

# Perceived Benefits and Concerns of Prospective Users of the SmartCampus Location-Aware Community System Test-bed

Eunhee Kim  
Management Information Systems Department  
Northern State University  
ekim@northern.edu

Maria Plummer    Starr Roxanne Hiltz    Quentin Jones  
Information Systems Department  
New Jersey Institute of Technology  
mmp36@njit.edu    hiltz@njit.edu    qgjones@acm.org

## Abstract

*The SmartCampus initiative aims to turn an urban university campus into a living laboratory for location aware community system services. To lay a foundation for this effort, the SmartCampus test-bed is being created through provisioning to 500+ students with personal computing devices (smart phones and tablet PCs), which will run a suite of applications that link “people-to-people-to-place”, or P3-systems. To explore anticipated usage and concerns, and to use this information to help to refine the design of various applications, semi-structured interviews were conducted with a cross section of 65 members of the NJIT campus community. The interviews employed hypothetical use scenarios to enable prospective users to give their opinions about applications that did not yet exist at the time of the study.*

*Most students were quick to see the possible benefits of applications that can allow one, for instance, to see the campus location of their ‘buddies’ at a glance. The major concerns were with privacy control, the validity of the data entered (e.g., will applications be used to make verbal attacks on others?), and interruptions / overload with information, which may be disruptive. The concerns raised are being used to help inform the design of test-bed applications.*

## 1. Introduction

Over the past 20 years, a range of ubiquitous social computing applications have been developed [1]. Such applications utilize ubiquitous computing technologies (e.g. RFID tags, smart phones, context-aware interactive large screen displays, etc.) to enable various social software applications. The term “social software” is a relatively recent but increasingly popular label for software that enables computer-mediated communication, collaboration and coordination that may lead to the formation of computer-supported social networks or communities. Popular examples of social software include email lists, instant messaging, and social network services. A well-known example of a ubiquitous social computing application is flickr.com’s geographically tagged picture sharing.

Increasingly ubiquitous social computing applications use contextual information to provide ‘people-to-people-place’, or P3-System services [2] such as location-aware social matching, and location-aware collaborative writing. A variety of proof-of-concept and commercial systems have been developed (see [3] for a review). Some systems enabled individuals and groups to associate text notes with locations, such as *GeoNotes* [4]. Others have provided users with an interface that provides awareness in terms of the location and availability of ‘buddies’ as means to increase informal interactions, such as UCSD’s *ActiveCampus Explorer* [5].

In theory, the deployment of P3-Systems is of particularly high value in physical environments with rich social fabrics and physical geographies. For example, in urban enclaves such as corporate office complexes with associated eating and shopping spaces, or college campuses in a downtown urban location, community members routinely miss opportunities to leverage interpersonal affinities for friendship, learning, or business through simple lack of awareness, which could be addressed by P3-systems. Further, the geographical spread of many enclaves results in basic coordination problems that such systems could resolve. It is in one such urban enclave that we creating a living laboratory for P3-services through the SmartCampus initiative.

## 2. Background

A number of groups have explored location-aware community computing in Campus environments. One of the first was the *Active Badge*, which was initially developed by Olivetti Research, in their laboratory at the University of Cambridge, UK in the early 1990s. The initial *Active Badge* provided a means of locating individuals within a building by determining the location of a small device, which transmits a unique infra-red signal every 10 seconds. Offices within the buildings were equipped with networked sensors that detected these transmissions [6, 7].

In the trial implementation of *Active Badge*, management requested that everyone should wear the badge for an initial period of two weeks and from then onwards wearing it was optional. In this trial implementation and in subsequent installations at other

locations, privacy seemed to have been a major issue [8]. It was initially reported that concerns about privacy diminished after the badges were put to use for a short period of time [7]. However, a case study on the project did not confirm this initial report and suggested that views on privacy depended on the Cambridge research group under discussion [8]. There was also the fear of this technology being abused by unscrupulous employers. Despite these concerns, the general acceptance of the system led the researchers to conclude that amongst professionals responsible for their own work time, the *Active Badge* was a very useful and welcomed office system [7].

In 2002, it was reported that over 1500 more advanced active badges with microprocessors that support bi-directional communication, as well as 2000 sensors had been deployed throughout a number of European universities including the University of Kent, Imperial College, London, Lancaster University, and the University of Twente, Netherlands. At Cambridge University Computer Laboratory alone, over 200 badges and 300 sensors were being used daily [7].

The University of California San Diego, in 2002, with the help of a donation of a large number of PDAs from Hewlett Packard, began a relatively large-scale test of two location-aware applications, namely ActiveClass and ActiveCampus Explorer, which were developed as part of the UCSD ActiveCampus project [5]. In contrast to the Active Badge implementation at Cambridge University, the UCSD's ActiveCampus Explorer utilized regular handheld devices, and deployed a suite of entirely different location-aware techniques within the application including campus maps, "buddy locator" and "digital graffiti" (messages about places left on the map), which are being adapted for inclusion in SmartCampus and will be described in more detail below. Consequently, in addition to the concerns about privacy and fear of misuse of data by authority, the UCSD team was faced with new technical and physical challenges summarized below [9]:

- PDA design – the short battery life; the complexity in configuring the PDA to conserve power; the time and expertise needed to restore settings if the main and backup batteries died or connectivity was lost; the difficulty in using the stylus to enter non-standard text messages.
- Software infrastructure – because of the limitations with the use of html, individuals must constantly monitor their PDA to be aware of the arrival of new campus explorer messages and to notice interesting graffiti.
- Graffiti issues – graffiti was not as visible as anticipated; clutter was created because of the inability to erase or hide unwanted graffiti.
- Physical constraints – placement of the PDA so that its screen can be easily viewed by users at all times was a problem; portability of the PDA, especially by women, was also an issue.

Griswold et al. [5] described their experience with ActiveCampus Explorer as positive despite the hindrances listed above. These authors also noted that students were willing to share their location with buddies as well as non-buddies and suggested that social barriers such as the desire to preserve total privacy did not seem to be as significant an issue as they initially anticipated. Despite these findings, other independent researchers were less positive about the potential utility of their system for students [9].

MIT's iSPOTS also provided location-aware services. In November 2005, the Massachusetts Institute of Technology (MIT) unveiled electronic maps that track across its campus, day and night, the devices such as laptops, wireless PDAs or even Wi-Fi equipped cell phones that people use to connect to the university's wireless network [10]. The initial objective of MIT's iSPOTS project, as reported in press releases and on the MIT web site [10, 11], appeared to be different from that of UCSD's ActiveCampus in that it was intended to understand better how wireless technology is changing campus life, and the implication for planning spaces and administering services. With iSPOTS, everyone connected to the school's network is automatically represented on a map showing sites of wireless Internet use. However, users can choose whether or not to have their identity revealed on another map that computes the traces of individuals passing through the MIT Campus.

At a very early stage in the project, researchers noted that "study labs that once bustled with students are now empty as people are no longer tethered to a phone line or network cable" [10]. The issue of privacy was raised with at least one student predicting that many of his fellow students would not choose to reveal their identity on the traces map [10]. Therefore, this was viewed as a challenge that had to be addressed by the project implementers.

The observations made in the Active Badge, UCSD ActiveCampus and iSPOTS implementations suggest that social barriers such as privacy concerns and potential misuse of data by authorities, as well as some technical and physical annoyances, have to be addressed in the implementation of NJIT's SmartCampus applications.

### 3. SmartCampus Test-Bed Overview

The aim of the SmartCampus initiative is to improve geographically concentrated social connectivity through the use of our People-to-People-to-Place (P3) systems. We believe that their use will lead to more social interaction, more collaborations, and larger and more inter-connected social networks, thus building the overall strength of community.

However, location-aware social computing applications also raise many issues, especially related to privacy and to user control over who can obtain what information and when and where. We need to determine the short- and long-term social impacts of systems of this type, both for

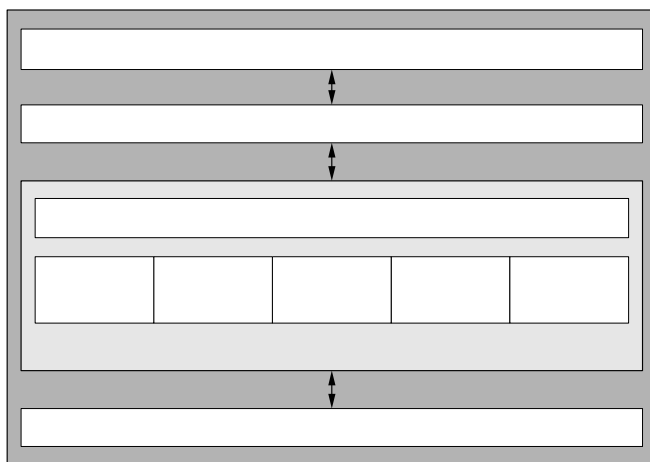
good and for bad, and to use observations and user preferences to tweak the system to encourage positive outcomes and discourage negative ones. Thus, our development and implementation of SmartCampus at NJIT is accompanied by an extensive program of research on acceptance and impacts, including interviews and questionnaires, and monitoring of what kinds of services are used where.

To understand the potential benefits and concerns of SmartCampus applications before describing our study we will provide an overview of the test-bed's design and initial suite of applications.

### 3.1 Technical Overview

The SmartCampus Test-bed has been designed to support the rapid development, prototyping and testing of P3-systems through a unified extensible service orientated architecture (SOA). Locatability is achieved through a modified version of Intel's PlaceLab's [4] code, and complete WiFi coverage of our campus, which is complimented by a small number of WiFi access points that do not provide connectivity but rather act as beacons to improve location accuracy.

Typically, an application consists of two components: (1) a thin system client that can reside on any mobile or personal computing device; and (2) a system service built on top of our SmartCampus middleware. The SmartCampus middleware securely collects individual, community, place, and social event data from associated system applications, which are continually mined to produce increasingly rich social models of the campus environment. A large spectrum of services can then access the knowledge derived from these models in a simple and secure way through a Service API.



**Figure 1. SmartCampus system architecture**

The SmartCampus middleware has the following five components (see Figure 1):

- *Data Collection* – This component collects static and

dynamic data from the clients, services, and physical infrastructure in various forms such as personal mobility traces, device tracking, user generated content such as place-labels.

- *Data Mining* – This module uses the data collected to infer new information such as places of importance to individuals and communities, and affinities among individuals or groups of users through social network profiling. This knowledge can be used to enrich user profiles and build social ties.
- *Security and Privacy Manager* – This module provides security primitives for authentication, authorization, auditing, and key management. It also introduces privacy-preserving techniques during data mining (e.g., anonymizing data) and real-time social matching (e.g., cloaking the identity of users during social introductions).
- *Data Cache* – To improve efficiency, the middleware maintains a cache of recently collected or mined data. This allows services to rapidly access data about on-campus users and provide quicker real-time answers.
- *Event Dispatcher* – This module is responsible for event registration, management, schedule, and delivery.

Collectively the SmartCampus SOA provides us with a means of effectively addressing privacy concerns through by providing a unified interface for controlling context aware management of locatability and interruptability. We will discuss how we plan to achieve this in more details after first describing our initial applications and the results of our first user-community study.

### 3.2 Initial P3-Systems

The initial suite of SmartCampus' P3-Systems includes: *CampusWiki*, a context-aware campus community Wiki that provides editable pages about campus places, people and organizations; *CampusMesh*, a location-aware social reminding, coordinating, and introduction system; *SmartCampus Social Desktop*, a friend-of-a-friend system linked that supports mobile device management; and *CampusNavigator*, which displays information about current and past activities at various campus locations. In addition, we have developed the *SmartCampus Assistant* which is used to load these other applications, set global privacy settings (locatability and interruptability) and help us model user behavior.

1. *CampusWiki*, a location-aware Wiki that allows users to collectively build a knowledge base about campus places, people, and organizations. Wikis support communities by enabling the creation of shared knowledge bases through collaborative authoring. Traditionally, Wiki content generation and retrieval are disconnected from the physical environment of users. Thus, the users' ability to support the creation and use of knowledge bases tied to relevant places for local communities is

limited. CampusWiki is designed so that mobile users can access this Wiki wherever they are and be provided with location-aware content for better socio-geographical navigation on campus. Furthermore, they can add or modify content relevant to various places.

2. CampusNavigator enables map-based “buddy awareness,” location-centered instant messaging, placed based recommendations and information including those generated by users through digital graffiti. One’s designated “buddies” can be located on campus if they are present (you can “see” a room and if a buddy is in it, if there is mutual agreement to sharing location data). Users can also decide to “cloak” their locations if they don’t want to be located. Besides seeing where your designated buddies are, you could send them an instant message, or leave a message on a place for them to see when they turn their device on next.
3. CampusMesh is a location-aware friend-of-a-friend system for social introductions, alerts and reminders. It would start by asking you and the other users of this service for a list of your interests and friends and co-workers and how you know these people. It will also be populated by data such as class lists available through the registrar, so that classmates can be automatically identified. Then, you could use the system to try to meet new people with whom you have an interest, an activity (such as a class or club) or a friend in common.

Theoretical analysis of the P3-System design space [3] in terms of privacy concerns suggests that each of these initial SmartCampus applications will have their own unique set of privacy issues that we will have to address.

*CampusWiki*’s main P3-interaction technique is use of virtual spaces that match physical locations for text-based discourse. This technique raises social concerns associated with traditional computer-mediated communication (such as anonymity enabling flaming) and in addition raises new concerns regarding ownership and location based access control. For example, the manager of a physical social space may wish to have extra control over the associated matching online content, even if a diverse community of users produces it. Further, in some instances it may only be appropriate for in situ users to be able to read and/or contribute to the community knowledge base as a means of controlling institutional reputation. In the case of CampusWiki this means that while students can post what they like, it cannot be read by users that do not have passworded access to the university network.

*CampusNavigator*’s presentation of dynamic activities pertaining to campus places’ through the use of matching virtual places distinguishes it from the other applications. This P3-System technique raises particular concerns in regarding the use of search to track individuals.

*CampusMesh*, with its focus on the use of P3-System collocation techniques to support affinity matching, raises concerns regarding information overload and identity management. For example, does a young woman entering a campus cafeteria want to take the chance of being inundated with notifications? Does she want to have to look around to figure out which of the nearby men is “Smartpants96”? Will she be disclosing her identity as soon as she looks around? Other issues arise when asynchronous processing is added to the mix. For example, proximity history could inappropriately reveal a budding romance.

While the P3-System framework gives us a reasonably nuanced understanding of the relationship between major design techniques and basic privacy concerns, it is important that we gain a deeper understanding in various real world contexts. Further, to maximize utility and usability, and to minimize possible negative social impacts of SmartCampus applications, we believe we should involve our community in all stages of design. This means both finding means to appropriately collect user information (their important places, friends, current location, etc.) and designing mechanisms for appropriately sharing users’ data through this model, e.g., plausible deniability, progressive identity revelation, trust and reputation measures, various user-controlled privacy settings. As part of this process, prior to the release and detailed specification of our initial set of SmartCampus applications, we conducted semi-structured interviews aimed at understanding better the potential needs and concerns of our user community. The open-ended questions explored prospective users’ initial attitudes towards possible ‘generic’ P3-System applications, within a university context. The interviews focused on perceived benefits, their concerns, and their intention to use such services if available.

### 3. Research Methodology

The first set of semi-structured interviews were conducted with a cross section of representatives of types of users (students and faculty and staff; residents and commuters; undergraduates and graduates, etc.) during the first few months of test-bed development. Thus, the opinions gathered at that time were used to influence the features and even the name of the systems under development.

#### 3.1. Procedures: The Interview Guide

At the time of the initial interviews, no prototypes were available to present to subjects. Our aim was therefore not to test core usability concerns but rather to derive a general understanding of user perceptions. The interview guide included a brief description of the SmartCampus project and a brief description of the then hypothetical applications being developed for the project. The guide presented a

brief scenario to illustrate the possible uses of each of these hypothetical applications. Each scenario was followed by a series of questions aimed at eliciting from the respondents information such as interest in the services provided by smartcampus systems, anticipated uses, concerns and possible reasons for not wanting to use the hypothetical applications. The interview guide also included questions on the respondents' current use of mobile wireless devices, their attitudes towards them and their general background (age, race, residence, degree program and year).

Prior to conducting the interviews, the interviewers, who were NJIT students in courses in Qualitative Research or Computers and Society, completed two training programs: an online course in the protection of human subjects offered by the US Dept of Health and Human Services Office for Human Research Protection, and a face-to-face lesson on conducting semi-structured interviews. Initial transcripts were required to be posted for quality inspection before the interviewers could proceed to conduct subsequent interviews. The study director and the student interviewers kept in continuous contact through an asynchronous conferencing system, so that any problems or questions or concerns could be discussed.

Below is the fourth version of the explanation and scenario used for a hypothetical application called "SmartCampus Explorer" similar to UCSD's ActiveCampus explorer, to illustrate the extensive information necessary to obtain informed opinions about an application that did not yet exist. It took four iterations until we found an explanation and scenario that was clear to all and did not raise more questions than it answered.

*"NJIT's Campus Explorer will enable map-based "buddy tracking," location aware instant messaging, and digital graffiti. What this means is that you would have a list of "buddies" who agree to allow you to see a map showing where they are on campus, when they are there and have their mobile device turned on. Users can also decide to "cloak" their locations if they don't want to be located. Besides seeing where your designated buddies are, you could send them an instant message, or leave a message on a place for them to see when they turn their device on next.*

*For instance, suppose it is lunch time and you want to see who is around; you could discover that one of your friends is near the volleyball court now, and send an instant message to ask if he is free to meet you at the cafeteria. By "digital graffiti," we mean that you could leave messages about places that will show up when other users scan that part of the campus map; for instance, you could note whether the daily special at the cafeteria is good or bad today. This graffiti will generally 'disappear' within 24 hours, so it is always timely."*

### Activity Scenario of Hypothetical SmartCampus Explorer

"Here's a scenario about one idea of how a student might use our hypothetical SmartCampus Explorer, for instance:

*Jane is working on a group project for her graduate course in Management. The group has been communicating by email but has a number of unresolved issues. It's an hour before class, and she wonders if they might already be on campus. They have all made each other "buddies" for the Campus Explorer System, so when she looks, she sees that two out of three are on campus already-one in the Library and one in the parking lot. She Instant Messages them and they agree to meet in Starbucks. After talking for a half hour, they have a question for the professor; Jane checks and he is visibly in his office, so they go to talk to him. By the time class starts they have been able to improve their plans a lot."*

After the explanation and scenario to explain each planned application, a set of open-ended questions was asked, including planned probes. The set for our hypothetical Campus Explorer was:

"1. Anticipated use - Do you think you would like to use the Campus Explorer? (If yes, what do you think you would use it for? If not, why not? )

If yes: Follow-up/ probes

What kinds of people do you imagine you would be willing to make a "buddy" who could track your location on campus?

2. Concerns - When you think about the Campus Explorer "buddy locator" system, what kinds of reactions and concerns come to mind? (Follow up with many probes on each of these and finally "anything else?")

Place probes: Are there places on campus where you would not like your exact location to be known, even to your buddies?

Times probes: Are there times of the day or week when you think you would want to turn off this tracking system, or that it should be turned off for the whole campus?"

The interviews were conducted and transcribed as a course project by students who were first trained in the technique of semi-structured interviews, and then coded using NVivo®, software to support content analysis. The initial major coding categories followed the topics listed in the interview guide, e.g., "concerns about CampusWiki features," while sub-categories, e.g., types of concerns, emerged through examination of the data. Two coders were used in order to increase reliability. They individually coded part of the same transcript and discussed discrepancies. These discussions set the guidelines for the rest of the coding, and the rest of the transcripts were coded independently, with exchange of information about

the addition of new categories that were emerging from the data.

### 3.2. Sample

The sample, being small, was not random but was rather a type of quota sample. Each interviewer, who interviewed three or four subjects, was instructed to be sure to include both campus residents and commuters, both undergraduates and graduates, both males and females, and to try to include one faculty or staff member if possible. The NJIT campus community is ethnically very diverse. Thus we are assured of having a range of viewpoints.

**Table 1. Demographic distribution**

		No. of Subjects (%)
Gender	Female	13 (20.0)
	Male	35 (53.8)
	N/A	17 (26.2)
Status	Undergraduate	37 (56.9)
	Graduate	8 (12.3)
	Faculty/Staff	18 (27.7)
	N/A	2 (3.1)
Age	under 20	16 (24.6)
	20-29	27 (41.5)
	30-39	2 (3.1)
	40 and over	14 (21.6)
	N/A	6 (9.2)
Campus Residents/Commuters	Residents	23 (35.4)
	Commuters	27 (41.5)
	N/A	15 (23.1)
Ethnicity	Caucasian-American	23 (35.4)
	Asian	11 (16.9)
	Hispanic	6 (9.2)
	African-American	3 (4.6)
	Others	4 (6.2)
	N/A	18 (27.7)

A total of 65 NJIT campus members were interviewed and transcribed (18 of the 65 subjects were faculty or staff). The demographic distribution of the sample is as follows:

Although the sample was not randomly selected, it is broadly representative of different types of members of the NJIT campus community; for instance, about 20% of the NJIT students are female. It does over-represent undergraduates and faculty and staff, and under-represent graduate students and African-American students.

### 4. Results

The SmartCampus test-bed seems to be accepted positively by its prospective users. Regarding interest in using the SmartCampus applications, most respondents said that they would use them, except for our hypothetical location-aware introduction system.

**Table 2. Anticipated use of SmartCampus**

		No. of Subjects (%)
CampusWiki	Yes	48 (73.8)
	No	8 (12.3)
	Not sure	6 (9.2)
	N/A	3 (4.6)
SmartCampus Explorer	Yes	43 (66.2)
	No	15 (23.1)
	Not sure	1 (1.5)
	N/A	6 (9.2)
CampusMesh	Yes	26 (40.0)
	No	28 (43.1)
	N/A	11 (16.9)

Given that the system continues to evolve and the biggest goal of this research is to find prospective users' perceptions about the system, the coding scheme was developed based on the two major questions in the interviews: anticipated benefits and concerns. The following section discusses what kind of potential benefits and concerns were identified by prospective users.

#### 4.1. Benefits

Most students were quick to see the possible benefits of a community system that can allow one, for instance, to see the campus location of all their buddies at a glance. For example, a female freshman who lives on campus says, "Definitely seeing if my friends are here is actually a good thing. I leave on weekends but I'll come back some time Saturday night, I never really know if they are here or who is here. So I have to end up calling a lot of people. So that would be nice to come back to campus to say, Oh, look, they're here!"

The content analysis coded a total of 151 passages in terms of anticipated benefits of the three applications. The biggest benefits identified were to check campus events, find people on campus, and social networking for CampusWiki, SmartCampus Explorer, and CampusMesh, respectively. (Note that some of the perceptions of which application would do what are not correct; for example, the CampusWiki will not "find people on campus," SmartCampus Explorer will. This confusion among applications is quite understandable given that the subjects had not actually seen or used any of the applications; nevertheless they are informative about what kinds of uses are anticipated for the entire set of applications.

**Table 3. Coding of anticipated benefits**

	Coded Passages
CampusWiki	Check campus events (26)
	Exchange information (13)
	Check crowdedness of places (10)
	Find people on campus (6)
	Use as bulletin board (5)
	Use time more efficiently (2)
	Collaborative work (1)

	Play games (1) Advertisement (1) Emergency management (1) Other (1)
SmartCampus Explorer	Find people on campus (30) Increase communication channels (5) Collaborative work (4) Community building (3) Check school event (2) Paging (2) Election promotion (1) Check schedule of tutoring center (1) Use office hours flexibly (1) Other (2)
CampusMesh	Social networking (16) Make friends (8) Identify people (7) Form study group (2)

## 4.2. Concerns

A total of 177 passages were coded regarding concerns about the SmartCampus system. The “huge, big fat issue of privacy” was raised for all three potential applications, but was especially prevalent for SmartCampus Explorer where privacy concerns represented over half of the responses. Even though the device can be ‘turned off’ or cloaked, there is great fear of the information on one’s location being made available to inappropriate people. For some this is just a general distaste. For instance, a male junior says, “I don’t want a computer knowing everything, and I don’t know who’s looking at this stuff... someone else that you didn’t want knowing where you are, asks your friend who knows where you are.” A female freshman also says, “Well, first of all, being tracked all the time and knowing where everyone is. That’s a little bit of invasion of privacy.” An Hispanic graduate student adds, “...but something out there is still monitoring where you are. So yes, I would feel a little creeped out or angry if I ever, ever discover that that was being used in any [unintended] way.”

For others, it takes the form of fear of the information being used for stalking, and of a lack of awareness of exactly who might be checking your location. An Hispanic freshman says, “People can add someone and not realize that that person can be a stalker.” A frequent opinion is that even though the system could identify the exact room in which a buddy is located, this is too threatening: “I’m not sure I would like a fine detail on exactly where I’m at. Being in the building, say in the campus center, is good enough. It doesn’t need to be exactly Starbucks or the ladies room,” says a female graduate student in her 40s.

Balancing these concerns are suggestions that the location system could potentially be used to increase campus safety. For instance, one potential user suggested that a kind of “911 code” could be silently sent to security,

which could then see exactly where the assistance request is coming from.

In addition, given that the application can send a message to others without a prior permission, the prospective users also have a concern about interruption. A male staff member says, “But con would be that if you are in a lecture room or studying in a library and somebody sends you a message or interrupts you, it will disturb your study.” A freshman living on campus observes, “You don’t want people following you around and just annoying you or whatever.”

For the hypothetical CampusWiki, over half of those describing a concern mentioned something having to do with the validity of the information that is posted, since anonymous posting is allowed. This is related to a desire for editor or moderator roles to assure appropriateness of material. For example, an undergrad living on campus says, “Maybe people can enter wrong information... ‘Oh, there’s a big party at Ballroom C.’ and you go there and there’s nothing there.” An undergrad Caucasian-American also expresses concerns saying, “I guess you could have people posting incorrect material, and some peoples’ interpretation of events differ, it may not always be accurate.” More seriously, a Caucasian-American male living on campus says, “People will post comments about other people, which may be considered slander. People can pretty much say anything about anyone.”

The concern about validity of data is also expressed as a concern about absence of moderation. A male staff says, “Yeah, keep it monitored, so only the comments that actually make sense for people, not some junk, can remain on the system.” A sophomore commuter adds, “Unless someone is dedicated to updating it, maybe some people won’t do it, except organizers of the event. If it is laid on very quickly, like an impromptu event, it may not be documented.”

For CampusMesh, the location aware friend of a friend system, the major concern is privacy, followed by intrusiveness and concerns that the information that people enter about themselves may not be accurate but rather an exercise in what might be termed extreme impression management, or probably worse, a way of playing practical jokes on people. A male junior says, “The bad thing, people can randomly message you and say that they want to meet you somewhere and they are just playing around with you.” Referring to intrusiveness, an African-American male living on campus says, “If you’re just sitting in the cafeteria and it vibrates like a million times... sometimes you just don’t want that, you just want to be left alone. So, it might be too invasive.” A male freshman says, “I think there are some restrictions there; because, I would like to meet a friend of a friend to get acquainted, and he or she might be in a bathroom or somewhere private and the machine kicks off and this will make them feel personal, when someone tries to get in touch with them while they are at private place or they are in class.” A male staff says, “...but it could get annoying at times when you don’t want

people to message you, unless you message them. Just because you have common friends and interests with some people, doesn't necessarily mean that you would want to meet them."

Validity of data is also a concern. A male staff in his 30s says, "First thing that comes to my mind is that I have no clue what kind of information my friend has entered in the system. If that friend is not a good friend of mine then he can enter data which does not reflect my personality." An Asian student living on campus is concerned, "But there's so many misuses that you can use with this, cause people can be lying about their credentials, people could be lying about people they know."

**Table 4. Coding of concerns**

	Coded Passages
SmartCampus Explorer	Privacy (37) Interruption (7) Stalking (7) Personal security (5) Tracking by others (4) System security (3) Buddy list control (2) Other (5)
CampusWiki	Validity of data (22) Privacy (10) Absence of moderation (8) Overload of irrelevant information (4) Slander and negative comments (4) Hard to use (3) Distraction in class (1) Filtering by user privilege (1) System security (1) Other (3)
CampusMesh	Privacy (10) Intrusiveness (9) Validity of data (9) Loss of control (8) Availability for specific purposes (2) Control by users (2) Negative evaluation for not using it (1) Personal security (1) Security of data (1) Trust (1) Other (1)

**Table 5. Coding of privacy concerns**

	Coded Passages
Privacy concerns	Big brother (6) Identity theft (5) Personal information collection (5) Mugging (3) Different levels of information disclosure (3) Stalking (2) Data validity (1) Privacy policy agreement (1)

In order to delve into privacy concerns of the respondents, probes were used for examples or explanations. Based on the answers, a total of 26 passages were coded as major privacy concerns. The biggest privacy concern is fear about 'big brother' followed by identity theft and personal information collection. For example, a male undergrad says, "...that's just kind of creepy. I mean I don't want to be clichéd but it's kind of like big brother and all that, just being able to be tracked down." Identity theft and personal information collection are also privacy concerns. A male junior says, "Maybe data mining or collection of information or theft of identity could be a threat to privacy." A female senior says, "My personal information should not be shared with others like my social security number or other personal information."

## 5. Limitations

Before discussing the findings in general and some of the design implications that we have extracted from the more detailed qualitative feedback it is important to note again the major limitation of this study. It was not possible to use prototypes to enable the respondents to experience the functionalities of any of the SmartCampus applications, and therefore, a printed copy of an early version of the proposed main interfaces as well as use scenarios were employed by the interviewers to describe the system. The use of the scenarios could have given respondents a very narrow perspective of the system capabilities. Consequently, several of the responses were directly related to the specific scenario given. It may have been more effective to construct a mockup of the application [15]. The construction of a mockup would involve the development of a prototype interface scenario and the use of a professionally produced video of this scenario in order to illustrate the ways in which the SmartCampus applications could be used. On the other hand, since details of the design and interface were not known at the time of this exploratory study, such "concreteness" may have sidetracked respondents into commenting on details of the prototype interface rather than on the general concepts of the services that could be provided, which was the purpose of this study.

It must also be noted that similar types of location-aware systems are and will be developed to serve commercial rather than social networking needs (see, e.g., [14]). For instance, these commercial applications will be able to direct a person to a restaurant or event nearby that is of potential interest. The concerns and benefits from commercial applications of P3 systems are likely to be different in many ways.

## 6. Discussion

The level of interest in using the SmartCampus applications in the future and concerns raised by the

respondents show some widespread attitudes of people towards the privacy issue that must be taken into account in the design and deployment process. The content analysis results find more passages associated with concerns, a significant portion of which are about privacy, than those associated with benefits (177 vs. 151). Nonetheless, most respondents said that they would be willing to use the SmartCampus applications. This could be an artifact of it being easier to talk about concerns about an unseen application than benefits, or perhaps reflective of previous findings that people can be divided into three groups in terms of their attitude towards privacy: the marginally concerned, the privacy fundamentalists, and the pragmatic majority [12]. The respondents in this study seem to belong to the pragmatic majority who may trade privacy for benefits. Although they are concerned about privacy, they would use the applications because expected benefits may exceed their concerns.

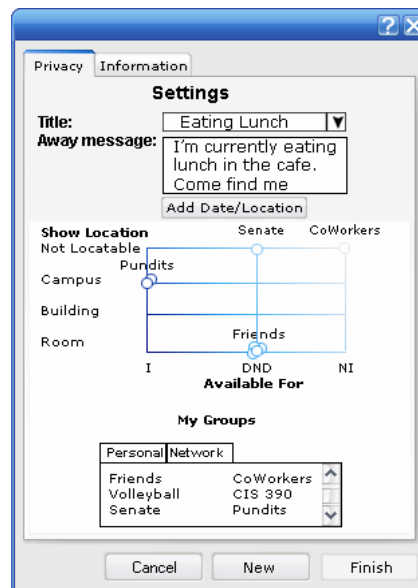
Furthermore, the incorporation of the suggestions made in this study into the system design is paramount. For instance, some respondents who were concerned about being interrupted at inappropriate times indicated that although the cloaking feature would be useful at these times, it should be possible to filter through high priority messages. A feature that prioritizes instant messages and alerts users only when they receive messages of high priority is therefore desirable. Respondents described high priority messages as not only being dependent on the sender but also the content of the message. Another example is that several respondents mentioned that they thought that a bathroom was an inappropriate location to be identified; as a result, SmartCampus Explorer will not identify such rooms, but only give a more general location, such as a floor of a building, for somebody who is in a bathroom.

These findings about user perceptions have a number of fundamental design implications. One is that privacy and information management for our user-community goes hand-in-hand. Individuals want P3-System services but they want to be able to ensure that they are not inappropriately interrupted, inundated with inappropriate messages, or constantly required to manage their availability settings. As a result, we believe that we need to provide users with:

1. A simple user interface on both mobile and desktop personal computing devices for the unified management of personal global SmartCampus privacy settings. Settings modified on this interface should be able propagate to all SmartCampus applications such as *CampusMesh*, *CampusNavigator* and *CampusWiki*.
2. Privacy management tools that enable users to simultaneously adjust both locatability and interruptability / availability.
3. The ability to set their preferences so that they are semi-automatically implemented (context-aware [9]) by the system based on location, time and social connectivity.

## 7. Future Research

The design implications of this study are being directly explored through our Smartcampus Development efforts.



**Figure 2. SmartCampus assistant mobile privacy manage UI**

For example, we are exploring unified privacy management techniques. Figure 2 presents a UI that we are experimenting with inside of the *SmartCampus Assistant* that will support the three requirements listed above. It allows the users to specify for social groups or places how locatable and interruptable they are by placement on a privacy grid. The X axis sets the degree of locatability and the Y axis the degree of interruptability, from interruptable, to a “do not disturb/away” message that passes through communication requests, to not interruptable, that simply provides an away message to users who attempt to communicate. In addition to this unified UI approach, we are also exploring when and where and how it is appropriate to propagate changes made in one SmartCampus application to other P3-Systems.

Taking into account community feedback from this study our *CampusWiki*, which is now implemented, is only accessible to those that have logged into our university network. In this way it can protect the university’s reputation while giving students a community outlet. Further, while it remains true to the Wiki principle of free community authorship, a tight group of students proof every new page creation and edit for unambiguously offensive content which they simply remove.

To build on and complement this work, we will be measuring and tracking student and faculty social and professional networks on campus, using a different set of techniques and instruments [17], as well as our *SmartCampus Social Desktop* application which provides users with an interface that allows them to see and leverage social ties and affinities. Our overall objective is to grow

the size and strength of social networks on campus, without causing undue problems related to invasion of privacy or intrusiveness of the applications.

This pilot study lays the foundation for a longitudinal study at various stages after the implementation of the SmartCampus test-bed and applications to measure actual acceptance of the technology and the concerns at those times. A comparison can then be made between actual acceptance and the level of interest in participation discussed earlier. Also, it might be possible to determine whether (a) the concerns in the subsequent studies are similar to the current ones expressed in this study, (b) new concerns surface after SmartCampus applications are adopted and put to use, or (c) any concern prior to using them disappears. We plan to use the categories and concerns developed in this set of semi-structured interviews to devise an online questionnaire that can be administered to users periodically to see how their concerns change with use. We also hope to be able to build theoretical models that will help to predict and explain the sources and strength of various types of privacy and intrusiveness concerns.

## 8. Acknowledgements

This research is partially supported by the National Science Foundation (NSF CISE 0454081 and 0534520); the opinions expressed are those of the authors and may not reflect those of the NSF. Among the many faculty and staff members of the SmartCampus team who have contributed to the project are Sameer Bajaj, Cristian Borcea, Sukeshini Grandhi, Nataniel Laws, Constantine Manikoupoulos, and Katia Passerini. The students who conducted and transcribed the interviews include Kristan Budhu, Andrew Corea, Cathy Dwyer, Richard Egan, Maia Eliozashvili, Elizabeth Avery Gomez, Steven Kominski, Vishal Kubani, Yun Chi Li, Alexander Onik, Umar Quasim, Ronald Singh, Tim Sneed, Kim Skov, Daniel Tymesco, Todd Will, and Paul Wozniczka.

## 9. References

[1] Q. Jones, C. Borcea, S.R. Hiltz, C. Manikopoulos, and B. Amento, "Urban Enclave Location-Aware Social Computing", *Proceedings of Internet Research 7.0: Internet Convergences*, Brisbane, Australia, 2006.

[2] Q. Jones and S.A. Grandhi, "P3 Systems: Putting the Place Back into Social Networks", *IEEE Internet Computing*, Sept-Oct 2005, pp. 38-46.

[3] Q. Jones, S.A. Grandhi, L. Terveen, and S. Whittaker, "People-To-People-to-Geographical-Places: The P3 Framework for Location-Based Community Systems", *Journal of Computer Supported Cooperative Work*, 13(3-4), 2004, pp. 249-282.

[4] F. Espinoza, P. Persson, A. Sandin, H. Nystrom, E. Cacciatore, and M. Bylund, "GeoNotes: Social and Navigational Aspects of

Location-Based Information Systems", *Proceedings of Ubicomp*, 2001, pp. 2-17.

[5] W.G. Griswold, R. Boyer, S.W. Brown, T.M. Truong, E. Bhasker, G.R. Jay, and R.B. Shapiro, "ActiveCampus - Sustaining Educational Communities through Mobile Technology", *Technical Report CS2002-0714, Computer Science and Engineering*, UC San Diego, July, 2002.

[6] R. Want, A. Hopper, V. Falcão, J. Gibbons, "The Active Badge Location System," *ACM Transaction on Information Systems*, 10(1), January, 1992, pp. 91-102.

[7] AT&T Laboratories Cambridge, "The Active Badge System", 2002, available online at: <http://www.cl.cam.ac.uk/Research/DTG/attarchive/ab.html>

[8] R. Harper, "Why people do and do not wear active badges: A case study", *Journal of Computer Supported Cooperative Work*, 4(4), 1995, pp. 297-318.

[9] I. Barkhuus and P. Dourish, "Everyday Encounters with Context-Aware Computing in a Campus Environment", *UbiComp*, 2004, pp. 232-249.

[10] B. Donald, "MIT Wireless Network Tracks Info On Users", Boston.com, November 3, 2005, available online at: <http://www.boston.com/business/technology/articles/>

[11] MIT "iSpots: Living and Working on MIT's Wireless Campus", 2005, available online at: <http://iSpots.mit.edu>

[12] A.F. Westin, Harris-Equifax consumer privacy survey 1991, Equifax Inc., Atlanta, Georgia, 1991.

[13] M.S. Ackerman, L. Cranor, and J. Reagle, "Privacy in e-commerce: examining user scenarios and privacy preferences", *Proceedings of ACM conference on electronic commerce (EC'99)*, Denver, Colorado, November, 1999, pp. 1-8.

[14] S. Spiekermann, J. Grossklags, and B. Berendt, "E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior", *Proceedings of ACM conference on electronic commerce (EC 2001)*, Tampa, Florida, October, 2001, pp. 38-46.

[15] M. Mantei and T.J. Teorey, "Cost/Benefit Analysis for Incorporating Human factors in the Software Cycle", *Communications of the ACM*, 31(4), April, 1988.

[16] C.F. Maitland, E.A.M. van de Kar, U. Wehn de Montalvo, and H. Bouwman, "Mobile information and entertainment services: business models and service networks." *Int. J. Management and Decision Making*, 6(1), 2005, pp.47-64.

[17] L.S. Plotnick and S.R. Hiltz, "Measuring Social Networks for SmartCampus", *Proceedings of America's Conference on Information Systems*, Acapulco, August, 2006.