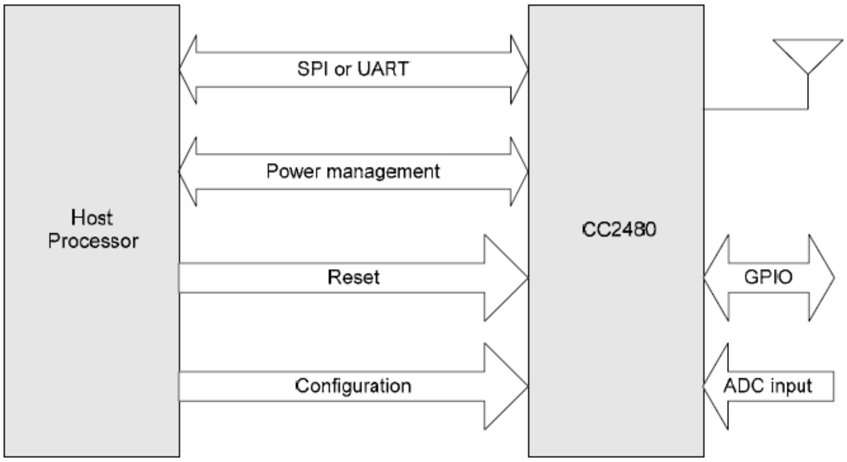


Figure 4.5 The diagram shows how a host processor interfaces with CC2480

Besides the SPI interface, there are three other hardware interfaces between the host processor (AV32UC3B) and CC2480.

1. ***Power Management***: This interface (only used if SPI interface is selected) consists of two signals (SRDY and MRDY) and is used to communicate the power management status and to wake up sleeping devices. The host processor can run in sleep mode and wait for an interrupt wakeup to save power.
2. ***Reset***: The host processor can reset the CC2480 through the RESET_N pin (hard reset). In addition, a software reset interface is provided.
3. ***Configuration***: This interface consists of the CFG0 and CFG1 pins on the CC2480, and is used to select SPI or UART transport and to select whether a 32 kHz crystal is installed.

In addition, several other configuration parameters may be configured on the CC2480 through the software interface.

1. ***ADC inputs***: the CC2480 has an onboard 12-bit ADC and 2 ADC input pins (A0 and A1). A software interface is provided for the host processor to perform an ADC conversion and read the value. For example, a built-in temperature sensor and battery monitor can be also read through the ADC interface.
2. ***GPIO pins***: Four configurable GPIO pins (GPIO0-3) are available on the CC2480. A

software interface is provided for the host processor to read, write and toggle the GPIO pins. In our design, two LEDs (D91 and D92 on the front) are connected to the GPIO pins on CC2480 to indicate the current network status of each node (i.e. a coordinator, a router or an end device).

3. ***Non volatile parameters***: This software interface allows the host processor to store and access 4 2-byte parameters and 2 16-byte parameters in the non volatile memory of the CC2480.
4. ***Software timers***: Up to four software timers may be configured by the host processor on the CC2480.

• Infrared Module

In order to provide a short range communication method for face-to-face interaction between badge users and the sensor portal, an IR receiver module (TSOP36238) was selected for receiving the IR data transmission. The TSOP36238 is an IR receiver module for the remote control system. A PIN diode and preamplifier are assembled on a lead frame; the epoxy package is designed as IR filters (Figure 4.6). The demodulated output signal can directly be decoded by a microprocessor. The 3 V supply voltage can support all major transmission codes. An IR LED was selected to pair with the IR receiver module for data transmission (Figure 4.6). This IR LED is connected to a PWM channel of the microprocessor for generating precision output. Via its 38 kHz carrier frequency, the information can be modulated and transmitted by various IR protocols. On the receiving end, the IR receiver module demodulates the signal and sends the output to a timer on a microcontroller.

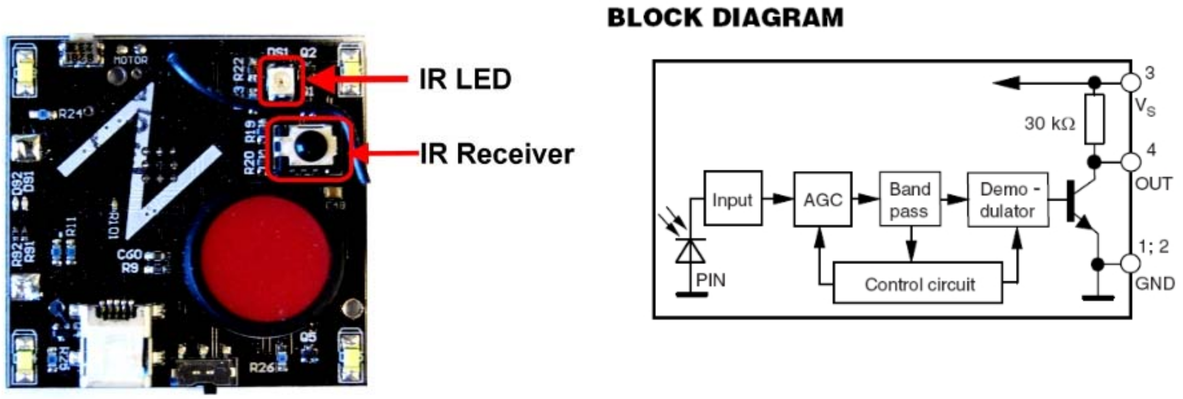


Figure 4.6 Left: the Infrared transceiver modules' layout on our PCB design. Right: block diagram of the IR receiver module.

4.1.3 Power Module

One of the most critical issues in the design of an active badge system is the power consumption. Although ZigBee is a low-power radio networking technology (RX: 27mA, TX: 27 mA), for an active badge system which requires a constant transmission, battery life can still be a serious challenge. Here, we use a single-chip charge and system power-path management IC (bq24030 from TI [36]) for charging the lithium polymer battery via a USB port or an AC adapter. The chip can support up to 2 Amperes (A) and charge the battery up to 4.2 Volts (V). Moreover, it can power the system while independently charging the battery, which reduces the charge and discharge cycle on the battery, allowing proper charge termination. The design of this chip makes it possible to supply power to the system from AC, USB, or battery sources continuously (See Figure 4.7). It is also possible to provide feedback of the charging status via LEDs or the output to the MCU. Here, we use two 0603 package LEDs (green D1 and red D2) to indicate the charging status. During charging, the red LED is on (Figure 4.8); when the fast charging is completed, the green LED will be on while the red is off. The chip pre-charges the battery when it is really low (<3V) and indicates the status with both LEDs on. In order to regulate the output voltage to provide the MCU with 3.3V, a step down converter chip (800-mA Synchronous step-down converter, TPS62050, 10 pin MSOP package) is also included in this circuit.

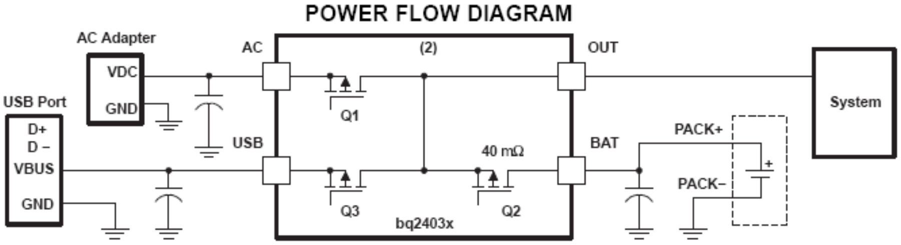


Figure 4.7 Power flow diagram of the system power-path management IC (bq24030). The power source can come from the USB port, AC adapter or the battery.

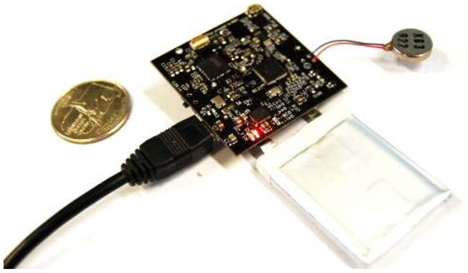


Figure 4.8 Demonstration of charging the battery and powering the system from a USB cable.

4.1.4 Output Devices

To provide instant feedbacks for the users, two output devices are provided on this badge. The first type of feedback, vibration, is from a vibration motor mounted on the back. The shaft-less vibration motor (310-10 Precision Micro-drives) we use is a 10mm diameter, 3.5mm thick motor which has an average rated speed of 12000 rpm. The start voltage is around 2.3 V and the start current is 85 mA. The overall vibration amplitude is about 0.8 G.

Another type of feedback is the visual feedback from LEDs mounted on the front of this PCB. Connected to the PWM channels, those LEDs can blink with different brightness for various indications and, in the same time, save the battery life.

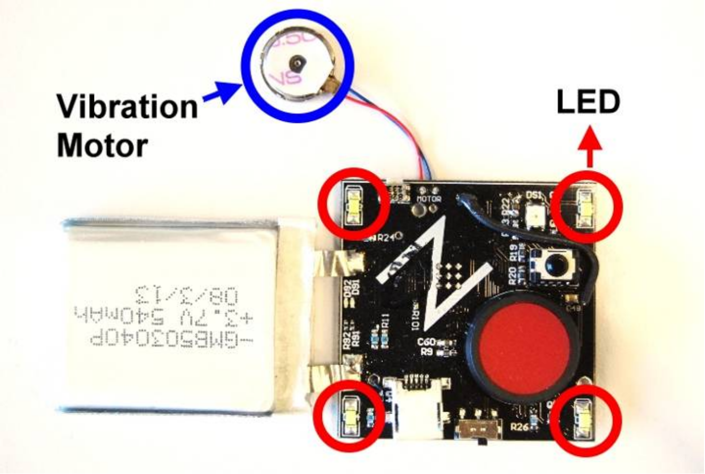


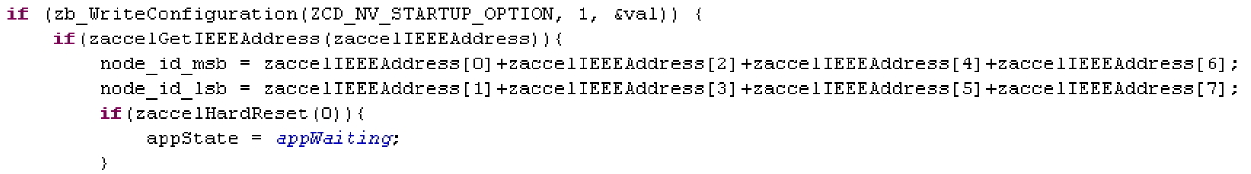
Figure 4.9 Output devices on the badge.

4.2 Software System

The software infrastructure for our system can be divided into three categories: the firmware for badge and portal communication (which runs on the nodes that sends and receives RF or IR beacons from the USPs and provides instant feedback from the output devices), the middleware that runs between a data server and the web interface and the application software that runs on each USP for providingd interactions on the touch screen. In this section, we will focus more on the communication protocols between each segment.

4.2.1 Badge and Portal Communication Firmware

The badge firmware inherited the communication protocols from the environmental sensors on each USP. The badge IDs are assigned from the MAC address of each ZigBee chip. The MAC address, also called IEEE address, long address, or extended address, is a 64 bit number that uniquely identifies each ZigBee device from all other ZigBee devices in the world [37]. Here, we use the combination of this 64-bit number to generate our 4-digit Hex badge IDs (Figure 4.10).



```
if (zb_WriteConfiguration(ZCD_NV_STARTUP_OPTION, 1, &val)) {
    if(zaccelGetIEEEAddress(zaccelIEEEAddress)){
        node_id_msb = zaccelIEEEAddress[0]+zaccelIEEEAddress[2]+zaccelIEEEAddress[4]+zaccelIEEEAddress[6];
        node_id_lsb = zaccelIEEEAddress[1]+zaccelIEEEAddress[3]+zaccelIEEEAddress[5]+zaccelIEEEAddress[7];
        if(zaccelHardReset(0)){
            appState = appWaiting;
        }
```

Figure 4.10 Codes for generating node IDs from each ZigBee chip’s unique MAC address.

The ZigBee stack for the CC2480 is the Z-Stack™ (TI's ZigBee compliant protocol stack for a growing portfolio of IEEE 802.15.4 products and platforms), and we adopted TI’s Simple API for our ZigBee communication firmware [35]. There are three types of ZigBee devices – ZigBee coordinator, ZigBee Router, and ZigBee End Device. The coordinator forms the root of the network tree and might bridge to other networks. Therefore, the USP ZigBee devices play the role of initiating the network and bridging across other networks. The routers can run an application function or act as an intermediate router for passing data from other devices. In our case, each USP ZigBee device boots up and searches for a network. If a network already exists, the device will join the network as a router; if not, the device will start its own network and boot up as a coordinator. The end device has just enough functionality to talk to the parent node, which can be either a coordinator or a router. This allows the node to be in low power (sleep) mode most of the time and only wakes up when needed for sending a signal or checking for incoming information. Therefore, all of the badges are by default an end device. They broadcast the node ID and different commands. The badges periodically broadcast a signal, allowing the server to locate each badge user. Also, when the user presses the privacy “blocking” button, the badge will send a packet with a ZB_BUTTON_PRESS byte. Table 4.1 shows the standard packet structure of our ZigBee communication protocol.

ZIGBEE_SIGNATURE_BYTE	NODE_ADDRESS_MSB	NODE_ADDRESS_LSB	ZB_COMMEND	ZB_BUTTON_PRESS
0x6E	**MSB of node ID**	**LSB of node ID**	**0x11**	**0x11**

Table 4.1 The ZigBee packet structure.

Another communication mode between badges and portals is infrared (IR). The USP sensor board uses its own variation of protocol from Sony’s SIRC protocol. It uses pulse width modulation (PWM) with carrier frequency of 38 kHz to encode the bits. The pulse representing a logical "1" is a 1ms long burst of the 38 kHz carrier, while the burst width for a logical "0" is 0.5 ms long; all bursts are separated by a 0.5ms long space interval, see Figure 4.11.

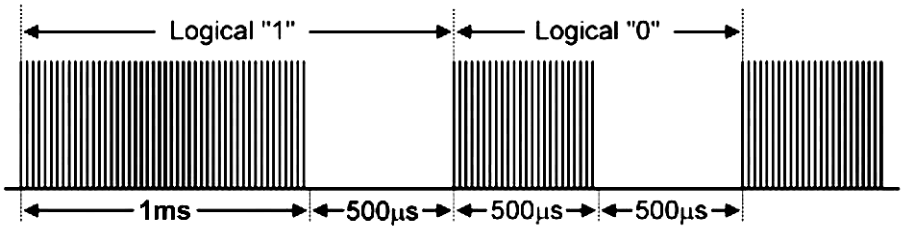


Figure 4.11 Pulse width encoding protocol for IR digital signal transmission.

The start burst is 2 ms wide followed by a standard 0.5 ms off bit. Below is an example of the IR packet. Starting from the “start signal” (2.5 ms), a standard IR packet in our protocol begins with the IR signature bytes (0x6D) and a series of commands (Figure 4.12).

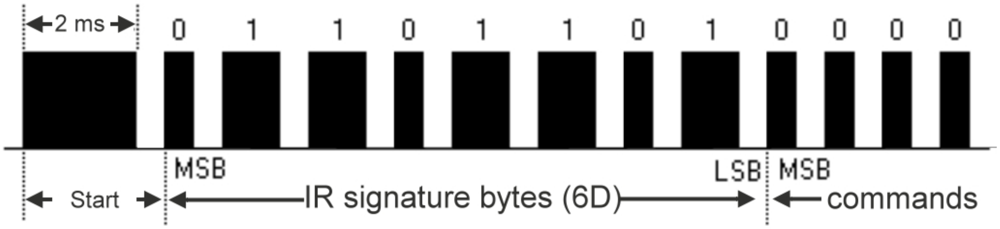


Figure 4.12 A standard IR packet in our protocol.

The table below shows a standard packet in our IR protocol. It starts with the IR signature byte (0x6D), follows by two bytes of node ID, and ends with the IR command and IR button press (if any button press).

IR_SIGNATURE_BYTE	NODE_ADDRESS_MSB	NODE_ADDRESS_LSB	IR_COMMEND	IR_BUTTON_PRESS
0x6D	**MSB of node ID**	**LSB of node ID**	**0x12**	**0x10**

Table 4.2 IR packet protocol.

From the above communication protocols, each USP sensor sense the incoming packets to our server and stores them in a database for later processing via the middleware.

4.2.2 Server Middleware

Middleware is the software that functions as a translation layer between an application on one server and other clients that want to access the application. Here, we use PHP as the middleware between our database (MySQL) and the web interface for our users to edit preferences and browse their information. The middleware processes the webpage, communicates with the file systems and database and then delivers a web page to the web server which is returned to the web browser. Figure 4.13 shows the architecture of our data processing on the server's end.

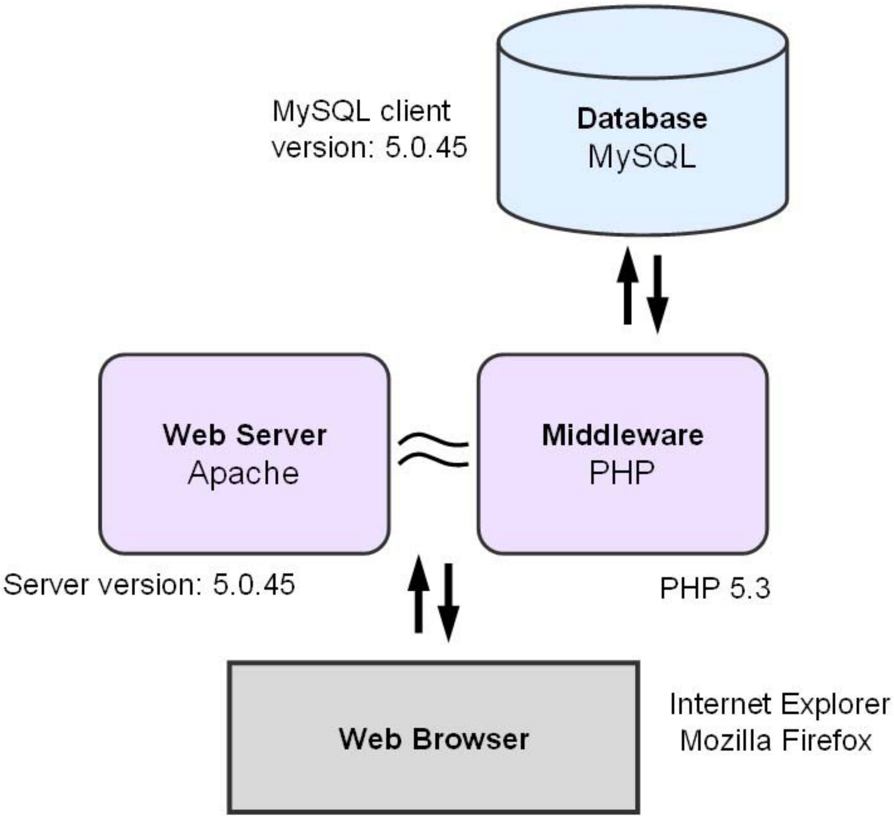


Figure 4.13 Diagrams showing how middleware works.

In the PHP code, we try to read and write into tables in the MySQL database and generate a webpage according to different users. There are four tables in our database for this application: User, Settings, Group, and Links (Figure 4.14). In the sign up page, users write data into the "User" table which uses a primary key to link all the information between different tables. The "Settings" table is used in the sensor setting page, where users can either set "all" or selectively edit the sensor settings by node_id. The "Group" table is for our ongoing experiment – social networking with a dense sensor network. Users can edit how they reveal different information to different group of people. In the “Links” table, the link to recorded images, video, and audio are stored. However, in our pilot user study, no video or audio were recorded; hence, that application is not evaluated here.

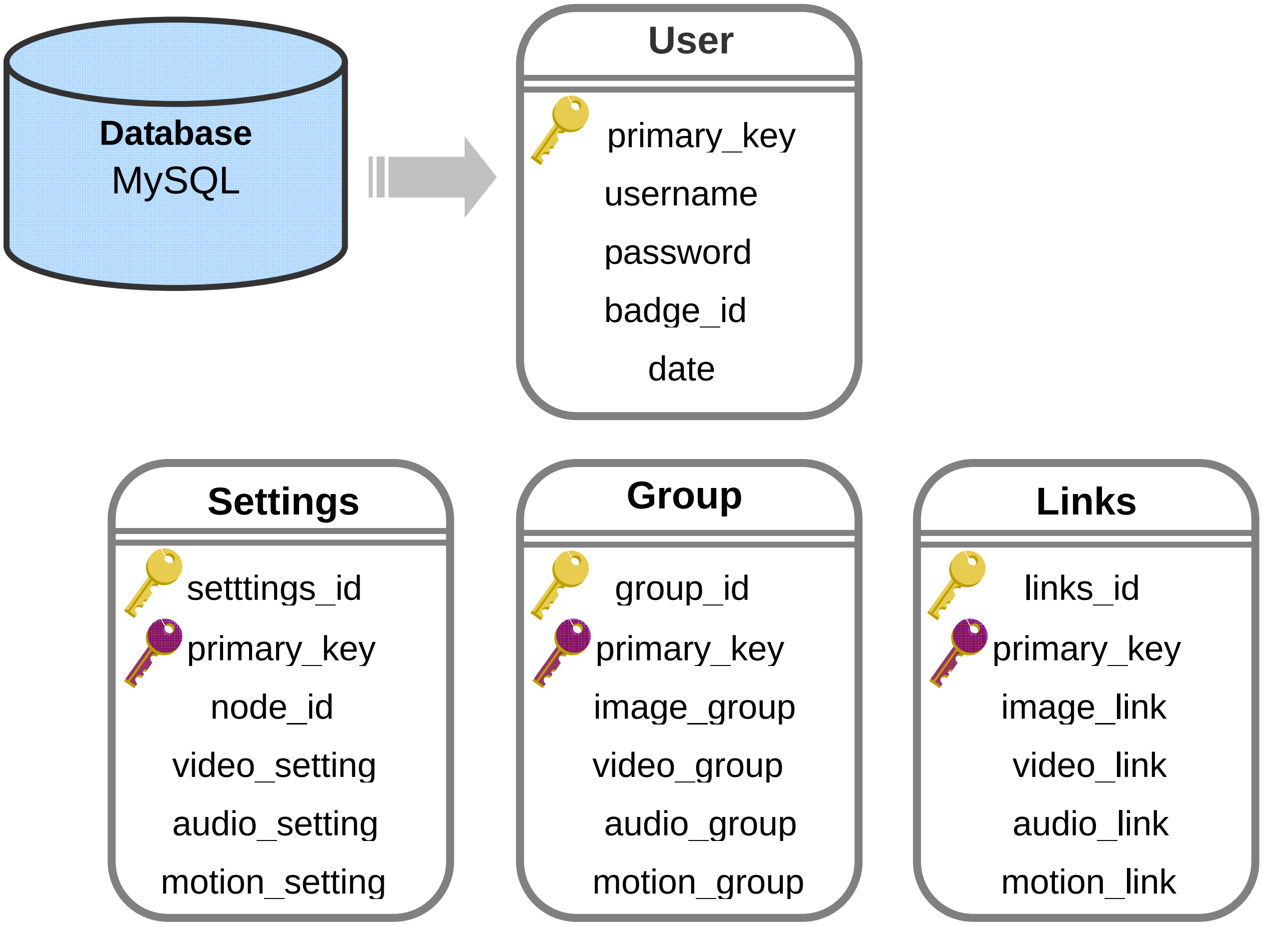


Figure 4.14 Data structure in the MySQL database.

Chapter 5

Evaluation

If the right to privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion.

–William J. Brennan

5.1 Overview

The goal of this evaluation is to study the privacy issue within a ubiquitous computing system through providing a user centric control of personal privacy settings in a sensor rich environment. This result will be used for future references in the design and deployment of pervasive sensor networks. To ask some fundamental questions regarding privacy in a pervasive sensor network, we used an active wearable badge system, a web interface for personal profile settings and a series of questionnaires to conduct this user study. The questions we would like to address are listed below:

1. What system parameters can be adjusted to meet the privacy requests for users working/living in a ubiquitous sensor network environment?
2. To what degree can a preset privacy setting meet users' needs without creating any conflicts between preset privacy and unexpected events?
3. Does cultural / educational background affect the judgments towards one's privacy?
4. What is the most important element (e.g., location, time) for one's privacy requirement?

5.2 User Study Design

We first conducted a one week (June 29th to July 3rd 2009) pilot user study to evaluate the usability and the usefulness of the active privacy badge system. This user study, approve by COUHES (Committee on the Use of Humans as Experimental Subjects) protocol # 0901003071, included 23 users in the media laboratory. The subjects were recruited based on the location of their offices / route with our ubiquitous sensor portal system. Each user was given an active badge, a USB to Mini-USB cable for charging the badge, a pre-experiment questionnaire, and an instruction sheet. The questionnaires and COUHES protocols are listed in Appendices B and C.

5.2.1 Method

Before the user study period, participants were asked to fill out a questionnaire and edit their privacy profile on our web interface. In the pre-experiment questionnaire (Appendix A for COUHES application), a series of questions regarding age, gender, education background, religion and opinions on technology about pervasive sensor networks were asked. The pre-experiment questionnaire was designed to provide ground truth about the users for comparing with their experiment results. Also, the users were asked to draw their everyday route on a floor plan of the Media Lab. The goal was to find some correlation between privacy and one's everyday routing information and discuss which is the most practical approach — preset privacy regions from online settings, privacy badge button presses, physical masking (on/off lamp switch or touch screen commands) – to solve the privacy issues in a ubiquitous sensor network.

During the experimental period, each user was asked to wear a privacy badge during their work time. The badge broadcast its ID every 10 seconds, allowing portals to change settings according to different preferences of each user. This information can be used to track the route of each user and acquire data about the time period they spent in the system.

Since we do not have enough badges for everybody in the Media lab, most occupants were left without a privacy badge. For the purpose of this study, it was important for us to find a way to raise significant privacy risks for our subjects while, at the same time, protect other non-badge users' privacy. Therefore, for this study, we chose not to record video, but only to enable broadcast video from node-to-node. Anyone can use the video tunneling application running on each USP to view the current video streaming from another active USP node. Figure 5.1 shows a demonstration of real-time video streaming during one of our sponsor events.

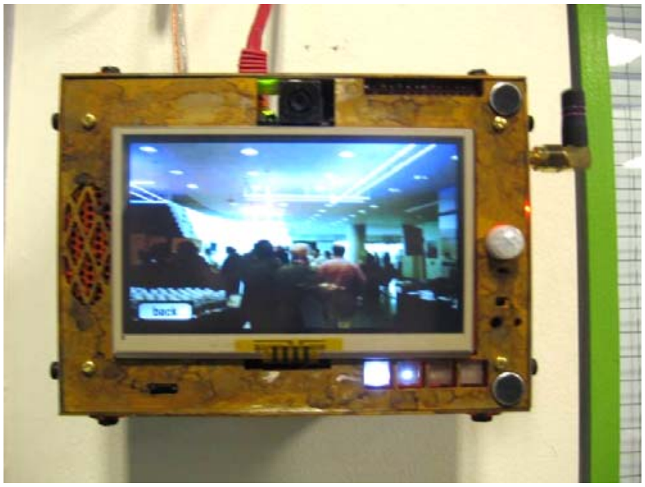


Figure 5.1 Example of real-time video streaming from another node.

Users have three different ways to disable this broadcasting— disabling the USP by cutting its power from a lamp switch, using the privacy badge's blocking button to block data transmission, and using the online setting to automatically disable the streaming at specific locations when nearly. The lamp switch will disable the portal, which can only boot up again when another person turns the switch on again while the privacy button and the pre-setting broadcasting only disable the USPs temporarily (at this point, only for 10 seconds). Participants were informed about the 10 seconds countdown time both from the consent form and the display on the touch screen.

5.2.2 Participant Profile

Twenty-three people volunteered to participate in this study. The recruitment process includes selecting people whose offices are all located on the third floor of the Media Lab, where eighty percent of the portals are located. The participants were mainly graduate and undergraduate students and some staffs / faculties working on the same floor. Of 23 participants, 37.5 percent were female (9 of 24) and 62.5 percent were male (15 of 24), which is very close to the overall gender radio at MIT (1907 of 6146 graduate students were female, 31 percent) [38]. The age distribution has a peak at the 25-30 age group. Of all participants, 29 percent (7 of 24) were between age of 20 to 25, 34 percent (8 of 24) between 25 and 30, 21 percent (5 of 24) between 30 and 35, 8 percent between 35 and 40 (2 of 24), 4 percent between 45 and 50 (1 of 24), and another 4 percent (1 of 24) between 50 and 55 (See Figure 5.2).

More than half (55 percent) of the participants are majoring in Engineering, which again matches the statistics of Engineering major at MIT (For example, 52 percent — 634 of 1217 of all S.B. degrees awarded in 2008 were in Engineering) [38]. 21 percent of the participants have Arts background, 8 percent majored in Humanities, 8 percent had Science background and 8 percent with other backgrounds (Figure 5.3).

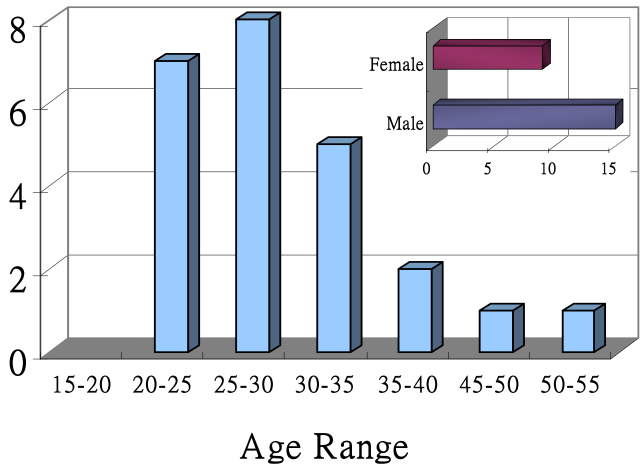


Figure 5.2 Distribution of age and gender of the participants.

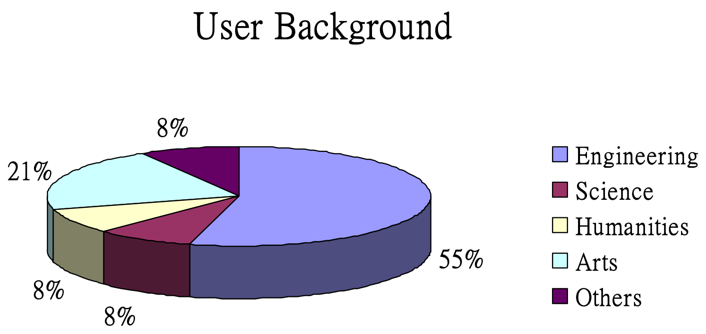


Figure 5.3 Distribution of background of the participants.

One important goal of this user study was to find out whether people who better understand technology care less about their privacy. Here, we tried to find the correlation of background and age with participants' opinions toward technology, and the privacy issue that comes along with the advancement of ubiquitous computing. Accordingly, the pre-questionnaire asked a series of questions about surveillance systems and sensor networks. The results are as follows.

- **Question 1 – The surveillance system on the street is necessary for enriching our safety:**

This question is designed to get a general idea about people's opinion on an existing system – the surveillance system on the street. Unlike the new sensor system we implemented, a surveillance system gives no feedback to the users and it always sparks a huge debate over whether this type of system brings us more good (ensuring the security) than bad (invading people's privacy). Of all 24 participants, 45 percent answered "disagree" or "mostly disagree", 25 percent answered "neutral" and 30 percent answered "mostly agree" or "agree". The result shows a slightly higher percentage towards "mostly disagree" but in general, it appears to be a normal distribution. Note that all of the participants with a Humanities background disagree with this statement (Figure 5.4).

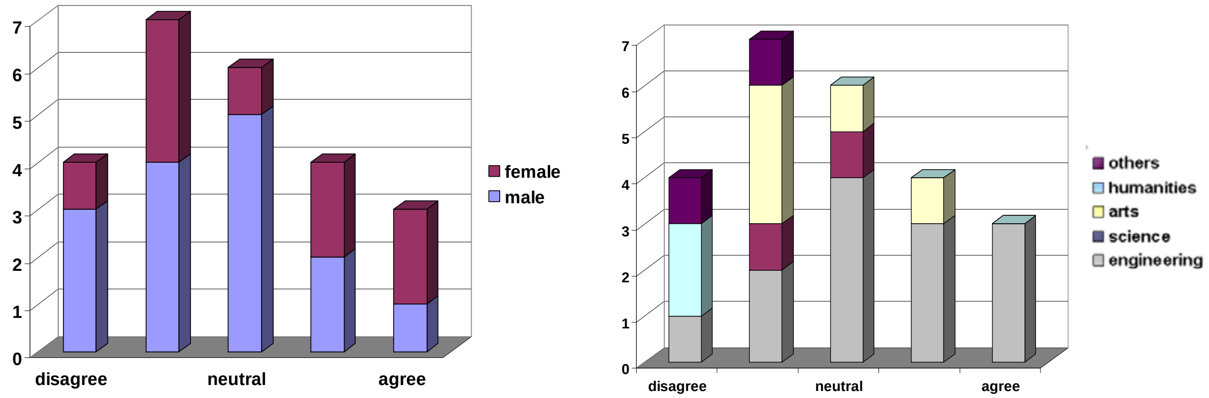


Figure 5.4 Necessity of surveillance systems.

- **Question 2 – A context-aware sensor network is important for enriching our lives:**

A context-aware sensor network built into a smart home / office is meant to collect personal data and automatically adjust to the needs of each individual to enhance their personal comfort (auto lighting, HVAC system for personal temperature and humidity control, etc). Unlike the surveillance system on the street, a context-aware sensor network normally does not involve video and audio data recording. In this question, 38 percent of participants answered "neutral"; 21 percent and 33 percent answered "mostly disagree" and "mostly agree" respectively. Only 4 percent of the participants answered "disagree" and another 4 percent answered "agree". The results indicate that the general opinion toward a context-aware sensor network is rather neutral

(Figure 5.5).

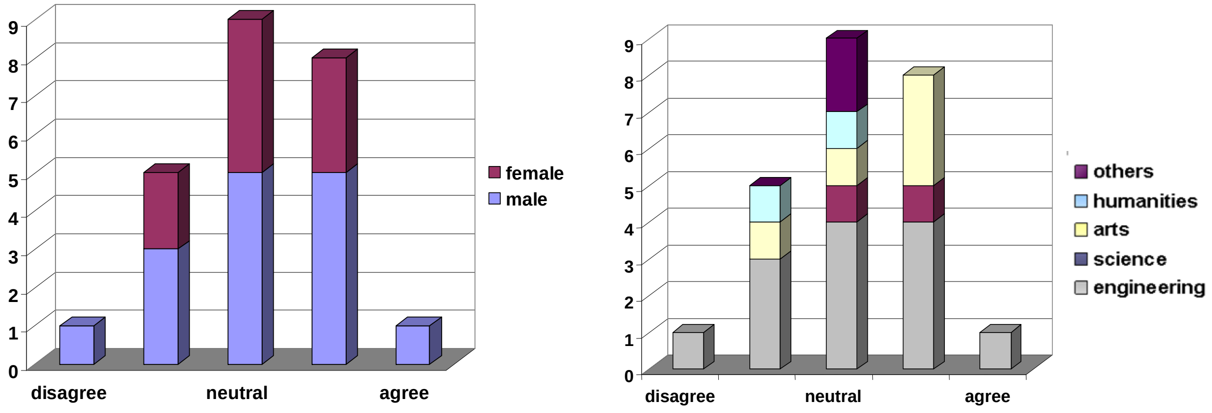


Figure 5.5 Importance of a context aware sensor network.

- **Question 3 – It is important for everyone to have control over their own privacy:**

This question tests the participants' opinion about personal privacy control. None of the participants answered "1" or "2", where "1" is 'disagree" and"2" is "mostly disagree". It is also worth mentioning that almost all female participants (89 percent) and people who are more than 40 years of age answered "5" which is "agree". Overall, 67 percent answered "agree", 25 percent answered "mostly agree" and 8 percent answered "neutral". The results support our assumption about the importance of personal privacy control (Figure 5.6).

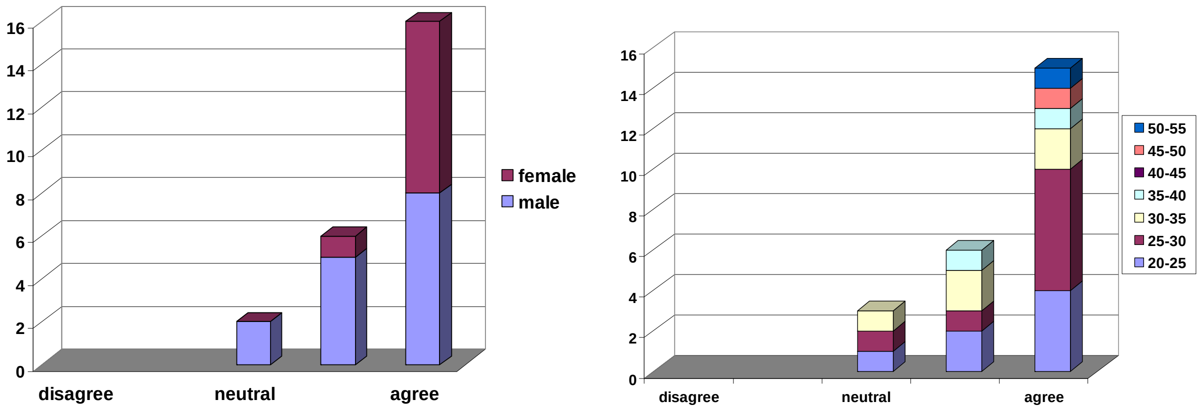


Figure 5.6 Importance of privacy control for each individual.

- **Question 4 –Ubiquitous computing or a sensor system in a building is totally unnecessary:**

The question asks about the necessity of having a sensor network with computational capabilities in a building. 59 percent of participants answered “disagree” or “mostly disagree”, 29 percent answered “neutral” and 12 percent answered “mostly agree” or “agree”. Unlike the neutral results from Question 2, the answers showed that, from our participants’ point of view, a ubiquitous computing sensor system in a building can be necessary.

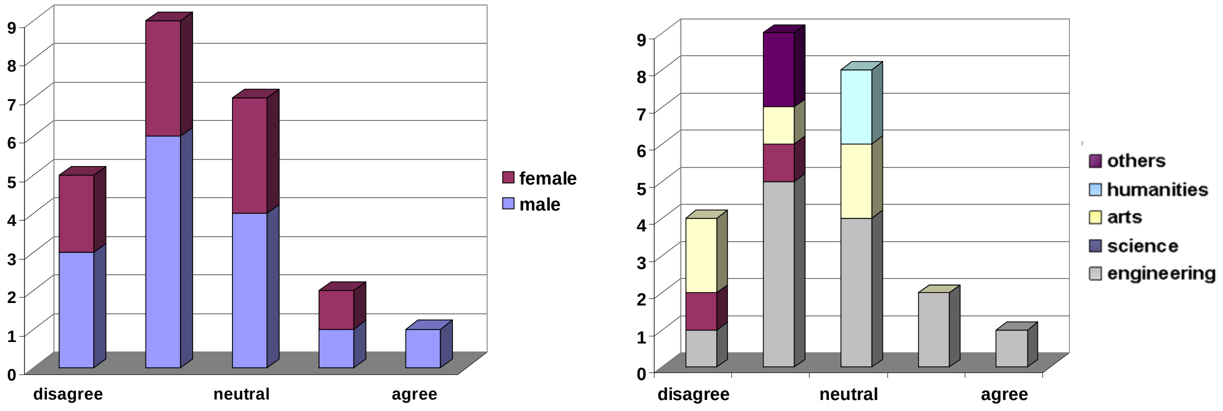


Figure 5.7 Whether ubiquitous computing in a building is necessary.

- **Question 5 – The sensor system in my work place is invading my privacy:**

The participants in this survey were selected because there are sensor portals near their offices. This question is designed to figure out whether our users feel the privacy threat of this sensor network. 13 percent answered “agree” and 25 percent answered “mostly agree” while 8 percent answered “disagree” and 29 percent answered “mostly disagree”. 25 percent of participants answered “neutral”. The interesting part is that the 13 percent of participants who answered “agree” were all female and the 8 percent “disagree” all came from male participants (Figure 5.8). Also, none of the participants with an engineering background answered “agree”. It is noted that gender and background are very important aspects in the study of privacy. One male participant with an engineering background commented on this question:” *The more I know about technology, the more I do not feel threatened.*” Another female participant with Arts background commented on the suggestion page: *“I feel threatened by an unknown electronic device in front of my office.”*

We have discovered that despite the fact that we provided the same information about our system, different backgrounds and the understanding of technology are still the main factors for people to accept a new technology. The strategy for gaining higher acceptance towards new technologies could be developing a good user interface for better understanding (such as the web interface for setting up privacy preferences and post processing the data) and creating a physical object for users' tangible control (such as the privacy badge) over those unfamiliar sensor networks around them. Different interface preferences (lamp switch, button on the touch screen, privacy badge settings and privacy button) are compared in the post-questionnaire.

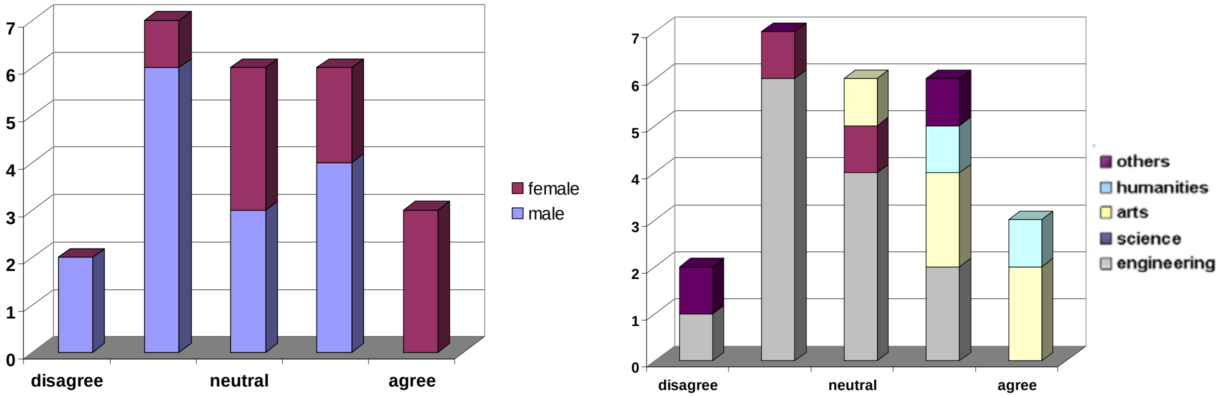


Figure 5.8 Whether sensor system near their work place is invading their privacy.

- **Question 6 – I enjoy technology. For example, the smart phone with a high resolution camera and a voice recognition system:**

In question 6 and 7, we tried to ask the same question in a different way. Question 6 asked the participants about their acceptance of the advancement of the latest electronic devices' capabilities, whereas question 7 asked a more general question about the acceptance of the advancement of new technology in multimedia. A smart phone with a high resolution camera and voice recognition system is almost the standard cell phone spec nowadays. However, only 25 percent of participants answered "agree" while 4 percent answered "disagree". 63 percent answered "mostly agree" and the rest, 8 percent, answered "neutral". On the other hand, when people are asked about their opinions on the advancement of new technology in multimedia (Question 7), 54 percent agreed it is enjoyable by answering "agree", 38 percent answered "mostly agree" and again, the rest, 8 percent, answered "neutral".

The result showed that most people hold a positive perspective over a new multimedia technology; however, the way we present the technology and the information we gather from our users can greatly influence the acceptance of a new electronic device among different groups.

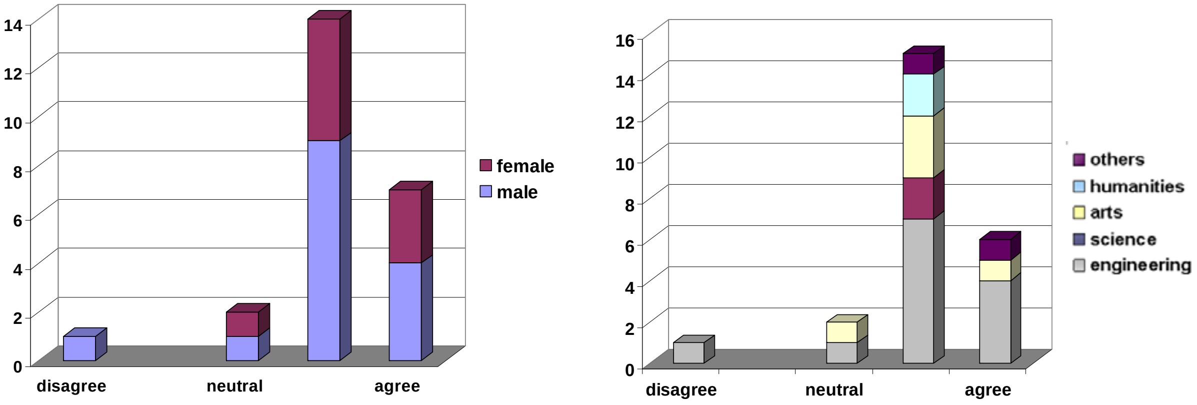


Figure 5.9 Whether high resolution camera and voice recognition on cell phone is necessary.

- **Question 7 – I enjoy experiencing the advancement of new technology in multimedia:**

As described above, most participants showed a strong interested in experiencing the advancement of new technology in multimedia. The difference between Question 6 and 7 is that, we described a new technology in Question 6 with components that can not only be used as an interactive tool in multimedia, but also can be a potential threat to users' privacy.

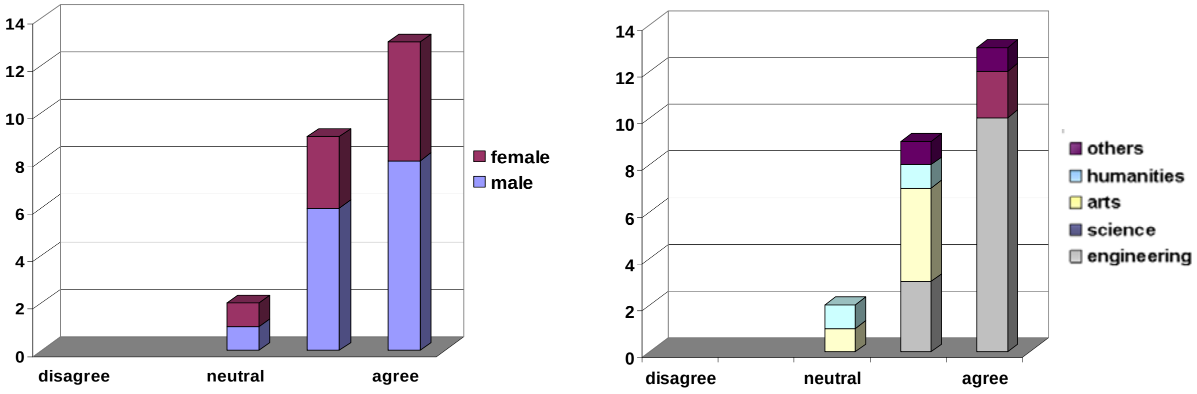


Figure 5.10 Whether the user enjoys the advancement of new multimedia technology.

The information we gathered from this pre-experiment questionnaire gave us a basic knowledge of our user group. It is worth mentioning that although we tried to recruit a diverse user group and did match the users' profiles with the background, gender and age distribution with the institute, MIT is a biased environment with a very high acceptance of new inventions and the users are most likely with an above average knowledge toward technology than the general public.

5.2.3 Participant Routing Information

Besides the pre-questionnaire questions, the participants were also asked to draw their everyday route so we can clarify the usage of each portal in different locations. An example of the routing information provided from one of our users is shown below in Figure 5.11.

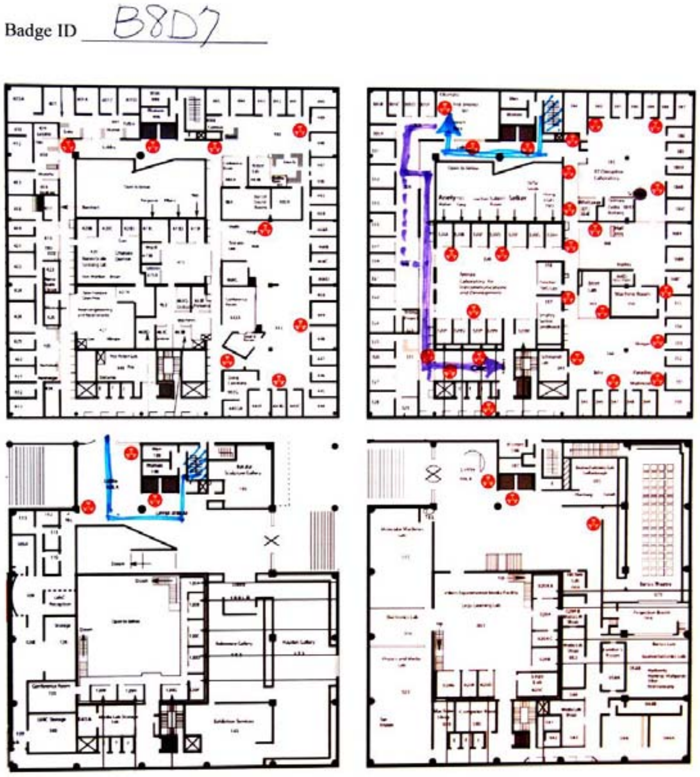


Figure 5.11 The everyday routing information provided by one user.

The assumption we had here was that there are two spots that most likely create the highest privacy risks – the common areas and the space in front of one's office. We will use this information to compare with the result we get from our participants' privacy settings on-line and their usage of the on-site control from the privacy badge.

With the routing information of each user, we can roughly derive the potential privacy threat of each portal from the overlap in the percentage of routing counts from all of our users. One example is the portal in front of the 3rd floor elevator. This portal overlapped with every user's routing choices. Therefore, the percentage of overlap here count is 100 percent. Figure 5.12 shows the routing selection of every user on the 3rd floor of the Media Laboratory. The number near each portal indicates the number of users' working areas near that portal. The orange boxes on each figure highlight the working space of the users whose routes are depicted in the figure.

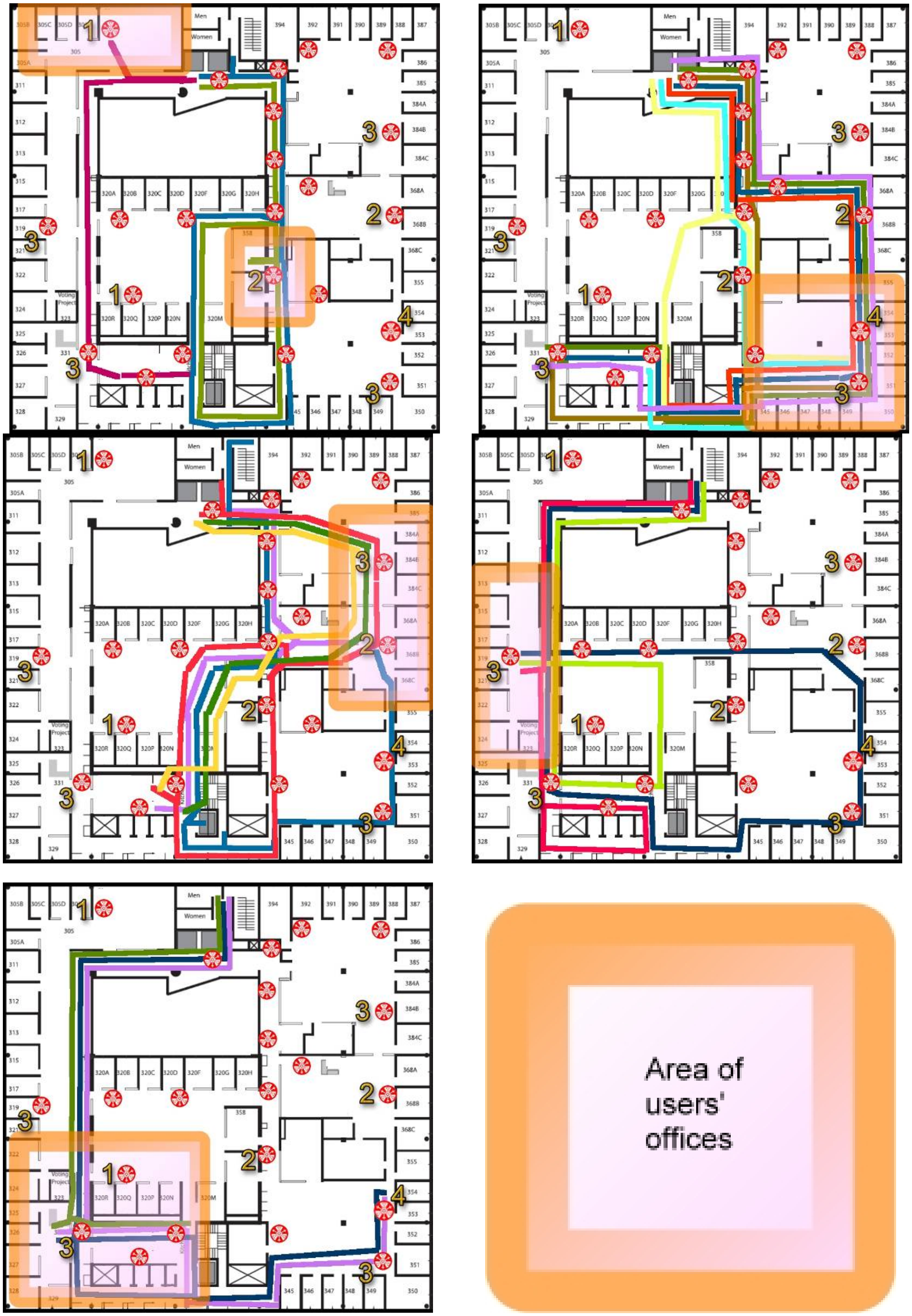


Figure 5.12 The everyday routing information provided by every user on the 3rd floor. The five

plots show five different office areas and the routing information of users from those areas.

From the information above, we can derive the most frequently visited spots that overlap with a portal, as shown in Figure 5.13. The percentage is indicated both by the size and color of each circle. The ones that have lower percentage counts are clearly the ones in front of offices and the one's that have higher counts are in the common areas such as the kitchen and the elevator.

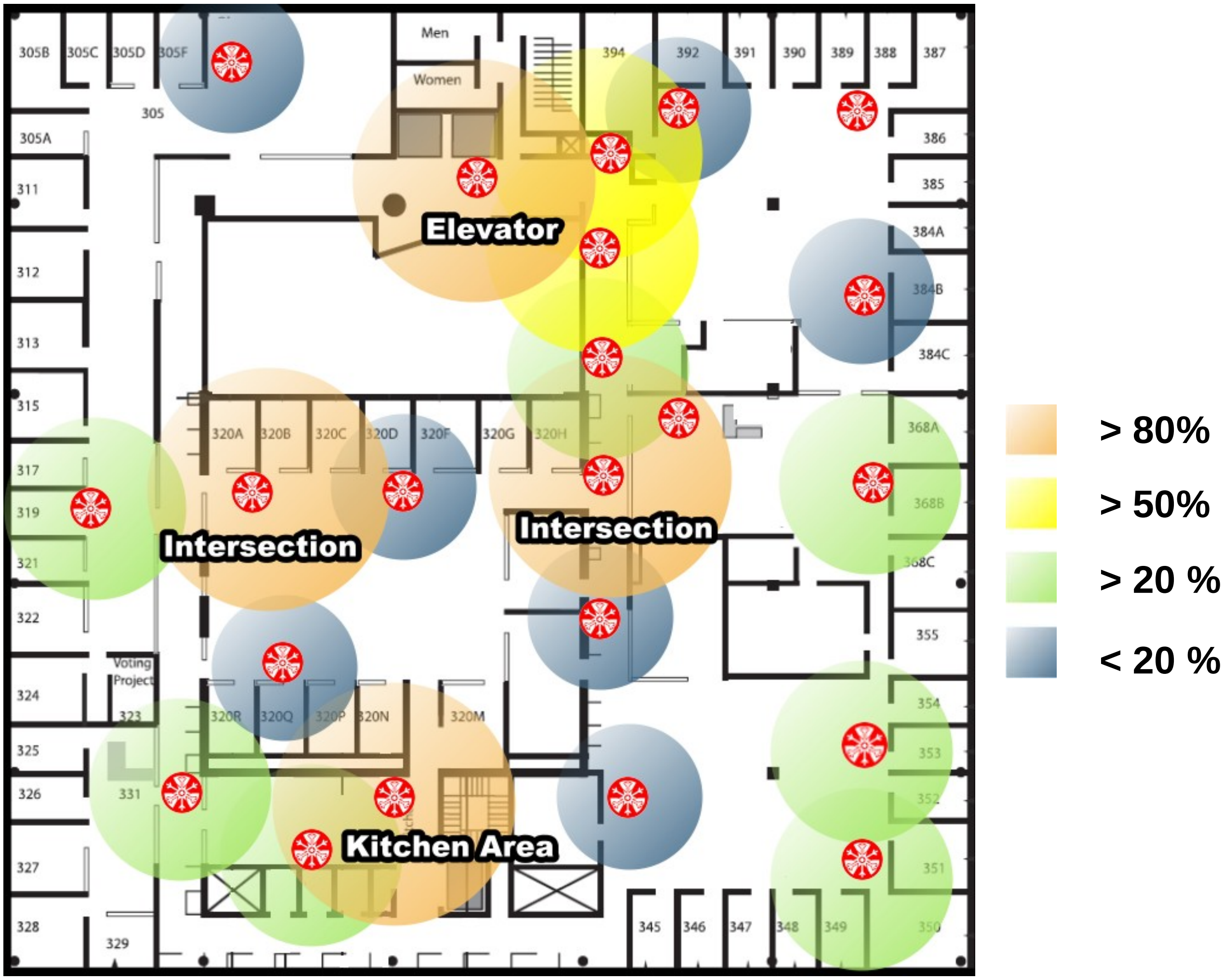


Figure 5.13 Overall percentage counts from the daily routing provided by 24 participants. Note that the most frequent visited areas are the common areas – elevator, kitchen area, and two intersections connecting offices to the major path.

5.2.4 User Study Results

The one week user study ran from Jun 29th to July 3rd. However, only four days of data will be discussed in this section due to the lack of our subjects' presence on July 3rd (due to the Independence Day holiday). From our data, we tried to derive the usage of each privacy protection method, and its effect on the overall system. This information can not only help us to evaluate the usability and acceptance of each privacy protection method in a ubiquitous computing sensor network, but also extrapolate the effect of using each method on a larger sampling of users. In this section, we start from the results of on-site button presses, then compare with the online preset privacy and, in the end, demonstrate the overall system effect from the use of a privacy-protecting active badge system.

In Figure 5.14, we see a normal distribution of the button press from active badge users where the peak is around 2-3 PM. The button press count per day was 80, 67, 63 and 73, from day 1 to 4 respectively. The average number of button press per day was 70.75, 2.95 button presses per user per day.

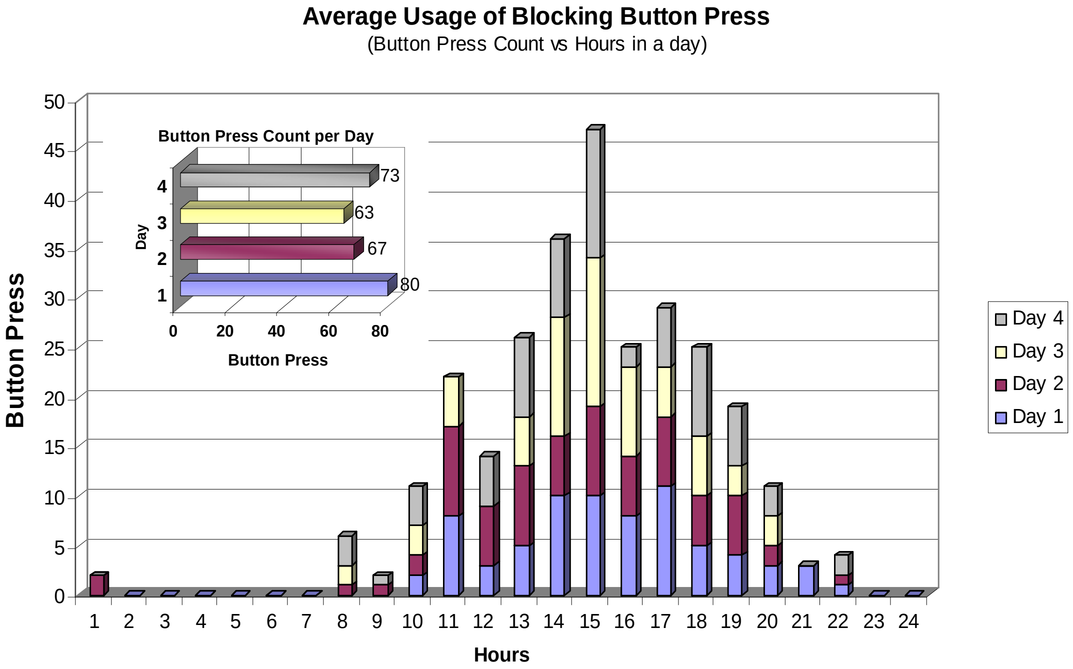


Figure 5.14 Average usage of the blocking button on privacy badges. The upper left figure shows the count of button presses from 23 users everyday.

Again, the users only press the privacy button when there is a conflict between the location-specified privacy of their online settings and the location of an unexpected private event (or if the private event is significant enough that participants wanted to be guaranteed).

We tried to analyze the correlation of the average number of active users versus button presses to see if the peak in Figure 5.14 was only the indication of more badge users in the building. Figure 5.15 is the plot of average number of active user over time calculated from the RF broadcast beacon log file during the test period. Unlike Figure 5.14, it has a smooth slope over time indicating that the peak of button presses has little to do with the population of badge users at that time.

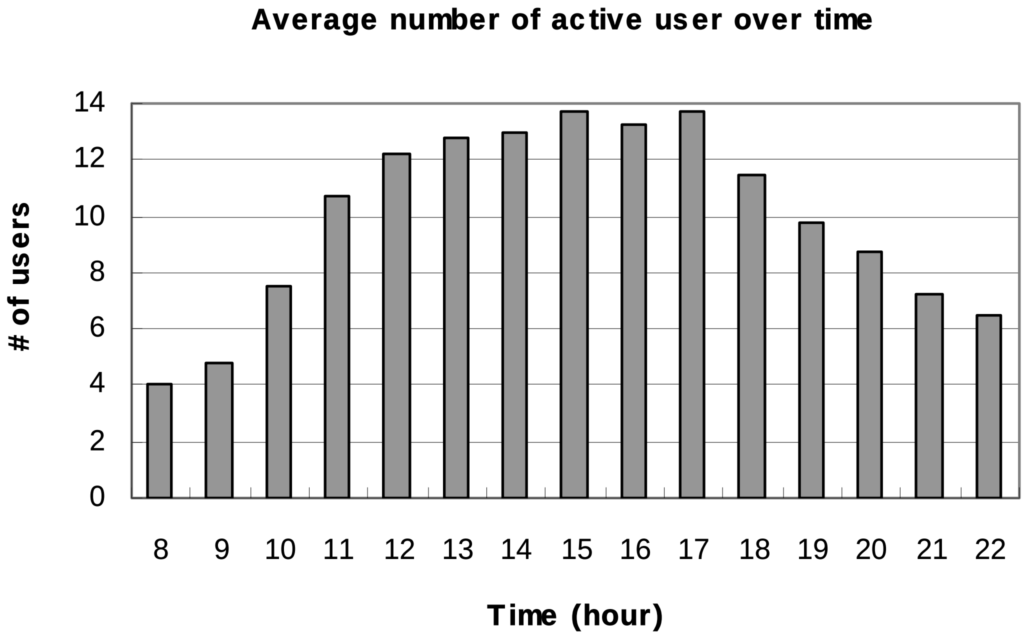


Figure 5.15 Average number of active user over time.

In Figure 5.16, we used the average button press count divided with the average number of users at that time to derive the more meaningful quantity of average button presses per user. This plot has the same characteristics as Figure 5.14 with a peak around 2-3 PM, proving that the average number of active badge user is not positively correlated to the button presses count. The peak may correlate with morning break (10-11 AM), afternoon break / lunch (2-3 PM) with broad tail late into the afternoon when more social interaction is exercised.

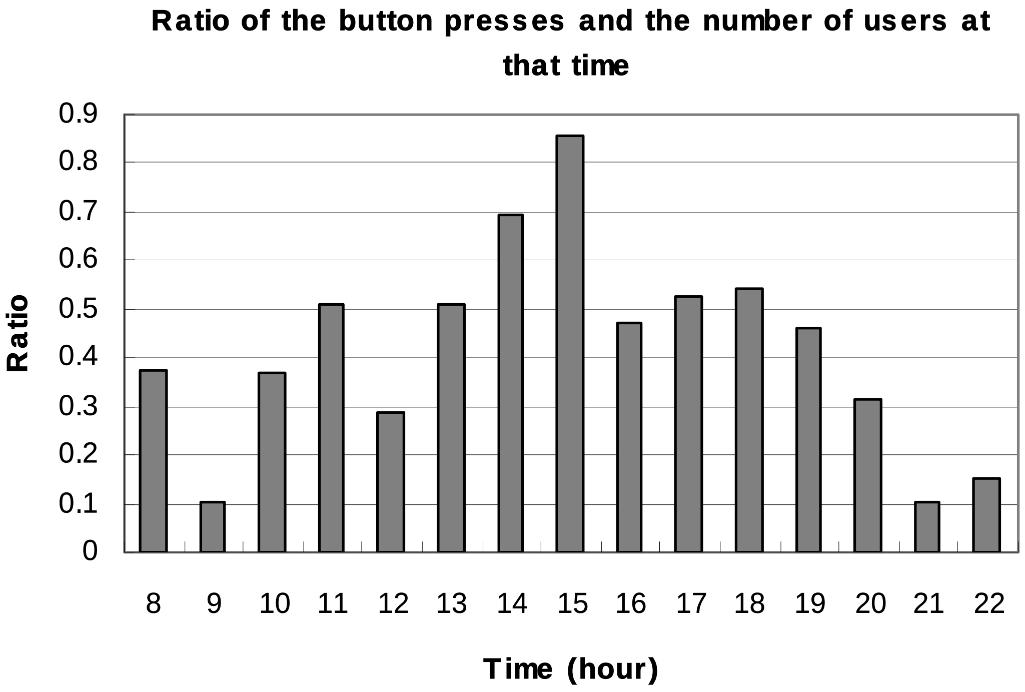


Figure 5.16 Ratio of button presses and the number of users at that time.

Figure 5.17 is a visualization of the location of button presses during the test period. The difference between Figure 5.17 and Figure 5.13 is that, unlike the privacy risk from our estimation via users daily route, people press the privacy button less in the common area (the kitchen area) and more in front of offices (for example, in front of office 319 and 351). A good explanation is that most people set up online the most strict privacy preference (block all sensor signal transmissions) in the kitchen area where most social conversation takes place. Therefore, fewer conflicts occurred in that area, resulting in fewer button press counts. The RF range of each badge is around 10 to 20 meters in the line of sight and about 5 meters after attenuating from a barrier such as a wall or a door.

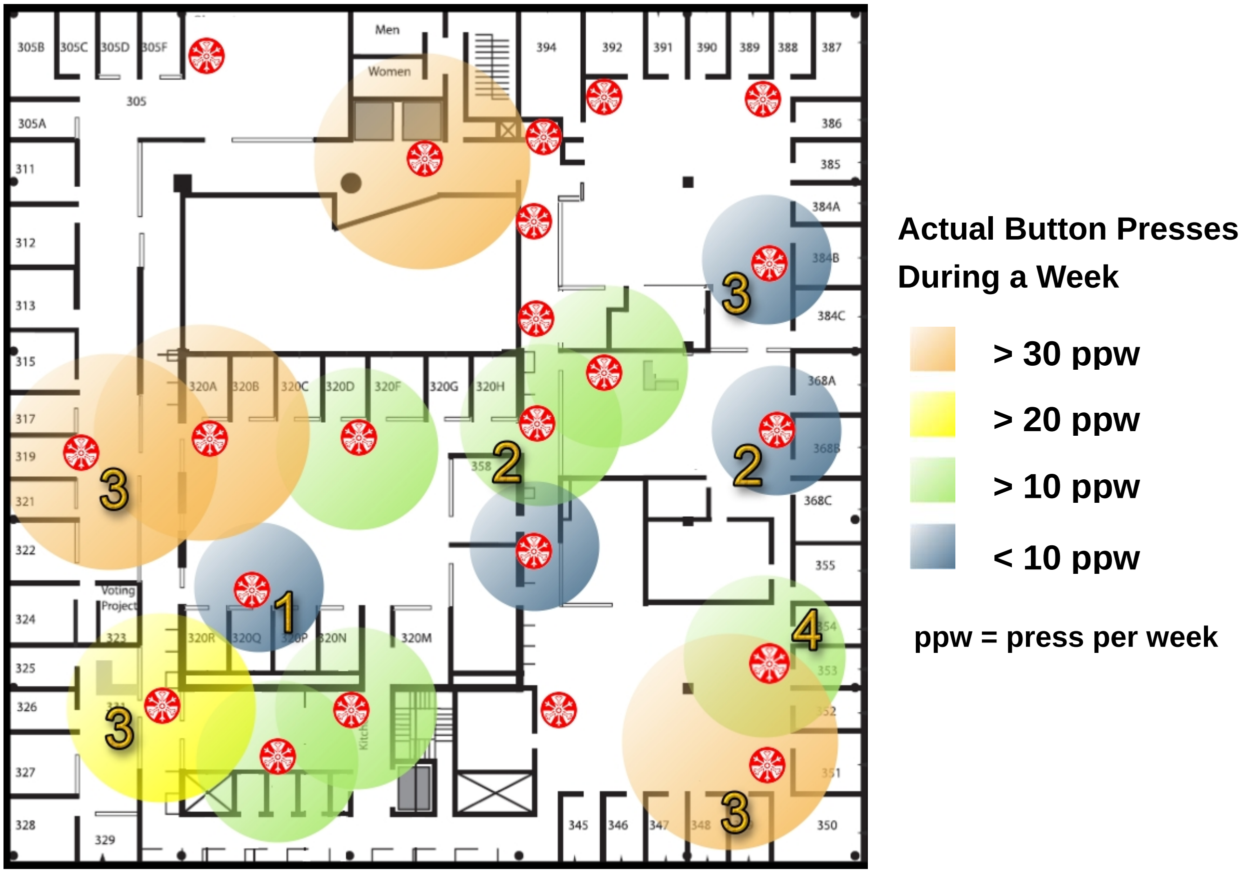


Figure 5.17 Visualization of button presses vs. location. Note the difference in the locations counts vs. Figure 5.13 could be derived from the online privacy setting.

We tried to verify the above assumption from looking into our users' online settings. From the database, we observed that of all 24 users, 17 set up their privacy through the "edit all sensors" page that can set up sensor preferences from all nodes at once. The results are as follows (Figure 5.18): 70 percent of participants set up their privacy preferences at once, 66 percent of all participants block all video transmission through the active badge, and 50 percent set all audio off, whereas only 34 percent set all motion sensors off. As for the privacy settings on individual nodes, 50 percent of all participants set up individual privacy on a location basis, 33 percent turned off the video recording / broadcasting on their daily route, another 17 percent disabled both video and audio, merely 4 percent disabled the motion sensor, and the remaining 8 percent did not set up preferences from this page.

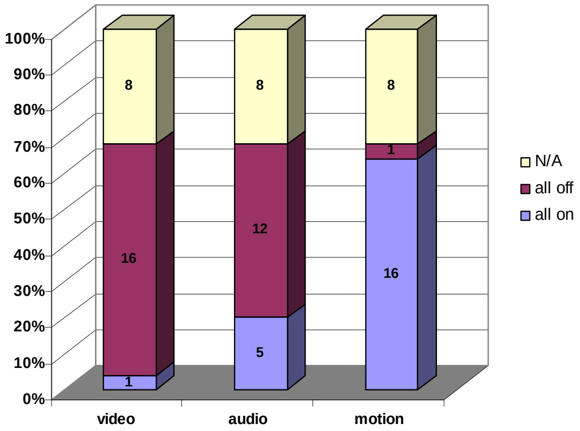


Figure 5.18 The percentage of users that chose to block each sensor from the broadcasting of their active privacy badge.

There are indeed users that set up a general rule for their overall privacy and then modify the settings at different locations. We looked into the kitchen area, where the differences between privacy button presses and our privacy risk estimation were the greatest. Of all 24 users, 12 people set up their privacy in the kitchen area separately. Along with the users with overall blanket sensor settings, the following figure shows the privacy preferences for all users in the kitchen area. 79.17 percent of participants turned off video transmission and 83.33 percent turned off audio. In contrast, 87.50 percent of users agreed to have the motion sensors on (Figure 5.19).

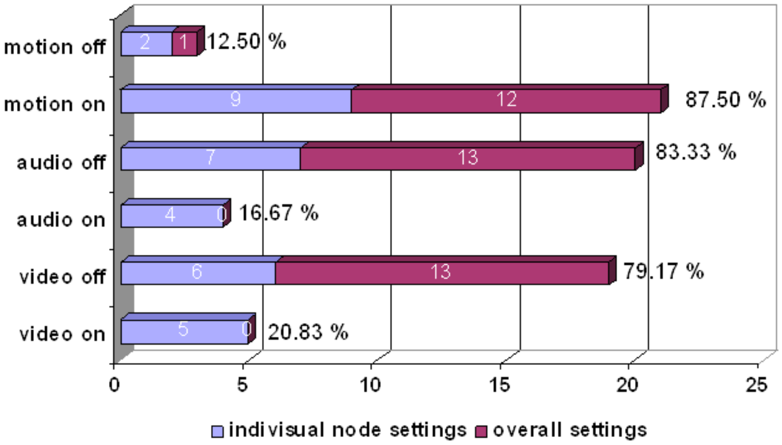


Figure 5.19 online pre-set sensor preferences for nodes in the kitchen area.

The results here are in accordance with Reynolds and Wren's [8-9] work on the ethical implications of choosing camera networks vs. infrared motion detector networks – motion sensors, though could also be used as a tracking device, creating less threat to privacy. Although we built the active badge system to solve the privacy issue on different occasions, to gain a balance between maintaining the full function of a ubiquitous interactive sensor network while preserving users' privacy in every way is still an unsolved issue.

The example above shows most of the time, the video and audio will be turned off by broadcasting from privacy badges. However, the essence of ubiquitous interactive media relies mostly on an abundance of video and audio capturing. Therefore, we tried to analyze the whole system availability from observing the percentage of portals that are blocked over time, and extrapolate from the data what the system availability would be to if everybody in the building had these badges. Figure 5.20 shows the average percentage of disabled portal units in a one day time scale. We counted the number of portals that had been turned off either by users' button presses or by the user that broadcast "block all sensors" every 10 minutes. The 4 day results are then averaged and plotted versus time. The average percentage of blocked portals is 8.06 percent.

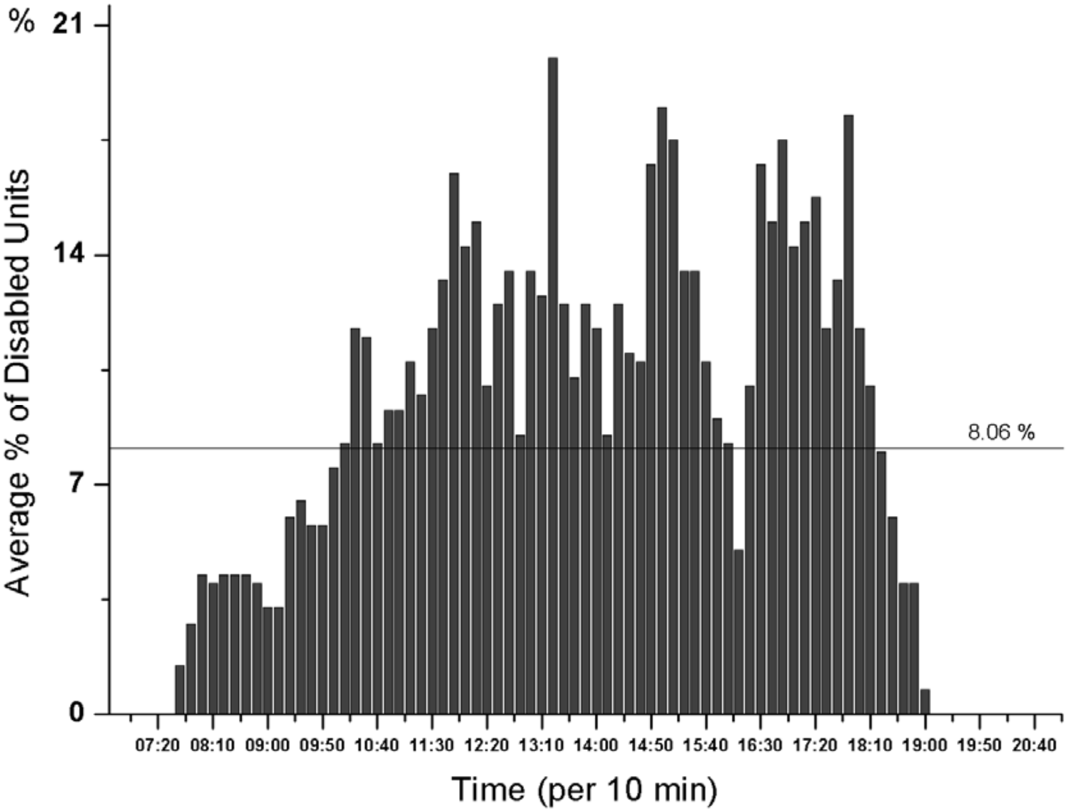


Figure 5.20 Average percentages of disabled portals over time. The average percentage of disabled portals is 8.06 percent.

In this user study, we recruited 24 users on the 3rd floor which usually accommodates around 90 people. In other words, 27 percent of occupants from the 3rd floor joined this study and this 27 percent population disabled an average of 8.06 percent portals' sensor transmission during this period. What this tells us is that if we give everyone in the lab an active badge system, an average of 29.81 percent portals will be disabled at all times. We can also conclude from the peak of Figure 5.18 that there could be times (a half hour to an hour) that a lab-wide active badge system would automatically disable more than half of the portals.

This evaluation proved that an active badge system has potential to shut down half of the network in our setting through preset privacy broadcasting, whereas as button presses mechanism only blocks the system for ten seconds allowing the network to run more smoothly. More discussion about the comparison between different privacy protection mechanisms will be provided in the next chapter.

5.2.5 Post-experiment Questionnaire

After the evaluation period, each user was asked to complete a post-experiment questionnaire. The questionnaire asked about the usability of this system and the acceptance of different privacy protection mechanisms.

- **Question 1: Do you feel in control of your privacy with the badge?**

Of all users, 59 percent answered “strongly agree” or “mostly agree”, 17 percent answered “neutral”, and 25 percent answered “mostly disagree” (Figure 5.21(a)). The results showed that although more than half of the users answered “agree”, some users still answered “mostly disagree”. From some of our users’ feedback, we found that the reason they felt they have no control with the badge is because of the lack of interaction between the user and the badge. The reason we did not include full interactive functionality in the badges is due to power issues. In this pilot study, we broadcast a RF signal every 10 seconds, which consumes ~30 mA constantly. Although the processor goes to sleep mode in between broadcasts, the battery still can not last more than three or four days without recharging. In order to prolong the battery life in cases where the users forget to charge the battery, we minimized functionality for the pilot testing. This problem can be addressed by increasing the broadcast interval or using a higher mAh battery.

- **Question 2: Is the badge effective enough to protect your privacy when needed?**

54 percent of users answered “strongly agree” or “mostly agree”, 33 percent answered “neutral”, and 13 percent answered “mostly disagree” (Figure 5.21(b)). Most of the users agree that the badge can protect their privacy when needed; however, some users commented that sometimes it is too late to press the privacy button when a private incident occurs. The problem can be improved by the on-line post processing function that we are currently developing. As long as the users can use their badge to tag the information that we recorded, it is possible for them to access that information and edit or delete anything that is related to them.

- **Question 3: Is the design intuitive to use?**

In this question, 71% of participants answered”strongly agree” or “mostly agree”, 42 percent answered “neutral”, and 8 percent answered “strongly disagree” or “mostly disagree” (Figure 5.21 (c)). The reason that 8 percent of participants were confused by the badge could be caused by the LEDs for Zigbee connection indication. The small orange LED connected to the GPIO pin on the Zigbee chip lights up whenever the badge is out of the network. Therefore, some users whose offices are at the edge of portals’ radio coverage got a lot of confusing LED blinking, causing the confusion of their usage. This can be improved through changing the firmware. Another problem is that, in order to save battery power, we programmed the badge like any other Zigbee battery-powered device – the processor goes to sleep mode most of the times. However, this gives no feedback for the users about whether the system is still alive or not. A possible solution is to add a dim but noticeable LED on the battery analog circuit for better indication of the badge power status. Also, there is no direct indication about what the four LEDs represent. In our next design iteration, we will add stickers on the case for users’ better understanding of the function of each LED or just use a low-power LCD with graphic icons.

- **Question 4: Is the web interface easy to use?**

63 percent of users answered “strongly agree” or “mostly agree”, 25 percent “neutral”, and 13 percent answered “mostly disagree” (Figure 5.21(d)). Most users commented that the overall interface is easy to use, but there is not a page where the user can get an overview about all the current settings they have. Some think that there should only be one page for all the sensor settings. Therefore, our next design will include better feedback about the current privacy setting status and complete the ongoing group dynamic application as well as the post-processing options.

- **Question 5: Do you think a web-based privacy setting is a good way to control privacy?**

Of all 24 users, 67 percent answered “strongly agree” or “mostly agree”, 17 percent “neutral”, and 17 percent answered “mostly disagree” or “strongly disagree”. (Figure 5.21(e)). The users that disagreed suggested that there are too many options on the web interface and all they want is an on-site control and the post-processing page. However, most users choose the privacy badge web-based setting as the approach that best suit their need for privacy control. Figure 5.21 (f) is the result when users were asked about which approach (users can have multiple options) can better suit their need for privacy control. 40 percent answered “online privacy settings”, 33 percent answered “on-site badge control” and another 19 and 8 percent answered “button on the touch screen” and “lamp switch” respectively.

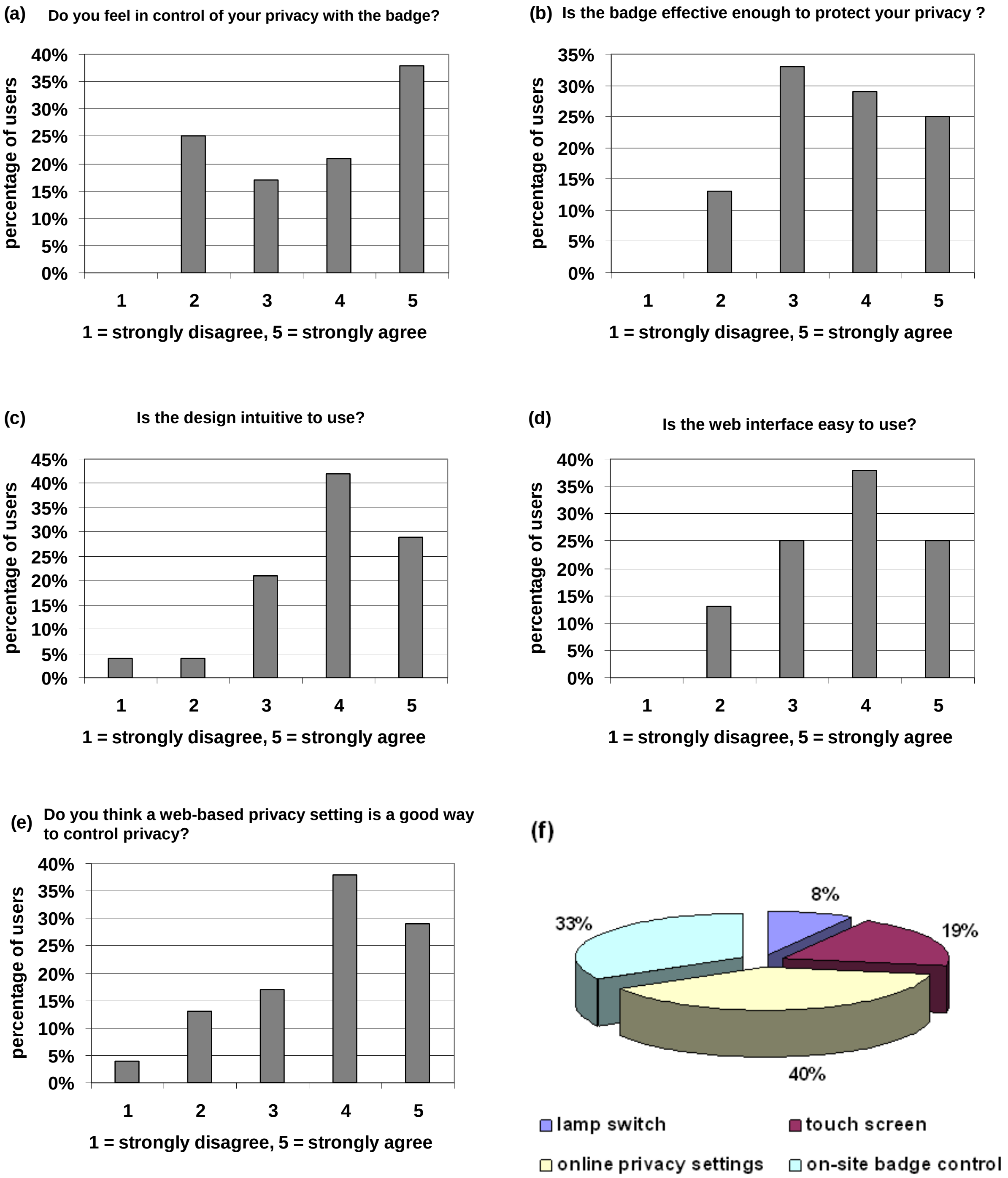


Figure 5.21 The results of post-experiment questionnaire.

Surprisingly, although a button on the touch screen for disabling the portals is not included in this user study, 19 percent of users think it is necessary to have a way to temporarily disable the portals without having to shut down the system from a lamp switch. This approach is especially useful for people without or who forget to bring a badge.

In conclusion, from our user study, we explored different possibilities of privacy protection in a ubiquitous computing environment. We also learned from the users' feedback about the shortcomings in the system design. More details about the conclusion and future work are further discussed in Chapter 6.

Chapter 6

Conclusions and Future Work

Although only a few may originate a policy, we are all able to judge it.

–Pericles of Athens

6.1 Summary

In this thesis, we presented multiple approaches for personal privacy management in ubiquitous sensor networks via an active badge system. The approaches include a badge for on-site privacy control through button presses or periodically broadcast RF beacons, a web interface for editing sensor preferences and post-processing the recorded information, and a physical method such as shutting off the power on each sensor unit from a lamp switch or locally disabling the portals from a button on the touch screen. In the pilot user study, we evaluated the usability of each method and the possibility of using this system as a building-wide privacy protecting facility. Our results indicated that the active badge for on-site control is the most effective and acceptable method among all, especially the periodically broadcast RF beacon for privacy control. However, several results also suggested that if every occupant in the building uses this approach to block data transmission in their vicinity, almost 30 percent of portals will be disabled. Therefore, it is crucial to find a balance between protecting users' privacy and maintaining enough data flow at the same time.

6.2 Discussion

To solve the problem where over-protected privacy may paralyze the full function of our ubiquitous interactive sensor network, we propose the following approaches:

1. Protecting users' privacy while maintaining enough data flow in the network through de-identifying portions of the data. For example, use a facial recognition or detection algorithm to blur faces instead of blocking all video transmission. Likewise, audio signals can be processed leaving no recognizable content in the recording.
2. A voting system can be introduced so that the privacy broadcasting can represent group consent. At the top of the hierarchy is still the button press but the preset privacy can be changed by the majority of users in the same area. Users will be notified if their settings are overwritten through the portals and the output devices on their badge.
3. To get maximum users interacting via the network, the portals should be able to maintain full function when there is a highly proximate person using the applications. Meanwhile, we can adjust the microphone sensitivity to confine the area of recording / broadcasting real-time audio.
4. In the revised portal system being designed now, a link quality index should be included to give more precise location information of the user. In the current system, the RF beacon can travel to several portals, blocking data transmission on multiple nodes. Therefore, with a better location engine, we can decrease the percentage of disabled units.

6.3 Future Work

Besides the approaches discussed in the above section, there is still room for improvements in the design of user interfaces based on the feedbacks from our users. A first step would be adding better indication on the feedback of the badges (such as different color LEDs for different privacy status or an iconic LCD display). In addition, developing a second iteration of the hardware for scaling down its size and power consumption can be advantageous.

Also, applications on the USPs that can involve more people in using this system for interaction would give us results to compare with the pilot study in this thesis. It would be interesting to see whether people will have higher acceptance of an interactive sensor network when there is more incentive to use the system for their own purposes (e.g. social networking, entertainment, ambient information and self-documentation applications that are now being developed). The system can also be developed as a location-based social networking platform. As suggested in chapter 3, for example, people can use the active badge to document and selectively share their lives with their friends and invite others in the same building via the USPs to join their social network.

Another user study should be conducted after the SPINNER/USP network is fully deployed when real-time multimedia is streamed and recorded over the network. Although there are always debates about privacy and personal information disclosure, millions of people are still uploading their pictures and videos online everyday. A study about personal blogging that shares narrative clips versus privacy control in pervasive sensing environment would be a major contribution to the field of privacy research in ubiquitous computing. In the end, the system, as constructed, is very fragile and can be hacked or defeated at many levels. For the system to be really used and trusted, protocol, software, and hardware need to be "hardened" against attack in order to get an acceptable level of security.

Bibliography

[1] D. Lyon, “The electronic eye: The rise of surveillance society ,“ 1994

[2] M.Laibowitz, N.-W. Gong, and J. A. Paradiso, “Wearable Sensing for Dynamic Management of Dense Ubiquitous Media,” Proc. 6th International Workshop on Body Sensor Networks (BSN09), IEEE CS Press, 2009, pp3-8.

[3] M.Laibowitz, “Distributed Narrative Extraction Using Wearable and Imaging Sensor Networks,” Ph.D. Thesis, MIT Media Lab, expected September 2009

[4] USP system introduction. http://www.media.mit.edu/resenv/portals/

[5] Ortmann, S., Langendörfer, P., Maaser, M, “A Self-Configuring Privacy Management Architecture for Pervasive Systems,” In: 5-th ACM International Workshop on Mobility Management and Wireless Access, Chania, Crete Island, Greece, 2007

[6] Moncrieff, S., Venkatesh, S., Andwest, G.. “Dynamic privacy in a smart house environment,” In Proceedings of the IEEE International Conference on Multimedia and Expo. IEEE Computer Society, 2034-2037, 2007

[7] http://en.wikipedia.org/wiki/Privacy

[8] E. Munguia Tapia, S. S. Intille, L. Lopez, and K. Larson, “The design of a portable kit of wireless sensors for naturalistic data collection,” In Proceedings of PERVASIVE 06. Berlin: Springer-Verlag, 2006.

[9] http://wiki.media.mit.edu/view/Necsys/FoodCam

[10]D. Olguin Olguin, J. A. Paradiso, and A. Pentland, “Wearable communicator badge: Designing a new platform for revealing organizational dynamics,” in Proc. 10th Int. Symp. Wearable Comput. (Student Colloq.), Oct. 2006, pp. 4–6.

[11] G-speak http://oblong.com/

[12] Nadav Aharony, “Virtual Private Milieus: Sharing Our Digital Aura through Social and Physical Proximity,” MS thesis, MIT Media Laboratory, 2008

[13] F Stajano, “Security for ubiquitous computing,” 2002

[14] BELLOTTI, V. AND SELLEN, A, “Design for privacy in ubiquitous computing environments,” In Proceedings of the 3rd European Conference on Computer-Supported Cooperative Work (ECSCW'93). Kluwer Academic Publishers, Norwell, MA, 77-92, 1993.

[15] J. I. Hong and J. A. Landay, “An Architecture for Privacy-Sensitive Ubiquitous Computing,” In MobiSys, 2004.

[16] R. Campbell, J. Al-Muhtadi, P. Naldurg, G. Sampemane1, and M. D. Mickunas, “Towards security and privacy for pervasive computing,” In Proceedings of International Symposium on Software Security, Tokyo, Japan, 2002.

[17]Beresford, A. and F. Stajano, “Location Privacy in Pervasive Computing,” IEEE Pervasive Computing, vol. 2(1): pp. 46-55,2003.

[18] A. Madan and A. Pentland, "Automatically Inferring Privacy Settings from Mobile Phone Data," *in submission*.

[19] http://www.twofortyfouram.com/product.html

[20] C. J. Reynolds and C. R. Wren, “Worse is better for ambient sensing,” Technical Report TR2006-005, Mitsubishi Electric Research Laboratories, March 2006.

[21] Wren, C.R.; Ivanov, Y.A.; Leigh, D.; Westhues, J., "The MERL Motion Detector Dataset", Workshop on Massive Datasets (MD), ISBN: 978-1-50593-981-8, pp. 10-14, November 2007

[22] M.Weiser. “The computer for the 21st century,” IEEE Pervasive Computing, pages 19–25, Jan-Mar 2002.

[23] Want, R., Hopper, A., Falcao, V., Gibbons, J., "The Active Badge Location System," ACM Transactions on Information Systems, Vol. 10, No. 1, Jan. 1992, pp. 91-102.

[24] GQ Maguire, M Smith, HWP Beadle, “SmartBadges: a wearable computer and communication system,” 6th International Workshop on Hardware/Software Codesign, 1998

[25] Mark Feldmeier, “Personalized Building Comfort Control,” PhD thesis, MIT Media Laboratory, 2009

[26]Borovoy, M. McDonald, F. Martin, M. Resnick, "Things That Blink: Computationally Augmented Nametags," IBM Systems Journal, Vol 35, Nos. 3 & 4, 1996.

[27] Borovoy, R., et al, "Meme tags and community mirrors: Moving from conferences to collaboration," in Proceedings of the ACM 1998 Conference on Computer Supported Cooperative Work, New York: ACM Press, p. 159, 1998.

[28] Laibowitz, M., and Paradiso, J.A., in Fersha, A., Hortner, H., Kostis, G. (eds), “The UbER-Badge, A Versatile Platform at the Juncture Between Wearable and Social Computing ,“ Advances in Pervasive Computing, Oesterreichische Computer Gesellschaft, 2004, pp.363-368.

[29] Olgu´ın Olgu´ın, D., Paradiso, J.A., and Pentland, A., “Wearable Communicator Badge: Designing a New Platform for Revealing Organizational Dynamics,” in the Proc. of Student Colloquium Proposals of the 10th International IEEE Symposium on Wearable Computing (ISWC), Montreux, Switzerland, October 11-14, 2006, pp. 4-6

[30] Daniel Olguin Olguin, Benjamin N. Waber, Taemie Kim, Akshay Mohan, Koji Ara, and Alex (Sandy) Pentland. “Sensible Organizations: Technology and Methodology for Automatically Measuring Organizational Behavior,” IEEE Transactions on Systems, Man, and Cybernetics-Part B: Cybernetics, Vol. 39. No. 1, February 2009.

[31] J. Lifton, M. Laibowitz, D. Harry, N.-W. Gong, M Mittal, and J. A. Paradiso "Metaphor and Manifestation - Cross Reality with Ubiquitous Sensor/Actuator Networks," IEEE Pervasive Computing, July-September 2009 (vol. 8 no. 3) pp. 24-33.

[32] Google Latitude. http://www.google.com/latitude

[33] Fackbook Inc. http://www.facebook.com

[34]AT32UC3B Series Preliminary datasheet
http://www.atmel.com/dyn/resources/prod_documents/doc32059.pdf

[35] TI CC2480 Data Sheet (Rev. A) http://focus.ti.com/lit/er/swra175a/swra175a.pdf

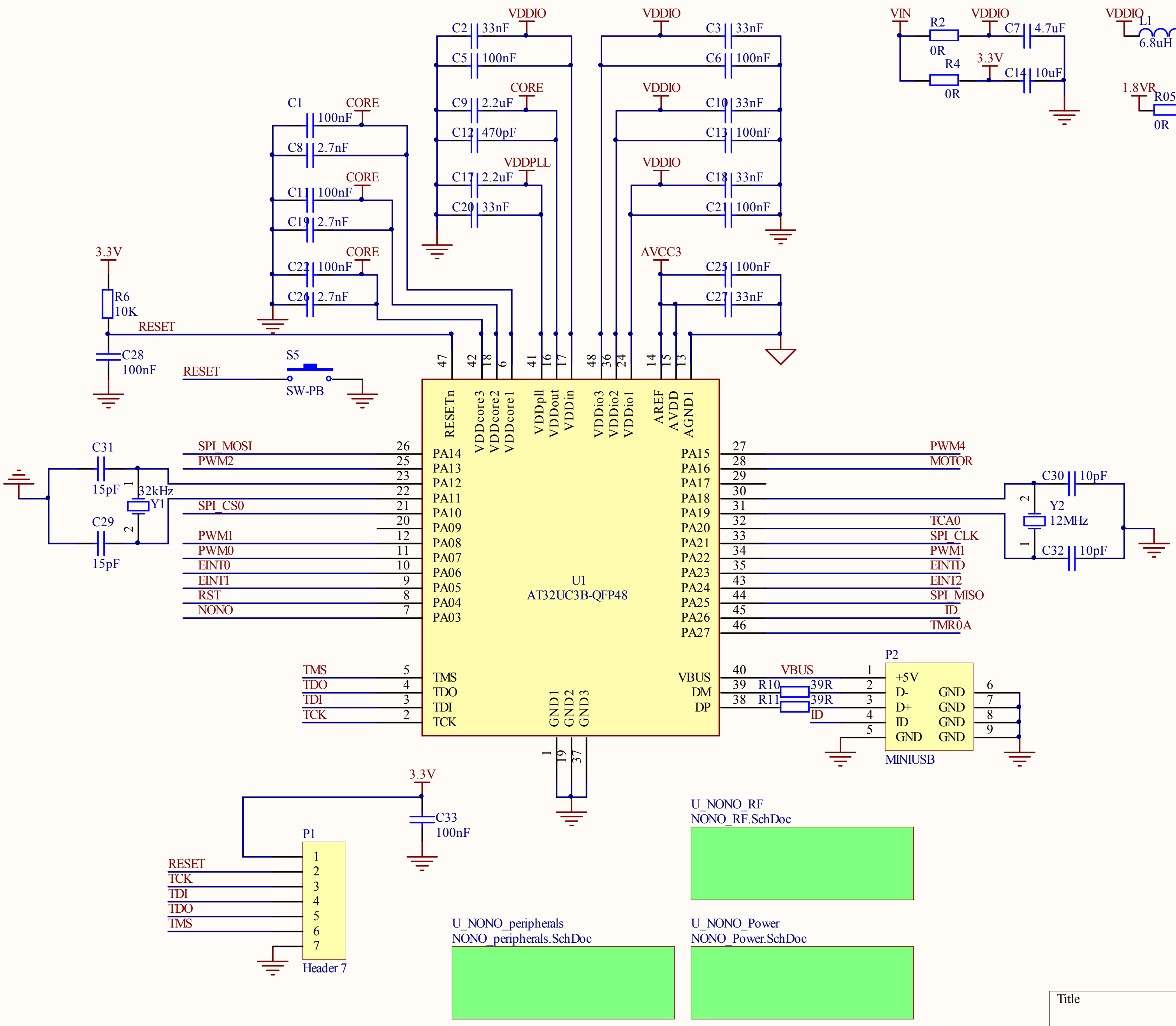
[36] TI bqTINY™ Data Sheet http://focus.ti.com/lit/ds/symlink/bq24030.pdf

[37] Zigbee Alliance http://www.zigbee.org/

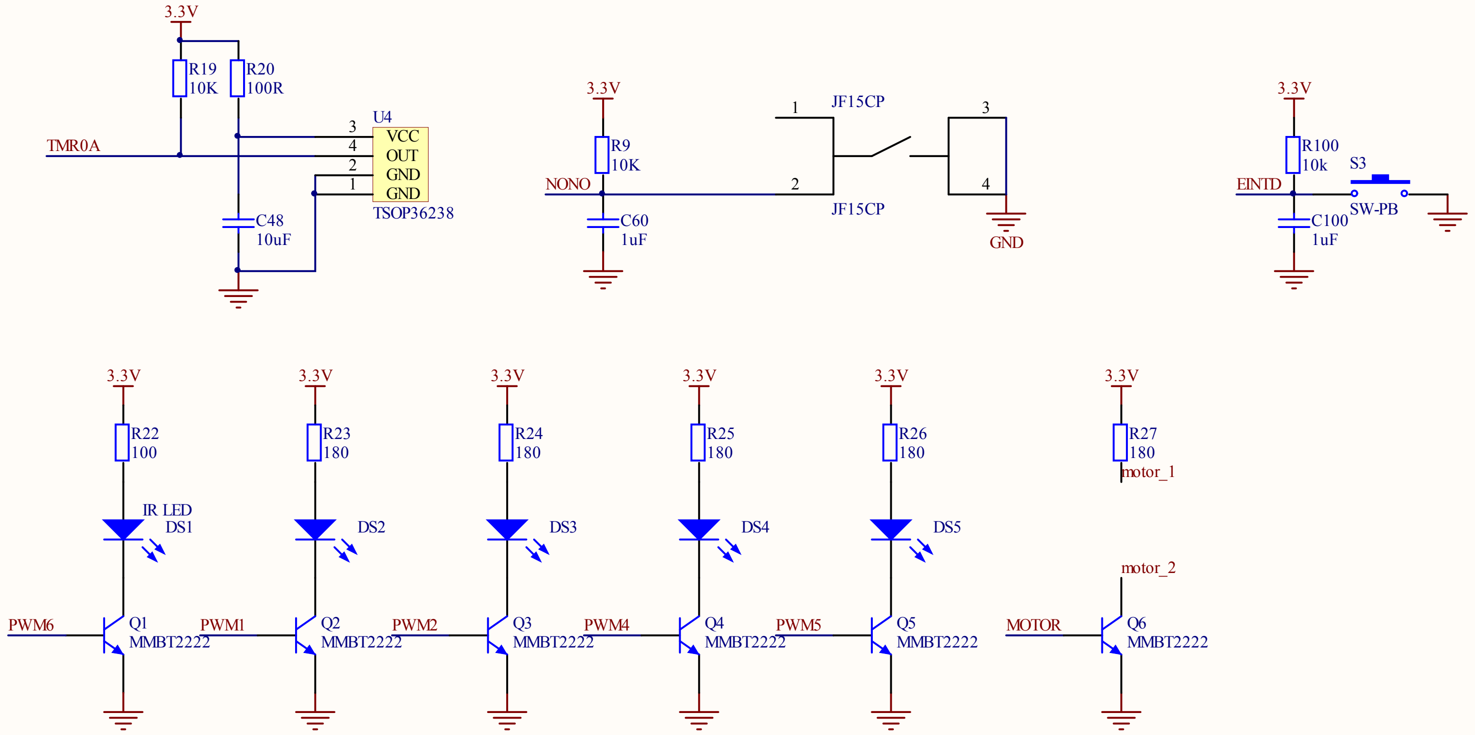
[38] MIT Office of Register http://web.mit.edu/registrar/stats/degrees/deg0708.html

Appendix A

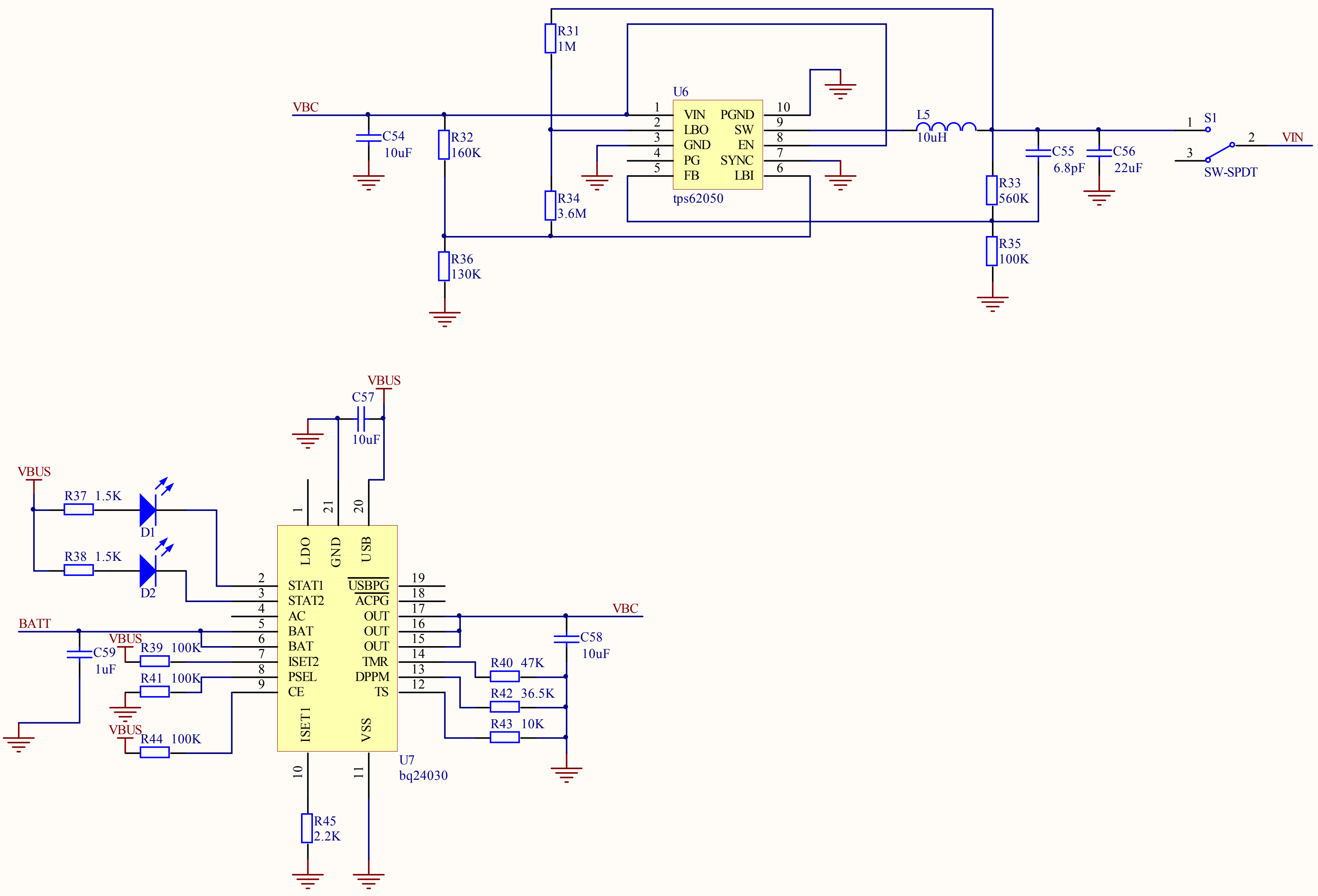
Schematics and PCB Layouts



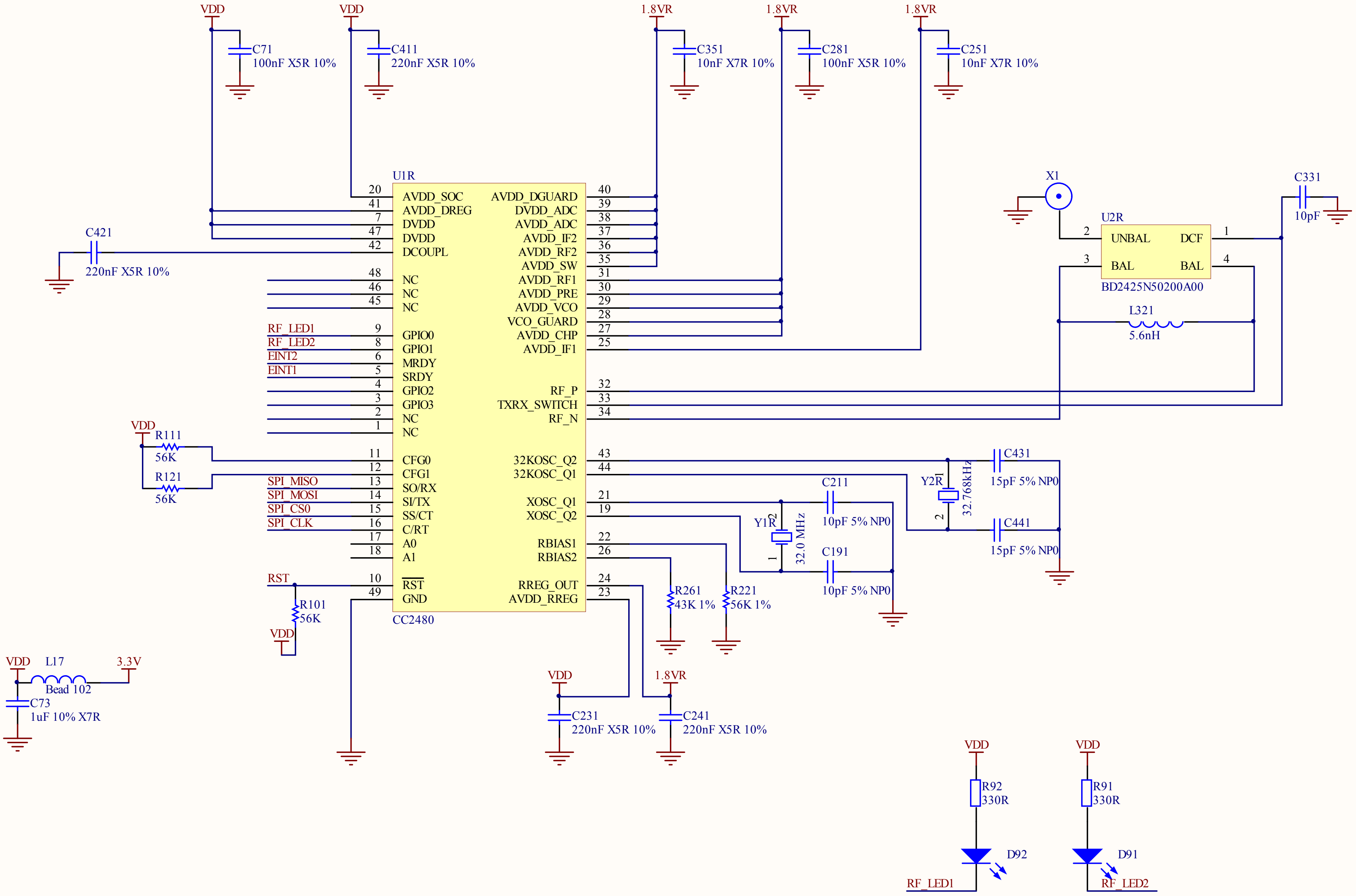
Title		
Size Letter	Number	Revision
Date:	7/31/2009	Sheet of
File:	E:\NONO_DOC\..\NONO_MCU.SchDoc	Drawn By:



Title		
Size Letter	Number	Revision
Date: 7/31/2009	Sheet of	
File: E:\NONO_DOC\..\NONO_peripherals.SchDoc	Drawn By:	



Title			
Size A	Number		Revision
Date:	7/31/2009	Sheet of	
File:	E:\NONO_DOC\..\NONO_Power.SchDoc	Drawn By:	



Title

Size
Letter

Number

Revision

Date: 7/31/2009

Sheet of

File: E:\NONO_DOC\..\NONO_RF.SchDoc

Drawn By:

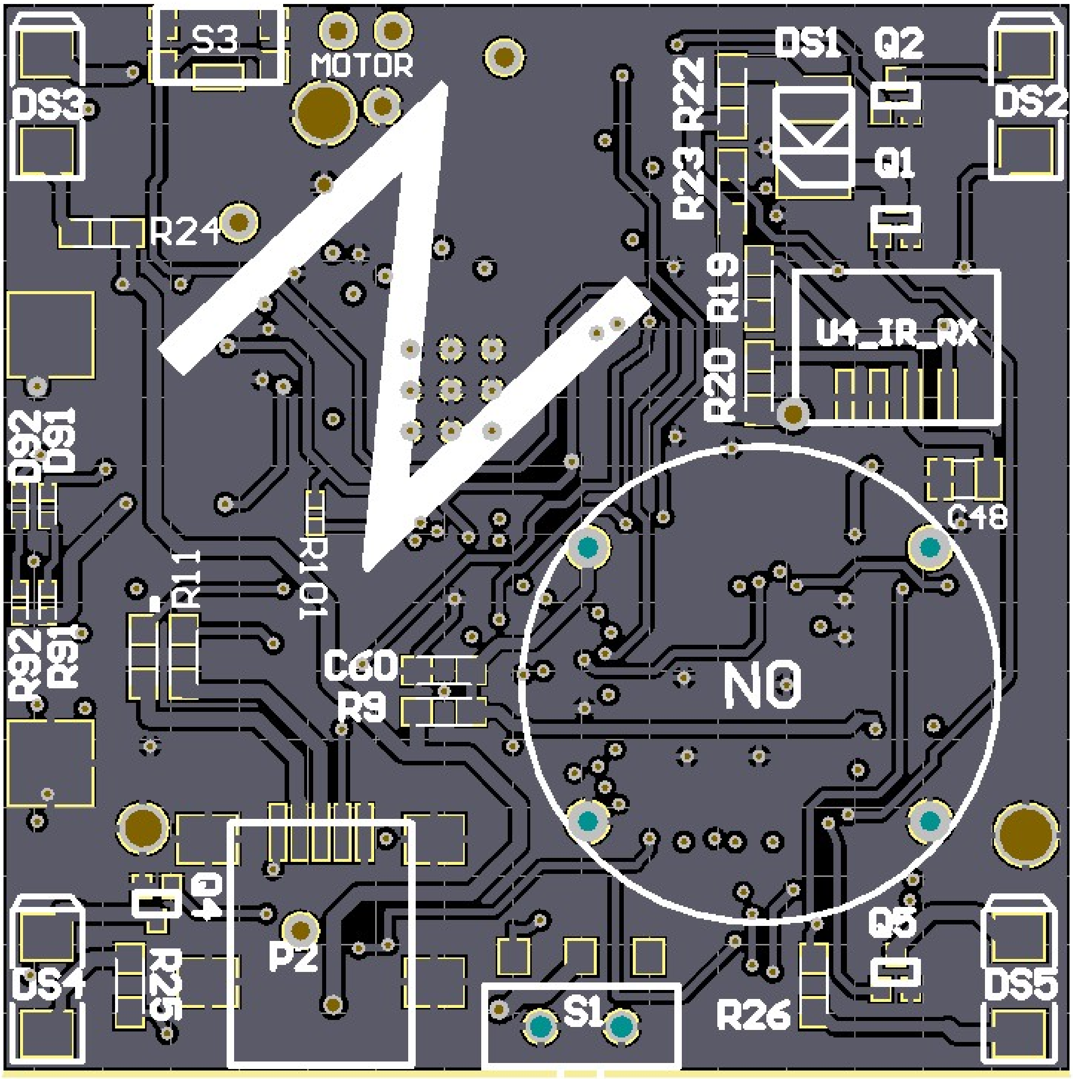


Figure A-5: Node PCB Layout Top Overview

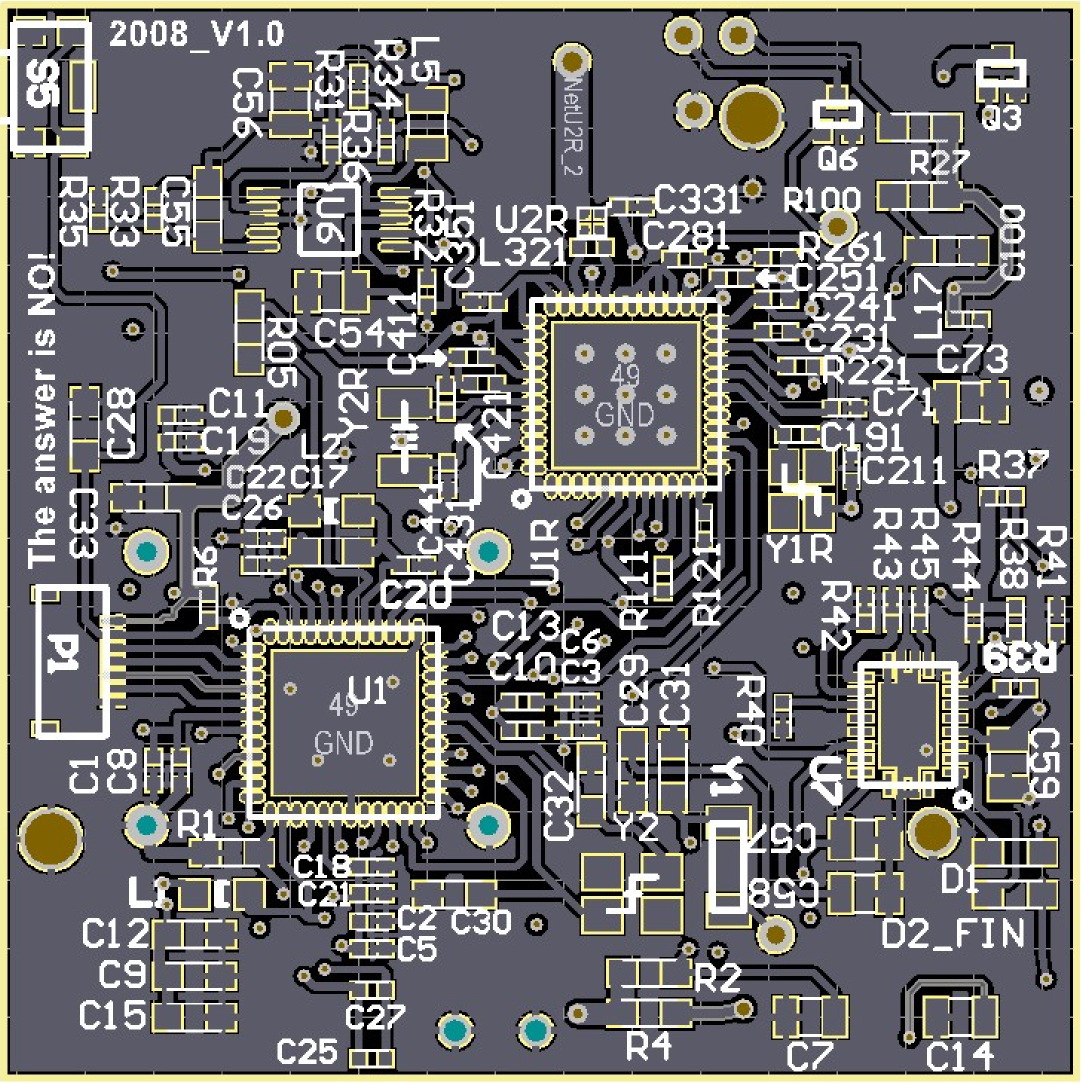


Figure A-6: Node PCB Layout Button Overview

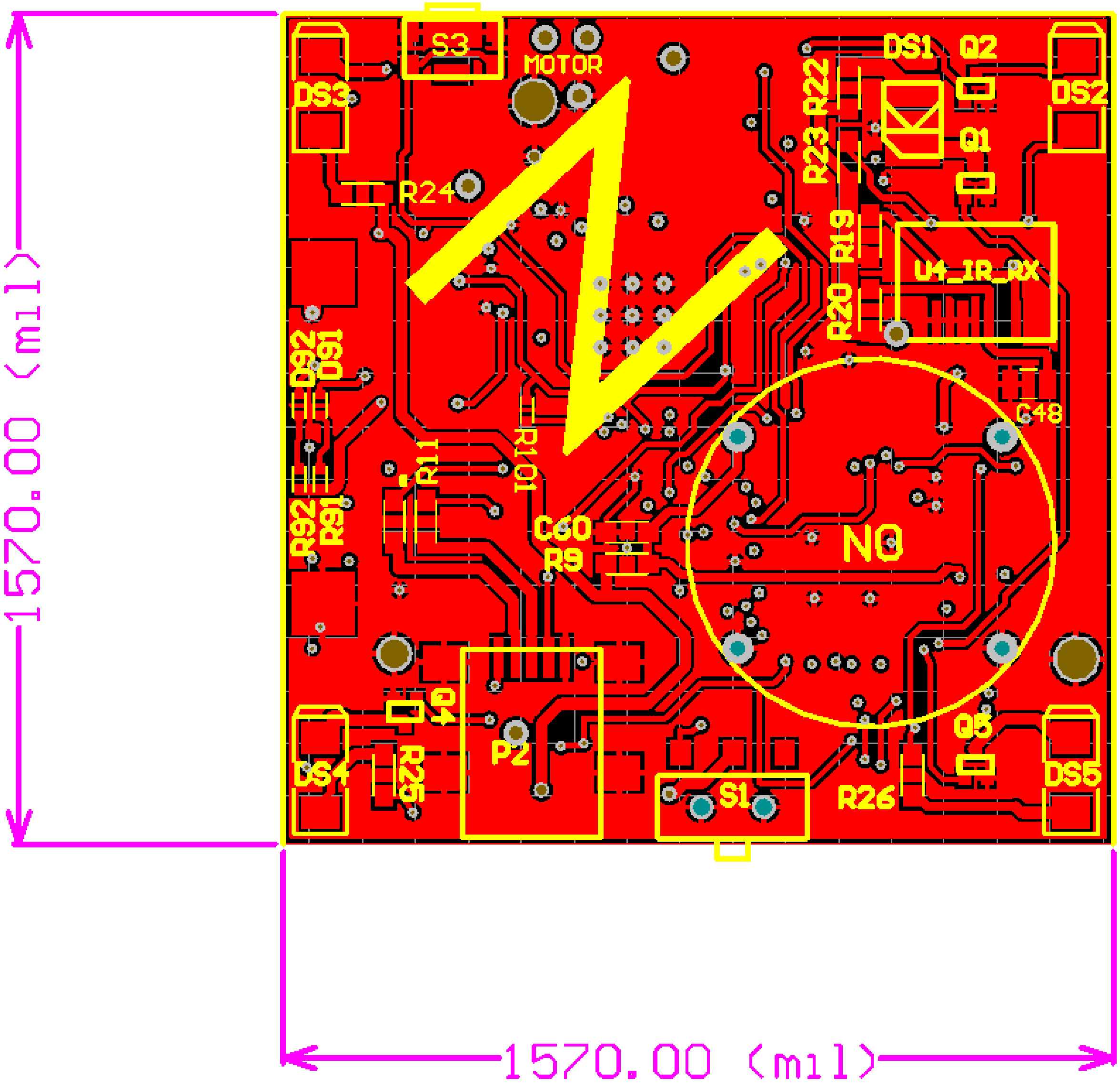


Figure A-7: Node PCB top Layout

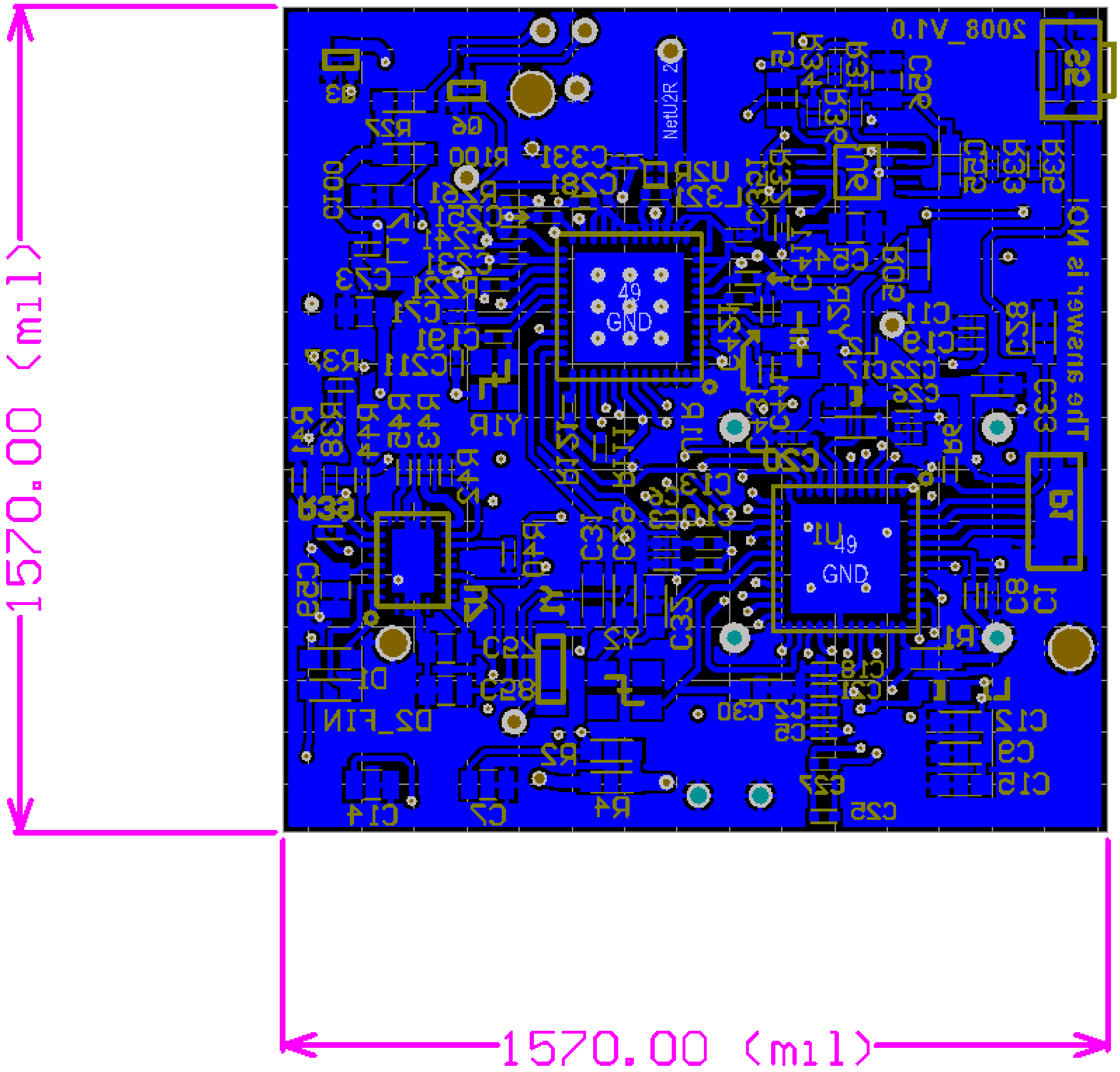


Figure A-8: Node PCB Button Layout

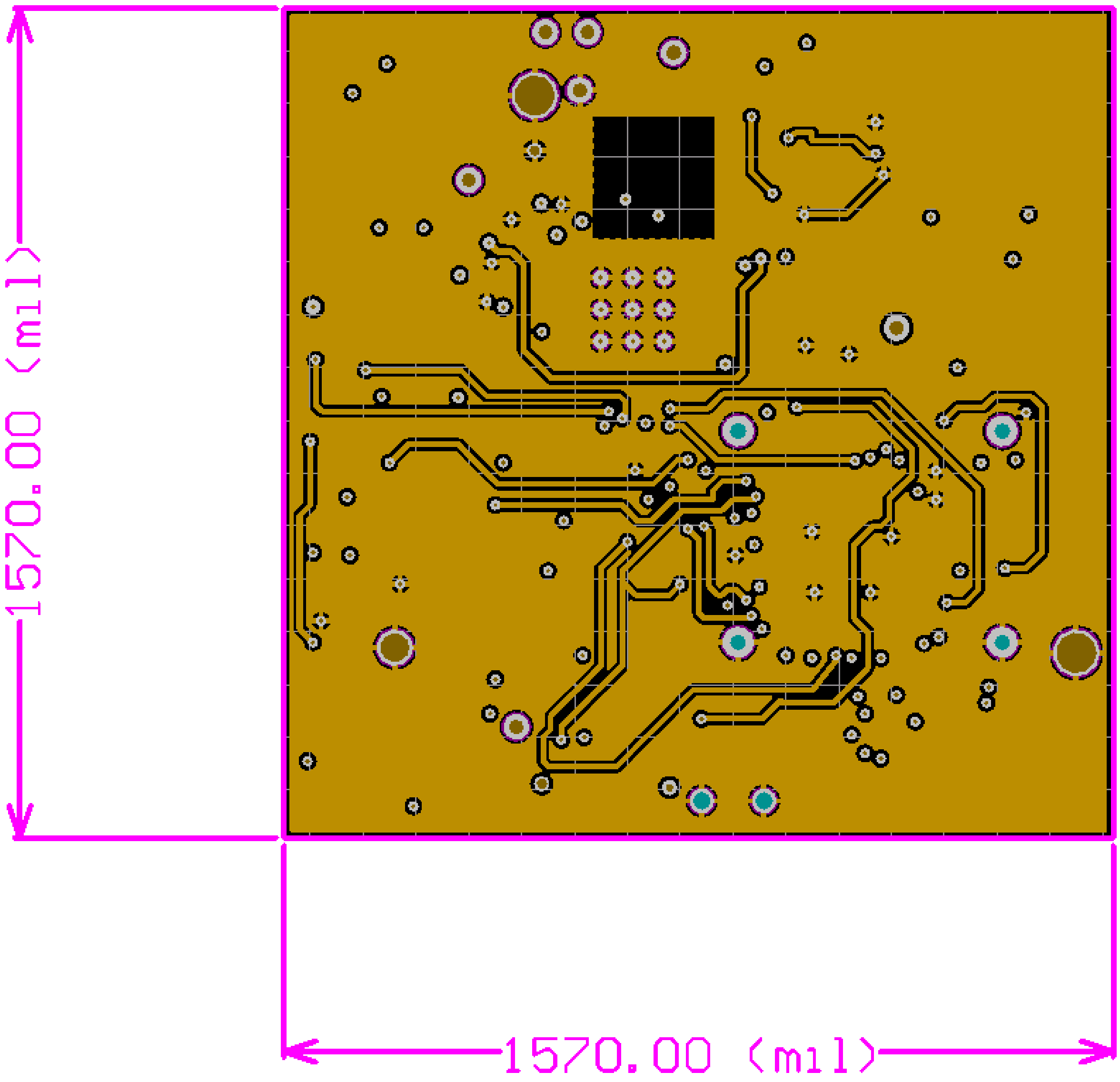


Figure A-9: Node PCB Middle Layer 1 Layout

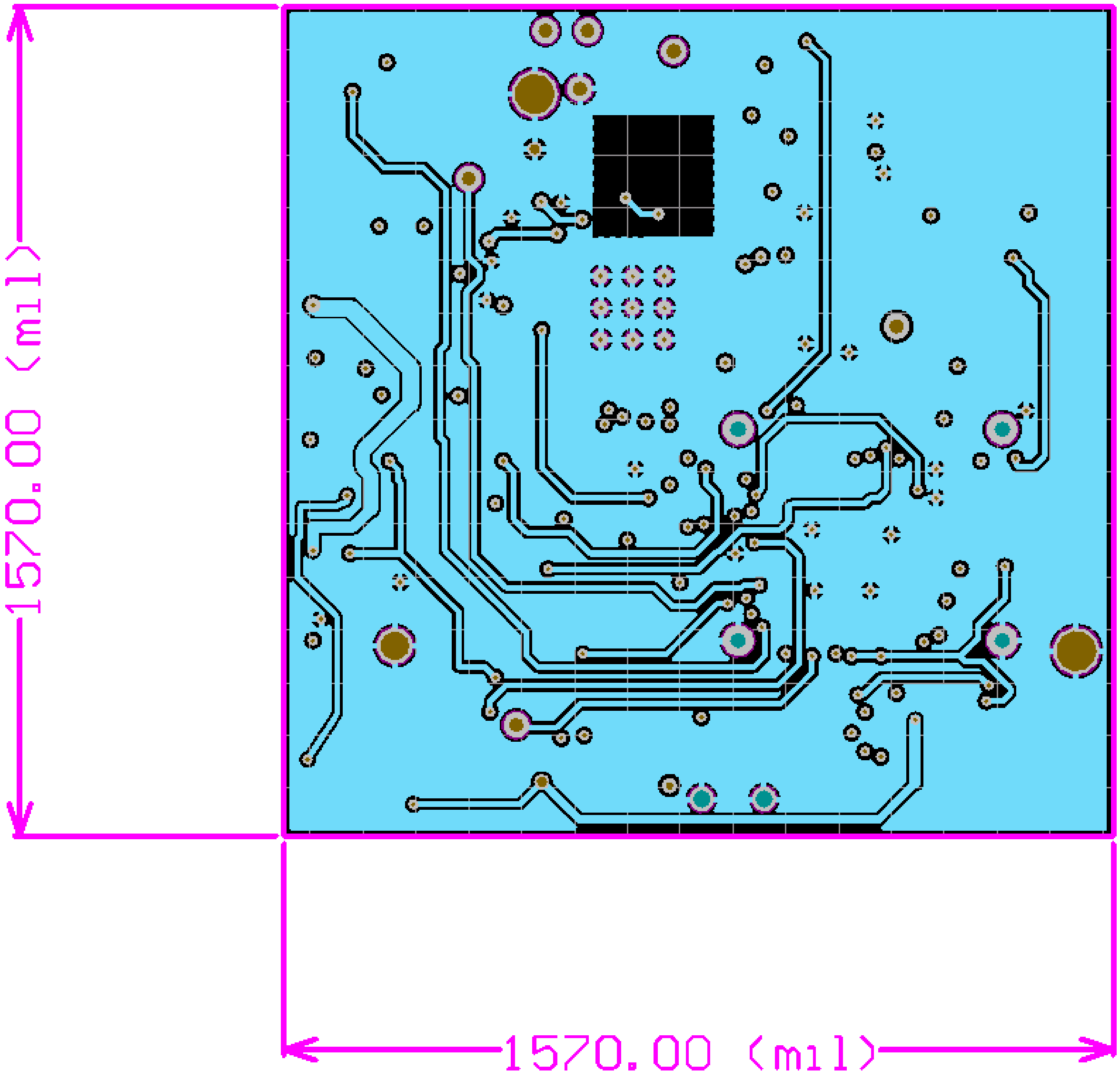


Figure A-10: Node PCB Middle Layer 2 Layout

Appendix B
COUHES Protocols

	Massachusetts Institute of Technology Committee on the Use of Humans as Experimental Subjects	**Application #** (assigned by COUHES)	09010030 71
		Date	

APPLICATION FOR APPROVAL TO USE HUMANS AS EXPERIMENTAL SUBJECTS (STANDARD FORM)

Please answer every question. Positive answers should be amplified with details. You may mark N/A where the question does not pertain to your application. Any incomplete application will be rejected and returned for completion. ***A completed CHECKLIST FOR STANDARD APPLICATION FORM must accompany this application.***

I. BASIC INFORMATION

1. Title of Study	
Ubiquitous Sensor Portals (USP) for the study of pervasive sensing environments	
2. Principal Investigator	
Name: Joseph Paradiso	Building and Room #: E15-327
Title: Associate Professor	Email: joep@media.mit.edu
Department: Media Art and Science	Phone: (617) 253-8988
3. Associated Investigator(s)	
Name: Mat Laibowitz / Nan-Wei Gong	Email: mat / nanwei@media.mit.edu
Title: Research Assistant	Phone: (617) 452-5639
Affiliation: Media Art and Sciences	
4. Collaborating Institutions. *If you are collaborating with another institution(s) then you must obtain approval from that institution's institutional review board, and forward copies of the approval to COUHES)*	
None	
5. Location of Research. *If at MIT please indicate where on campus. If you plan to use the facilities of the Clinical Research Center you will need to obtain the approval of the CRC Advisory Committee. You may use this form for simultaneous submission to the CRC Advisory Committee.*	
E15	
6. Funding. *If the research is funded by an outside sponsor, please enclose one copy of the research proposal with your application. A draft of the research proposal is acceptable.*	
Source:	Contract or Grant Title:
Contract or Grant #:	OSP #:
7. Human Subjects Training. *All study* personnel **MUST** *take and pass a training course on human subjects research. MIT has a web-based course that can be accessed from the main menu of the COUHES web site. COUHES may accept proof of training from some other institutions. List the names of all study personnel and indicate if they have taken a human subjects training course.*	
Joseph Paradiso (Yes), Mat Laibowitz (Yes), Nan-Wei Gong (Yes)	
8. Anticipated Dates of Research	
Start Date: Feb 2008	Completion Date: April 2008

II. STUDY INFORMATION

1. Purpose of Study. *Please provide a concise statement of the background, nature and reasons for the*

proposed study. Use non-technical language that can be understood by non-scientist members of COUHES.

The goal of this study is to test, debug, and evaluate a new system of distributed wireless sensors, cameras, and wearable devices. This system is intended as a research platform for the development of new media applications and experimentation with distributed sensor networks. The specific tests that will be executed in this study will be:

1) To map data collected from wearable sensors to video collected from the distributed video network with the ultimate goal of enabling users to catalog and browse their own collected video. The system will not record video unless a consenting participant wearing the wearable devices is detected. Also, there are multiple ways to deactivate the system. The users can physically turn the power off from the lamp switch, or deactivate the data streaming from a privacy badge, and there will be an option for blocking signal transmission on the touch screen for users without a badge. Through this method of identification, the data can be immediately owned by the participants and can be released to the researcher after examination.

2) To collect real data about the acceptance of such a system with regards to personal privacy and develop tools and methodologies for assuring personal privacy in the future of user-created pervasive media.

2. Study Protocol. *For* ***biomedical, engineering and related research****, please provide an outline of the actual experiments to be performed. Where applicable, provide a detailed description of the experimental devices or procedures to be used, detailed information on the exact dosages of drugs or chemicals to be used, total quantity of blood samples to be used, and descriptions of special diets.*

For applications in the ***social sciences, management and other non-biomedical disciplines*** *please provide a detailed description of your proposed study. Where applicable, include copies of any questionnaires or standardized tests you plan to incorporate into your study. If your study involves interviews please submit an outline indicating the types of questions you will include.*

You should provide sufficient information for effective review by non-scientist members of COUHES. Define all abbreviations and use simple words. Unless justification is provided this part of the application must not exceed 5 pages.

Attaching sections of a grant application is not an acceptable substitute.

The system consists of three major device components. The first component is the sensor network composed of "Ubiquitous Sensor Portals" installation distributed throughout the MIT Media Lab building E15. Each portal, mounted on a pan/tilt platform, has an array of sensors, as well as audio and video capabilities. The ubiquitous sensor portals are capable of streaming real time sensor data over the network and can initiate interactions between different portals. The second component is a set of wearable sensors that can collect human-centric behavioral and social data and communicate to the Ubiquitous Sensor Portals. The final component is the dynamic privacy badge which will allow users to create a profile of their particular privacy levels based on location, data resolution, and time.

We will initially run three distinct research studies on the system. The first application has been nicknamed SPINNER. SPINNER is a novel media network application designed to detect and capture fragmented events of human behavior that can be automatically collected and sequenced into a cohesive narrative. Parametric models of effective narratives will be developed that can be mapped on to sensor-detectable elements of human activity. The SPINNER project will also develop methods for using wearable sensors to annotate, catalog, and browse recorded media in real-time. The SPINNER system will use the Ubiquitous Awareness Portals and the wearable sensors.

The second study will use the system to support efforts in Cross Reality, where events in the real world drive phenomena in a virtual environment that is unconstrained by time, space, or the constraints of physics. For our initial X-Reality work, we will be using SecondLife by Linden Labs.

The third application of the system will be the configurable privacy badge. The badge is built to study the privacy concerns for users in a sensor-rich environment. The badge can talk to the Ubiquitous Sensor Portals through infrared and Zigbee, a wireless mesh networking standard. By sending a unique ID, the badge can be used for tagging sensor data in order to claim ownership for further editing. Also, it can send out an opting in or opting out signal to control the ubiquitous awareness portals. With this device, users can have in-situ control of their privacy and immediate feedback of the privacy levels in different scenarios. The functionality of the configurable privacy badge can also be included in the wearable sensors used for SPINNER, however it remains important to have an available device that collects no sensor data and provides the privacy control for the ubiquitous system. Appendix A shows a questionairre to be filled out before the test about the participants's opinion of privacy protection and a questionairre to be answered afterwards evaluating the system.

For all three applications, privacy is of the utmost importance. Appendix B shows the general layout of the system to best initially respect privacy during the experiments. As the data from the third experiment is collected, we will be able to dynamically adapt this topology, accordingly providing increasing amounts of personalized privacy control.

The devices all provide obvious indication when data is being collected and all tests will be announced. All devices will also be equipped with an immediate blackout function should anyone feel threatened or uncomfortable.

3. Drugs and Devices. *If the study involves the administration of an investigational drug that is not approved by the Food and Drug Administration (FDA) for the use outlined in the protocol, then the principal investigator (or sponsor) must obtain an Investigational New Drug (IND) number from the FDA. If the study involves the use of an approved drug in an unapproved way the investigator (or sponsor) must submit an application for an IND number. Please attach a copy of the IND approval (new drug), or application (new use.).*

If the study involves the use of an investigational medical device and COUHES determines the device poses significant risk to human subjects , the investigator (or sponsor) must obtain an Investigational Device and Equipment (IDE) number from the FDA.

Will drugs or biological agents requiring an IND be used? YES□ NO☒

If yes, please provide details:

Will an investigational medical device be used? YES□ NO☒

If yes, please provide details:

4. Radiation *If the study uses radiation or radioactive materials it may also have to be approved by the Committee on Radiation Exposure to Human Subjects (COREHS). COUHES will determine if you need COREHS approval.*

Will radiation or radioactive materials be used? YES□ NO☒

If yes, please provide details:

5. Diets

Will special diets be used? YES□ NO☒

If yes, please provide details:

III. HUMAN SUBJECTS

1. Subjects	
A. Estimated number: 30	**B. Age(s): 20~60**

C. Inclusion/exclusion criteria

i. What are the criteria for inclusion or exclusion?

The test will be open to volunteers from the Media Lab community. Due to all the devices being located in E15, we are limited to resident Media Lab students and faculty.

ii. Are any inclusion or exclusion criteria based on age, gender, or race/ethnic origin? *If so, please explain and justify*

no

D. Please explain the inclusion of any vulnerable population (e.g. children, cognitively impaired persons, non-English speakers, MIT students), and why that population is being studied.

MIT students will be included because they will be the most likely to be in proximity to the system for the longest amounts of time. They are not being selected specifically because they are MIT Students. Since participation is completely voluntary, it is expected that the convenience to their workplace and interest in this research topic will attract mainly Media Lab students and faculty.

2. Subject recruitment *Identification and recruitment of subjects must be ethically and legally acceptable and free of coercion. Describe below what methods will be used to identify and recruit subjects*

The subjects will not be specifically recruited. The call for participation will be publically posted with the requirements of the study and compensation.

Please attach a copy of any advertisements/ notices and letters to potential subjects

3. Subject compensation *Payment must be reasonable in relation to the time and trouble associated with participating in the study. It cannot constitute an undue inducement to participate*

Describe all plans to pay subjects in cash or other form of payment (i.e. gift certificate)

10 dollars a day or gift equivalent. This is considered reasonable compensation due to the potential privacy concerns and potential discomfort of wearing the devices. Other than these issues, the participants will mainly go about their time as they would otherwise and the test should not get in the way of whatever else they are doing.

Will subjects be reimbursed for travel and expenses?

no

4. Potential risks. *A risk is a potential harm that a reasonable person would consider important in deciding whether to participate in research. Risks can be categorized as physical, psychological, sociological, economic and legal, and include pain, stress, invasion of privacy, embarrassment or exposure of sensitive or confidential data. All potential risks and discomforts must be minimized to the greatest extent possible by using e.g. appropriate monitoring, safety devices and withdrawal of a subject if there is evidence of a specific adverse event.*

What are the risks / discomforts associated with each intervention or procedure in the study?

The potential risks of this study will be the apparent privacy invasion and the discomfort of wearing/carrying small sensor devices.

What procedures will be in place to prevent / minimize potential risks or discomfort?

A participant may turn off the devices at any time and choose when and where to participate in the study. All data and video collected will be available first to the participant and will require approval before being included in the study. We will provide opt-in and opt-out functions to allow custom levels of privacy with regards to the collected data.

5. Potential benefits

What potential benefits may subjects receive from participating in the study?
The feeling of contributing to the future will be strong. Participating in this study will be a unique expererience and inspire future work in the field of distributed and ubiquitous systems. Participants will receive significant technical insight in to the design of a large production-ready system that will help them in their own research.

What potential benefits can society expect from the study?
This system has far-reaching benefits. It is the first of its kind and looks to break new ground in distributed media networks, video annotation and browsing, and the use of narratology for the real-time understanding of events. It is the first system that will collect real data on privacy for distributed sensor systems which are currently based entirely on assumption. This is the direction of things to come -- multi-purpose, high-bandwidth sensors integrated in the surroundings respectfully providing a suite of life-enhancing applications.

6. Data collection, storage, and confidentiality

How will data be collected?
Data will be collected via video cameras with obvious indication of when and what they are recording. If there is consent, audio will be recorded. The audio and video data will be combined with the sensor data and made available via SD card in a readble form for review by the participant.

Is there audio or videotaping? YES ☒ NO☐ ***Explain the procedures you plan to follow.***
All audio and video data will be made available to the participant prior to being viewed by anyone else. It will be recorded to a SD card in the posession of the participant who can review it, edit it, and return to the researcher at will.

Will data be associated with personal identifiers or will it be coded?
Personal identifiers ☒ Coded ☐ ***Explain the procedures you plan to follow.***
While the data will use coded identifiers, the video will contain recognizable images. The participant will have option of blurring out anything recognizable and provided the data with only coded identifiers.

Where will the data be stored and how will it be secured?
At first, it will only be stored in the possession of the participant. Once approved and returned it will be stored on a secure, private-networked file server, accessable only by the researchers.

What will happen to the data when the study is completed?
It can be returned, destroyed, or stored away offline according to the wishes of the researchers or participants.

Can data acquired in the study affect a subject's relationship with other individuals (e.g. employee-supervisor, patient –physician, student-teacher, family relationships)?
no

7. Deception *Investigators must not exclude information from a subject that a reasonable person would want to know in deciding whether to participate in a study.*

Will information about the research purpose and design be withheld from subjects?
YES ☐ NO☒ ***If so, explain and justify.***

8. Adverse effects. *Serious or unexpected adverse reactions or injuries must be reported to COUHES* *within 48 hours. Other adverse events should be reported within 10 working days.*

What follow-up efforts will be made to detect any harm to subjects and how will COUHES be kept informed?

We will be provide regular updates directly to COUHES by either written reviews or arranged presentations.

9. Informed consent. *Documented informed consent must be obtained from all participants in studies that involve human subjects. You must use the templates available on the COUHES web-site to prepare these forms. Draft informed consent forms must be returned with this application. Under certain circumstances COUHES may waive the requirement for informed consent.*

Attach informed consent forms with this application.

10. The HIPAA Privacy Rule. *If your study involves disclosing identifiable health information about a subject outside of M.I.T., then you must conform to the HIPAA Privacy Rule and complete the questions below. Please refer to the HIPAA section, and to the definitions of protected health information, de-identified data and limited data set on the COUHES web-site.*

Do you plan to use or disclose identifiable health information outside M.I.T.?

YES □ **NO**☒

If YES, then the subject must complete an Authorization for Release of Protected Health Information Form. Please attach a copy of this draft form. You must use the template available on the COUHES web-site.

Alternatively, COUHES may grant a Waiver of Authorization if the disclosure meets criteria outlined on the COUHES web-site.

Are you requesting a Waiver of Authorization?

YES □ **NO**☒

If YES, explain and justify.

Will the health information you plan to use or disclose be de-identified?

YES □ **NO**☒

Will you be using or disclosing a limited data set?

YES □ **NO**☒

If YES, then COUHES will send you a formal data use agreement that you must complete in order for your application to be approved

IV. INVESTIGATOR'S ASSURANCE

I certify the information provided in this application is complete and correct

I understand that I have ultimate responsibility for the conduct of the study, the ethical performance of the project, the protection of the rights and welfare of human subjects, and strict adherence to any stipulations imposed by COUHES

I agree to comply with all MIT policies, as well all federal, state and local laws on the protection of human subjects in research, including:

- **ensuring all study personnel satisfactorily complete human subjects training**
- **performing the study according to the approved protocol**

- **implementing no changes in the approved study without COUHES approval**
- **obtaining informed consent from subjects using only the currently approved consent form**
- **protecting identifiable health information in accord with the HIPAA Privacy Rule**
- **promptly reporting significant or untoward adverse effects**

Signature of Principal Investigator ______________________ Date __________

Print Full Name and Title ____

Signature of Department Head _________________________ Date __________

Print Full Name and Title ____

Please return 3 hard copies of this application (1 with original signatures) to the COUHES office E25-143b.

Appendix A for COUHES application— Questionnaire

Pre-experiment Questionnaire Badge ID _________

1. Are you Male or Female? ___ Male ___ Female

2. What is your age? ___15-20 ___20-25 ___25-30 ___30-35
___35-40 ___40-45 ___45-50 ___50-55

3. What is your educational background?
___ high school ___ undergraduate ___ graduate school (master, PhD)

4. What is your major?
___ Engineering _____________ (for example, electrical engineering)
___ Science _____________ ___ Humanity _____________
___ Art _____________ ___ Others _____________

5. What is your religion/race? (optional) ___________________________

Please rank the following concepts from 1 to 5 (1 = strongly disagree, 5= strongly agree).

6. The surveillance system on the street is necessary for our safety.
1 2 3 4 5

7. A context aware sensor network is important for enriching our lives.
1 2 3 4 5

8. It is important for everyone to have control over their own privacy.
1 2 3 4 5

9. Ubiquitous computing or a sensor system in a building is totally unnecessary.
1 2 3 4 5

10. The sensor system in my work place is invading my privacy.
1 2 3 4 5

11. I enjoy technology. For example, the smart phone with a high resolution camera and a voice recognition system.
1 2 3 4 5

12. I enjoy experiencing the advancement of new technology in multimedia.
1 2 3 4 5

Post-experiment Questionnaire

Please rank the following concepts from 1 to 5 (1 = strongly disagree, 5= strongly agree).

1. Do you feel in control of your privacy with the badge?

1 2 3 4 5

2. Is the badge effective enough to protect your privacy when needed?

1 2 3 4 5

3. Which of the following approaches best suit your need for privacy control?

Lamp switch ________ button on the touch screen ______

Privacy badge setting _______ privacy badge button _________

4. is the design intuitive and easy to use? (if not, please write down the suggestion)

1 2 3 4 5

5. is the web interface intuitive and easy to use? (if not, please write down the suggestion)

1 2 3 4 5

6. Do you think a web-based privacy level setting is a good way to control your privacy?

1 2 3 4 5

What improvements / changes would you like to suggest?

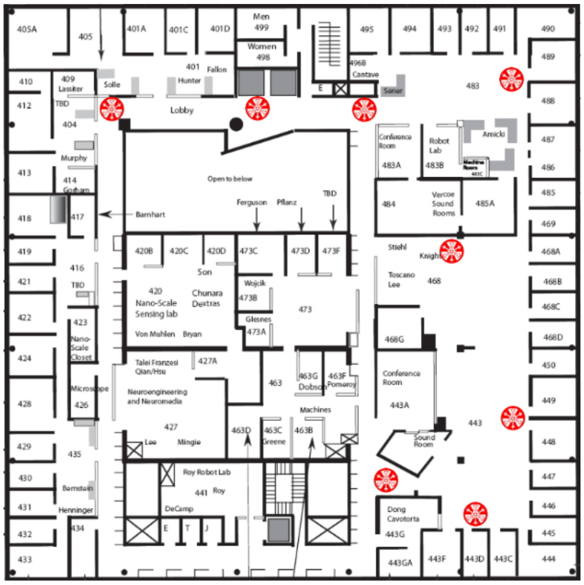
1.

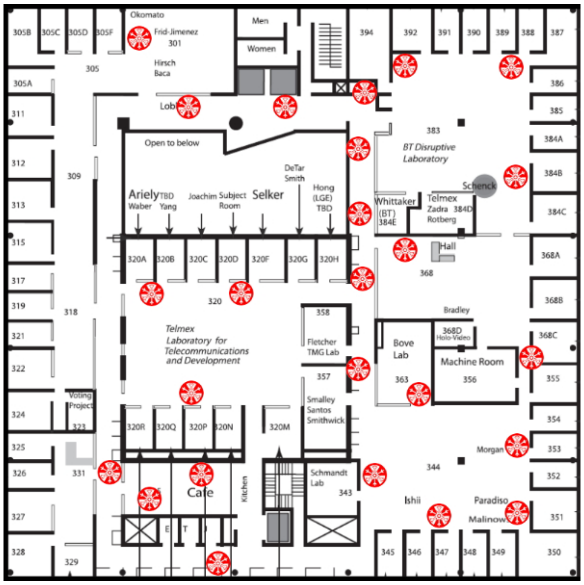
2.

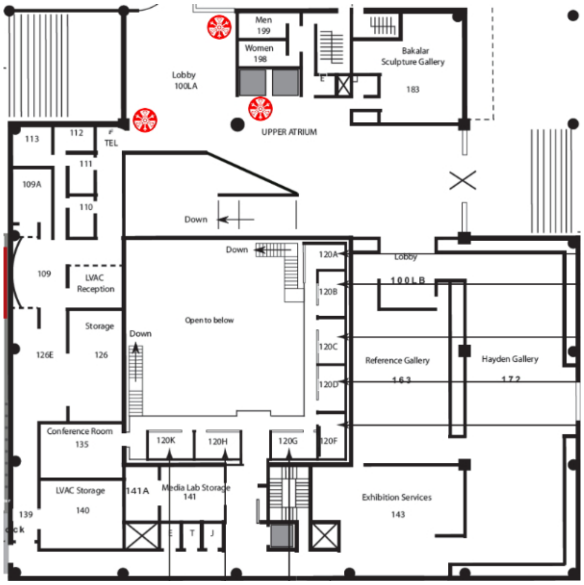
3.

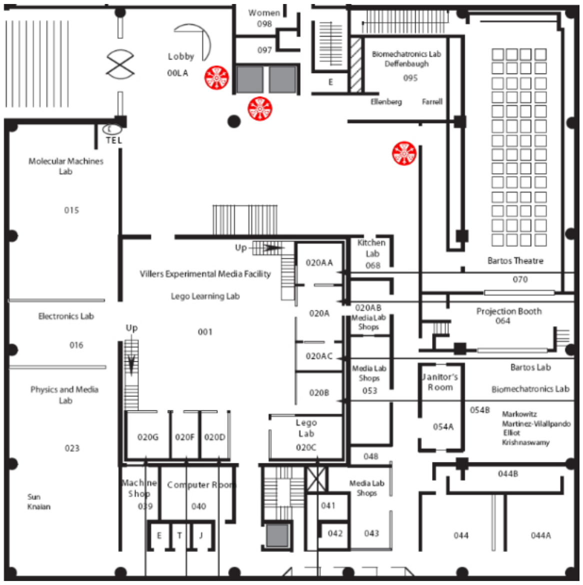
Please indicate the location of your office and the route you usually take during a day on the next page.

Badge ID ____________________


405A
405
401A
401C
401D
Men 499
Women 498
495
494
493
492
491
490
489
496B Cantave
401 Fallon
Hunter
409 Lassiter
Solle
410
412
TBD
Lobby
E
Sener
483
488
404
Murphy
413
414 Gotham
418
417
Barnhart
Open to below
Ferguson
Pflanz
TBD
Conference Room
483A
Robot Lab
483B
Amicki
Machine Room
487
486
485
484
Vercoe Sound Rooms
485A
469
419
416
420B
420C
420D
473C
473D
473F
Stiehl
Knight
468A
421
TBD
Son
Wojcik
Toscano Lee
468
468B
422
423
420 Nano-Scale Sensing lab
Chunara Dextras
473B
473
468C
Nano-Scale Closet
Glesnes
473A
Von Muhlen
Bryan
468G
468D
424
Talei Franzesi Qian/Hsu
427A
463G Dobson
463F Pomeroy
Conference Room
450
Microscope
463
443A
449
428
426
Neuroengineering and Neuromedia
Machines
443
427
463D
463C Greene
463B
Sound Room
448
429
435
Lee
Mingle
430
Roy Robot Lab
447
Barnstein
441 Roy
431
Henninger
DeCamp
Dong Cavotorta
446
432
434
E
T
J
443G
445
433
443GA
443F
443D
443C
444


Okomato
305B
305C
305D
305F
Frid-Jimenez 301
Men
Women
394
392
391
390
389
388
387
305
Hirsch Baca
305A
386
Lobby
385
311
Open to below
383
BT Disruptive Laboratory
384A
312
309
DeTar Smith
Schenck
384B
Ariely TBD
Waber
Yang
Joachim Subject Room
Selker
Hong (LGE) TBD
Whittaker (BT) 384E
Telmex Zadra 384D Rotberg
313
384C
315
320A
320B
320C
320D
320F
320G
320H
Hall
368A
368
317
320
368B
319
Bradley
358
318
Telmex Laboratory for Telecommunications and Development
Fletcher TMG Lab
Bove Lab
368D Holo-Video
368C
321
Machine Room
356
357
363
355
322
Voting Project
Smalley Santos Smithwick
354
324
323
320R
320Q
320P
320N
320M
344
Morgan
353
325
331
Schmandt Lab
326
343
352
Cafe
Kitchen
Ishii
Paradiso
327
Malinow
351
E
T
328
329
345
346
347
348
349
350


Men 199
Women 198
Lobby 100LA
E
Bakalar Sculpture Gallery
183
UPPER ATRIUM
113
112
TEL
111
109A
110
Down
Down
120A
Lobby
109
LVAC Reception
100LB
120B
Open to below
Storage
Down
120C
126E
126
Reference Gallery 163
Hayden Gallery 172
120D
Conference Room 135
120K
120H
120G
120F
LVAC Storage 140
141A
Media Lab Storage 141
Exhibition Services 143
139
E
T
J
ck


Women 098
097
Lobby 00LA
Biomechatronics Lab Deffenbaugh 095
E
Ellenberg
Farrell
TEL
Molecular Machines Lab
015
Up
Kitchen Lab 068
020AA
Villers Experimental Media Facility
Bartos Theatre
070
Lego Learning Lab
020AB Media Lab Shops
Electronics Lab
020A
Projection Booth 064
Up
001
016
020AC
Media Lab Shops 053
Bartos Lab
Janitor's Room
Physics and Media Lab
Biomechatronics Lab
020B
054B
023
020G
020F
020D
Lego Lab 020C
054A
Markowitz Martinez-Villalpando Elliot Krishnaswamy
048
044B
Sun Knaian
Machine Shop 039
Computer Room 040
041
Media Lab Shops
E
T
J
042
043
044
044A

Appendix B for COUHES application— Consent form

CONSENT TO PARTICIPATE IN
NON-BIOMEDICAL RESEARCH

[Configurable Privacy in a Pervasive Sensing Environment]

For spinner application system

You are asked to participate in a research study conducted by Joe Paradiso / Mat Laibowitz / Nan-Wei Gong, from the *department of Media Arts and Science* at the Massachusetts Institute of Technology (M.I.T). Results of this study will be included in *Mat Laibowitz's PhD thesis and Nan-Wei Gong's Masters' thesis.* You were selected as a possible participant in this study *because your office is near by one of the possible locations where the sensor system for privacy-related experiments will be deployed.* You should read the information below, and ask questions about anything you do not understand, before deciding whether or not to participate.

- **PARTICIPATION AND WITHDRAWAL**

Your participation in this study is completely voluntary and you are free to choose whether to be in it or not. If you choose to be in this study, you may subsequently withdraw from it at any time without penalty or consequences of any kind. The investigator may withdraw you from this research if circumstances arise which warrant doing so.

- **PURPOSE OF THE STUDY**

This goal of this research is to study the privacy issue within a ubiquitous computing system through providing a user centric control of their personal privacy setting in a sensor rich environment. There are two sets of different functionality in our sensor system – broadcasting information for interaction and recording sensor data for story narrative. We will conduct different sets of experiments base on the fundamental differences of those two functionalities and analyze the privacy issue for future references in the design and deployment in pervasive sensor networks.

- **PROCEDURES**

If you volunteer to participate in this study, we would ask you to do the following things:

You will be asked to carry the configurable privacy badge throughout the day. The badges will be fully charged before and assigned randomly to all the users. During the day, the ubiquitous sensor portals can be broadcasting sensor data to different portals and the Second Life platform, which is an online platform with open access for anyone. You can use the opting out button on the badge to block and stop the broadcasting. The broadcasting will restart after 1 minute. You will be asked to stay in your work area during the work hours. The total length of time for participation will be 4 hours a day, 10 am~12 pm and 2 pm ~ 4 pm. There will be no audio streaming unless you initiate the interaction physically from the touch screen. The portals cab be physically (by the touch screen) and logically (by the web server or badge signal) disabled. Also, the screen will provide a reciprocal feedback (the images of people who is watching you) when it is streaming video.

- **POTENTIAL RISKS AND DISCOMFORTS**

The user participated in this research will have full control of their privacy with the badge. The potential risks of this platform will be privacy invasion of the non-badge users who accidentally entered the sensing zone during our experiments and broadcast or being recorded without knowing it. Thus, a proper notification will be prepared in the experiment area for such potential privacy risks, and the portals will provide a visible notification when a connection is activated.

- **POTENTIAL BENEFITS**

The research and platform will contribute to the study of privacy protection in the future development of pervasive sensor networks such as a smart home. For the Media Lab community, the installation of this platform is very important since this is the most sophisticated lab wide sensor network which allows everyone to conduct their research in.

- **PAYMENT FOR PARTICIPATION**

There will be no payment for the subjects this experiment since the hours of experiments are also the work time during week days and the process will not interfere while their work. Participation of the interaction with portals will be voluntarily.

- **CONFIDENTIALITY**

The sensor data will not be recorded. The ID of the badge is a random number which will give no identity about you. This research is to study the human centric control of the privacy issue hence no data will be collected except the ID of RF beacons. You will be asked to complete a questionnaire after the experiment which may ask your personal information such as age, educational backgrounds. But any information that is obtained in connection with this study and that can be identified with you will remain confidential and will be disclosed only with your permission or as required by law.

- **IDENTIFICATION OF INVESTIGATORS**

If you have any questions or concerns about the research, please feel free to contact

Joseph Paradiso	joep@media.mit.edu	(617) 253-8988
Mat Laibowitz	mat@media.mit.edu	(617) 252-5615
Nan-Wei Gong	nanwei@media.mit.edu	(617) 452-5639

- **EMERGENCY CARE AND COMPENSATION FOR INJURY**

If you feel you have suffered an injury, which may include emotional trauma, as a result of participating in this study, please contact the person in charge of the study as soon as possible.

In the event you suffer such an injury, M.I.T. may provide itself, or arrange for the provision of, emergency transport or medical treatment, including emergency treatment and follow-up care, as needed, or reimbursement for such medical services. M.I.T. does not provide any other form of compensation for injury. In any case, neither the offer to provide medical assistance, nor the actual provision of medical services shall be considered an admission of fault or acceptance of liability. Questions regarding this policy may be directed to MIT's Insurance Office, (617) 253-2823. Your insurance carrier may be billed for the cost of emergency transport or medical treatment, if such services are determined not to be directly related to your participation in this study.

- **RIGHTS OF RESEARCH SUBJECTS**

You are not waiving any legal claims, rights or remedies because of your participation in this research study. If you feel you have been treated unfairly, or you have questions regarding your rights as a research subject, you may contact the Chairman of the Committee on the Use of Humans as Experimental Subjects, M.I.T., Room E25-143B, 77 Massachusetts Ave, Cambridge, MA 02139, phone 1-617-253 6787.

SIGNATURE OF RESEARCH SUBJECT OR LEGAL REPRESENTATIVE

I understand the procedures described above. My questions have been answered to my satisfaction, and I agree to participate in this study. I have been given a copy of this form.

____

Name of Subject

____

Name of Legal Representative (if applicable)

____ ______________

Signature of Subject or Legal Representative Date

SIGNATURE OF INVESTIGATOR

In my judgment the subject is voluntarily and knowingly giving informed consent and possesses the legal capacity to give informed consent to participate in this research study.

____ ______________

Signature of Investigator Date