A FRAMEWORK FOR USER-CENTRIC PRIVACY MANAGEMENT IN SMARTPHONES REGARDING BLUETOOTH LOW ENERGY BEACONS

by

Emmanuel Anokhuagbo Bello-Ogunu

A dissertation submitted to the faculty of
The University of North Carolina at Charlotte
in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in
Computing and Information Systems

Charlotte

2016

Approved by:

____
Dr. Mohamed Shehab

____
Dr. Bill Chu

____
Dr. Heather Lipford

____
Dr. Weichao Wang

____
Dr. Boyd Davis

ABSTRACT

EMMANUEL ANOKHUAGBO BELLO-OGUNU. A framework for user-centric privacy management in smartphones regarding Bluetooth Low Energy beacons. (Under the direction of DR. MOHAMED SHEHAB)

Businesses and organizations such as retail stores, airports, and hospitals have begun to leverage the recent advances in localization technology to provide quality location-based services to their customers. Beacons are one example of this technology, which use Bluetooth Low Energy (BLE) signals to broadcast a unique identifier that is detected by a compatible device to determine the location of nearby users. Beacons can be used to provide a tailored user experience with each encounter, yet can also constitute an invasion of privacy, due to their covertness and ability to track user behavior. This is coupled with their potential for targeted advertising, and a lack of available information regarding their usage, degree of threat, and control. Therefore, I hypothesize that user-driven privacy policy configuration is key to enabling effective and trustworthy privacy management during beacon encounters. To accomplish this goal, I first investigate users' awareness and perceptions of beacons. I identify the privacy concerns users have, the related information they are willing to share, and the challenges they experience regarding the context of beacon encounters. I then demonstrate the effectiveness and usability of a crowdsourcing-based approach to deriving context-based beacon categorization and privacy labels. Lastly, I develop a framework for beacon privacy management that provides a policy configuration platform. Through evaluation of a proof-of-concept, I test different configuration schemes to refine the framework and offer recommendations for future research.

ACKNOWLEDGMENTS

> *It is not necessary for all men to be great in action. The greatest and sublimest power is often simple patience.* -Horace Bushnell

If there is one virtue that is required, tested to its limit, and matured over the course of a doctorate program, it has to be patience. Without the grace of God and the intercession of the blessed Mother Mary, I would not have had the patience to continue on this long and arduous journey to a PhD, nor the power to persevere through the many challenges that I faced along the way. Hence, first and foremost I give thanks to my heavenly parents, and I acknowledge the grace bestowed on me in the process.

Additionally, I have to thank my family for all that they did for me, from the words of wisdom to the home-cooked meals, and everything in between. John and Veronica, my parents, instilled in me the value of education and a commitment to success, and more than that, their own pursuit of advanced degrees served as visible examples of what was possible. Their constant message to me was to "place no limits on yourself where none exists, for possibilities are limitless." My younger siblings, Perpetua, Veronica, Faustina, Mariam, John Jr., and Felicity additionally provided encouragement and support, but also much needed levity throughout. On top of that, my siblings kept me humble: doctorate or not, I'll always be the same old nerdy brother to them; thankfully, that will never change.

I'd like to express heartfelt gratitude to my mentor and advisor, Dr. Mohamed

Shehab, whose expertise was invaluable in guiding me in the right direction. I believe one of the single most important factors to success in a doctorate program is having the right academic advisor, and I was fortunate in having one so knowledgeable, hands-on, and above all, curious. Moreover, he deftly balanced the ability to both support me and challenge me, allowing me grow into an independent researcher that never stopped questioning. Furthermore, my dissertation committee, consisting of Dr. Heather Lipford, Dr. Bill Chu, Dr. Weichao Wang, and Dr. Boyd Davis, offered their expertise and scrutinized my work, which helped to broaden the value of my contributions. Though not on my dissertation committee, Dr. Jamie Payton and Dr. Zbyszek Ras were also faculty members who were instrumental in fostering the necessary skills to be successful in my doctorate program.

The work in this dissertation would not be possible without the funding I received from various sources, including the Federal CyberCorp Scholarship for Service (SFS), Graduate Assistance in Areas of National Need (GAANN) Fellowship, and a Google Research Award. This significant support allowed me to focus on contributing high caliber research without concern for how to manage the financial demands of my program.

I had the good fortune of working with many stellar colleagues throughout my graduate career. Through various conversations, and even collaboration in some instances, these individuals promoted valuable exchanges of information, and they helped to elevate the quality of my work to a higher standard. In no particular order, these colleagues included Fadi Mohsen, Abeer AlJarrah, Yousra Javed, Stephen MacNeil, Mick Smythwood, Scott Heggen, Pamela Wisniewski, Daniel Yonto, and

Coline Dony. I am especially grateful for the many interactions I have had with them, and will always treasure the relationships formed with them.

I would be remiss not to mention my closest friends and biggest fans, who provided a level of support that could not be matched by anyone else. Words are not enough to explain how grateful I am to Osarieme Omokaro for standing by me and being my mirror, my sounding board, and my font of inspiration. She is a giant on whose shoulders I stood to reach new heights, and I will be forever grateful for her presence. To my best friend, Jonathan Lee, I say thank you for being there for me, for fact checking me, and for taking genuine interest in my research. If I could, I would give him an honorary doctorate for the amount of effort put into helping me advance my work. Additionally, I'd like to acknowledge Ryan Hess and Jake Lussier, two people that were continually in my corner, both in a professional and personal capacity. I appreciate them for always reminding me to celebrate the little victories along the way.

Lastly, I'd like to recognize the countless participants, reviewers, and other scholars, too many to name here, whom I have met, interacted with, or relied on along the way. Without these people, I would not have been able to make any progress in my research.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

Smartphones are experiencing tremendous adoption and growth, with the latest statistics reporting more than half of all U.S. adults now owning smartphones, and 76% of millennials using smartphone devices [38]. The increasing trend toward widespread smartphone usage is only further pushing businesses and technologies to focus on mobile experiences in order to remain competitive and draw more customers. Furthermore, the Internet of Things (loT) has become a powerful force for business transformation, and its disruptive impact is currently being felt across all industries and all areas of society. Gartner predicted that 4.9 billion connected things would be in use through 2015, which would be a 30% increase from 2014, and would reach 25 billion by 2020 [17]. Bluetooth Low Energy beacons are an example of "Internet of Things" (IoT) technology that is experiencing early adoption in a wide array of industries. The beacon technology consists of new low-powered and low-cost bluetooth transmitters that can notify bluetooth-enabled smartphones of their presence. Beacons use Bluetooth Low Energy (BLE) technology to frequently broadcast a universally unique identifier, which is picked up by a compatible app or operating system and sent over the Internet to determine the device's physical location. This technology enables smartphones to determine the precise location of the current user in both outdoor and indoor contexts. Being able to seamlessly locate the precise location of users gives way to a wide spectrum of applications. For example, retail stores can pinpoint the products customers are interested in during their in-store visits, which can be used to provide real time advertisements or discount notifications on the user's smartphone. In 2014, twenty of the 30 Major League Baseball parks have installed beacons to guide fans to their seats, provide “bonus" content, and promote team merchandise [46]. Moreover, Macy's recently expanded the use of beacons to all of its stores nationwide; this rollout marks the largest beacon deployment in retail to date, with more than 4,000 devices planned to power engagement and marketing efforts throughout the department store chain [16].

Despite their obvious utility, the seamless and precise tracking capabilities of the beacon technology raises several privacy and security concerns. This is also coupled with their potential for use by third-parties to provide targeted advertising, and a lack of consumer information regarding their usage, degree of threat, and control. Recently, a company that controls thousands of New York City's phone booth advertising displays had planted tiny beacons in pay phone booths in Manhattan to track people's movements [4], and this was immediately denounced by several privacy advocates. Users should be notified when they are in a zone that contains beacons and should be given the choice to opt-in or opt-out. Given these issues, I believe there is a need to address several challenging questions:

- What do people know about Bluetooth Low Energy beacons?
- What forms of location-related information disclosure associated with BLE beacons can pose a privacy risk to users?
- What mechanisms should beacon providers enable to ensure user privacy during

beacon encounters?

- What tradeoffs can be made in beacon encounter information in order to convince users to share limited yet still meaningful information?

These are critical questions that need to be answered in order to facilitate the adoption of this technology. Some approaches have been proposed to address similar location privacy concerns in related technology [7, 35, 37, 45]. The related work is covered in more detail in Chapter 2. However, as BLE beacons are an emerging technology, there is a need to conduct an investigation specific to beacon technology. Such research can contribute to the design of a user-centric beacon privacy framework that is general and flexible enough to ensure information privacy in various circumstances without compromising the benefits of information disclosure. In this dissertation, I will make steps towards this direction.

1.1 Statement of Hypothesis and Approaches

This research presented here hypothesizes that:

User-driven and context-based privacy policy configuration is the key to enabling effective and trustworthy location privacy management during beacon encounters.

To accomplish this goal, I first investigate users' awareness and privacy perceptions toward Bluetooth Low Energy beacons. I identify the privacy concerns users have, the related information they are willing to share, and the challenges faced in understanding the context surrounding beacon encounters. I then explore a crowdsourcing-based approach to introduce context in beacon encounters during indoor localization. I demonstrate the effectiveness and usability of this crowdsourcing-based approach using a mobile app designed as a Game With A Purpose [48], to derive context-based beacon categorization and privacy labels. Given the feasibility of the crowdsourcing approach, I then propose the creation of a beacon privacy framework that will provide a user-driven, context-based policy configuration platform for beacon encounters. Lastly, I then perform a user study to evaluate the effectiveness of the framework and refine it, as well as offer recommendations on future work.

1.2 Summary of Contributions and Dissertation Organization

The contributions of this beacon privacy framework research are as follows:

- An identification of the privacy concerns users have, the related information that users are willing to share, and the limitation in users' understanding of context regarding beacon encounters.
- A crowdsourcing-based approach to introducing context in beacon encounters during indoor localization.
- A user-centric beacon privacy framework to provide users with context-based policy configuration and enforcement for beacon encounter information sharing.

The remainder of this dissertation is organized as follows: Chapter 2 discusses the Bluetooth Low Energy beacon technology in detail, reviews its current applications, and explores related work. Chapter 3 explores the current privacy perceptions surrounding BLE beacons, and discuss the results of the user study conducted that informed these perceptions. Chapter 4 provides some background information on the concept of crowdsourcing, and then I demonstrate the effectiveness of a crowdsourcing-based approach through the results of a separate user study. In Chapter 5 I introduce the framework proposed to achieve an effective and usable solution to location privacy management during beacon encounters, and in Chapter 6 I discuss the specific proof-of-concept developed to evaluate the beacon privacy framework through a user study. Lastly, Chapter 7 discusses future work and concluding remarks.

CHAPTER 2: BACKGROUND & RELATED WORK

Bluetooth beacons are based on Bluetooth Low Energy (BLE), or “Bluetooth Smart," which is part of the Bluetooth 4.0 specification. Standard Bluetooth is widely used in cars, audio equipment, mobile phones, and other technology for the purpose of transmitting large pieces of information up to approximately 100 meters. In fact, about 90% of all mobile phones sold today are Bluetooth-enabled, according to Bluetooth SIG [43]. The main focus of BLE, however, is delivering small amounts of data on low energy consumption through lower transfer rates. This minimizes the impact on a device’s battery life. BLE communication consists of two main types, namely advertising and connecting. Advertising is a one-way communication discovery mechanism, where devices that wish to be discovered transmit packets of data in intervals from 20 milliseconds to 10 seconds. The packets can have a maximum length of up to 47 bytes. BLE beacons only use the advertisement channel: they transmit data at regular intervals, advertising their presence, and this data is received by other devices, such as smartphones, as pictured in Figure 1. The beacon devices do not communicate through connecting, or pairing with other devices, as would be the case with devices on the standard Bluetooth protocol.

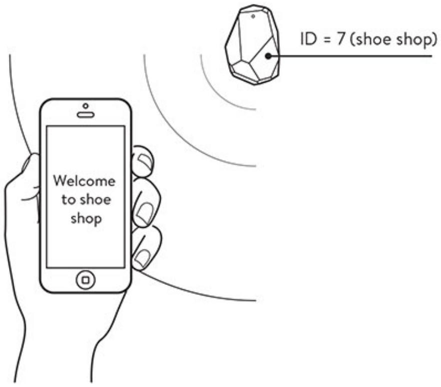


Figure 1: A representation of a smartphone detecting a beacon using BLE technology Source: community.estimote.com

2.1 iBeacons

In 2013 Apple introduced the “iBeacon,” the company’s proprietary implementation of the BLE beacon technology, at their 2013 Worldwide Developer Conference (WWDC). The underlying technology is similar to other BLE beacons, and all beacon solutions typically support iBeacon. The main difference comes from the data packet format. Apple’s iPhone 4s devices and newer, as well as the 3rd and 4th generation iPad and iPad Mini, all have built-in platform support for receiving Bluetooth Low Energy signals. They also support the peripheral role of BLE, which is where the smartphone itself can transmit BLE signals to other devices. Recently, newer Android devices have also come equipped with the BLE capability, but even with hardware support, the accompanying operating system needs to be version 4.3 (“Jellybean”) or higher to support BLE. Android version 5.0 (“Lollipop”) and later support the peripheral role of BLE. This means that a user can act as a “walking beacon” with their smart device.

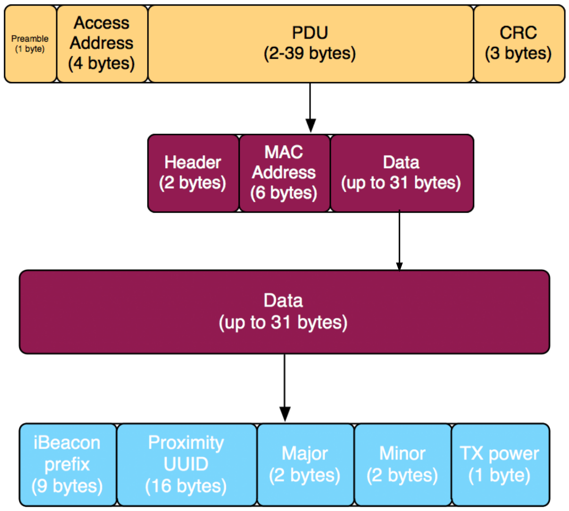


Figure 2: Beacon advertisement data packet

The format of the BLE data packet that is advertised, as pictured in Figure 2, includes a prefix (9 bytes), which is a fixed value reserved for each beacon manufacture. Next in the payload is the universally unique identifier (UUID), a 16 byte value which is used to distinguish beacons at a specific location. For example, the beacons belonging to a store chain will all have the same UUID value. The Major number (2 bytes) follows the UUID and is used to group a related set of beacons; again as an example, all beacons in a specific store would be assigned the same Major number. There is also a Minor number (2 bytes), which is used to identify individual beacons; for example, each beacon in a store will be assigned a different Minor number. Lastly, the TX power is the Received Signal Strength Indication (RSSI), which is the strength of the beacon signal measured at 1 meter from the beacon device. The TX power and the power measurement at the receiver are used by the receiver to estimate the proximity or distance of the beacon from the receiver (smartphone device). This proximity can be determined using one of two methods, as depicted in Figure 3:

- *Beacon monitoring*, which is where the entry and exit of beacon regions is measured; this happens can happen while the app is running in the background.
- *Beacon ranging*, where distances between beacons is calculated. This works only when the app is in the foreground.

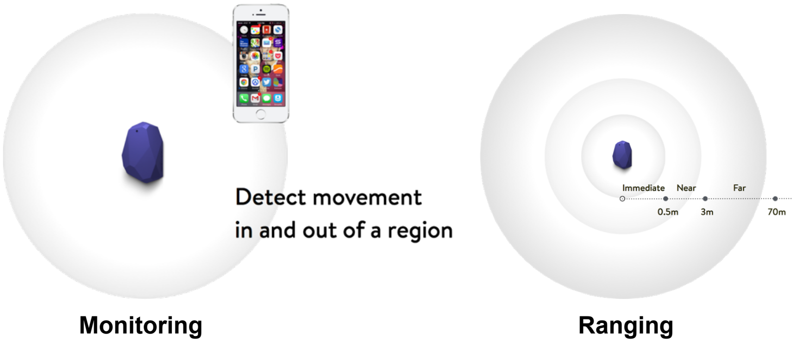


Figure 3: Beacon proximity determinations: monitoring and ranging

Source: community.estimote.com

When a user is within the proximity of a broadcasting beacon, the user's smartphone receives the beacon UUID advertisement, which is subsequently sent to the server via the smartphone apps registered to listen to beacon advertisements. In addition, the receiver is able to provide an estimate of the distance from the beacon based on the receiver's power. Figure 4 shows the interaction between the three main entities of beacon technology, namely the beacon, a user's smartphone, and an online server. In this architecture, the main computing device is the user's smartphone which has the beacon enabled mobile app installed, and is connected to the internet to send the user's beacon encounter to a server. Without the beacon-enabled app that is configured to detect beacons, a mobile device would not be affected by nor do anything with the received BLE advertisements. The beacon architecture allows

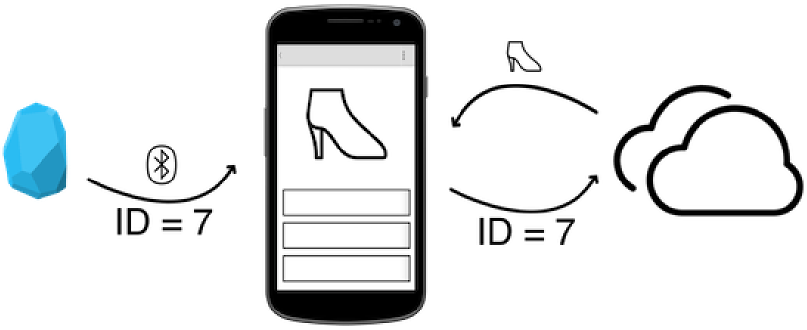


Figure 4: Interaction between a beacon, a smartphone, and a server

the retailer to know the beacons encountered by a given user, the proximity to these beacons, and the temporal behavior of the user in the beacon proximity. In addition, the retailer is able to track the user's movement in the store by correlating the beacon encounters in the store over a period of time.

The main metrics derived from the beacon encounters can be summarized as follows:

- Activity Path: How does the customer navigate in the store? The user's path in a region can be estimated by aggregating and triangulating multiple beacon encounters. This information is useful to retailers when designing product placement to ensure marketing and advertisement objectives.

- Activity Time: How long was the customer engaged in a particular activity? This information is estimated by aggregating the same beacon encounters and calculating the duration of time the user spends in the proximity of a specific beacon; this metric's accuracy is dependent on the beacon advertisement frequency and scanning rate of the smartphone.

- Visit Frequency: How often does the customer engage in a particular activity? This information is derived by computing the number of unique beacon encounters that occur per consecutive time frames. For example, it can be used to estimate the number of times the user has visited the store in a given month.

- Core Actions: Does the customer engage in actions that indicate they have adopted an idea, product, brand? For example, by performing causality analysis, it can be deduced what the user does after a beacon encounter. Did the user buy the product? Did she visit the mobile app?

2.2 Motivating Example

Although location-based services provide mutual benefits for consumers and retailers, one challenge is the growing privacy concerns of customers and the risk of location-based profiling. Retailers can infer things like personality traits, gender, ethnicity and economic status based on frequency of visits to certain locations, dwell times, and purchases. For example, imagine a college student that frequently visits the men's athletic wear section of his campus bookstore. This same student frequently visits the glassware section close to the shot glasses. From the frequency of aisle visits and duration of stay, it can be inferred that the student is probably a male and an athlete, but also potentially a heavy drinker or frequent partier. This could result in sensitive information that reveals intimate and personal facts about the student, which, if true, would likely be uncomfortable sharing, as it shows behavior conflicting with their role as an athlete and what is expected of them [18]. If this were false, this lends itself to an inaccurate persona formed of him. Consequently, the student should be equipped with a mechanism to manage his information privacy when it comes to beacon encounters. I intend to achieve this by defining beacon privacy policies at the mobile architecture level, in such a way that both the service provider and the customer can benefit from the aggregate data gleaned from location-based profiling, without putting customers at risk of privacy invasion.

2.3 Related Work

2.3.1 Online Tracking

One of the most common ways of tracking online consumer behavior and activities is through the use of browser cookies. Cookies are small text files used by web servers to identify and track users' browsing habits for sessions, days, months, years or indefinitely, depending on how they are configured [34]. Cookies are placed on a user's hard drive when they visit a website and are then used during subsequent visits to customize the browsing experience and provide targeted ads to the user. Although cookies cause no damage to files or systems, the use of cookies can constitute an invasion of privacy; their covertness and ability to track user behavior and browsing data for an indefinite duration of time, coupled with their use by third-parties to provide advertising, and a lack of consumer information regarding their usage, degree of threat, and control [34].

Numerous studies conducted on user awareness and perceptions of cookies shows that users lack a true understanding of their usage, function, advantages and disadvantages. In a study conducted by Ha et al., the majority of participants had no idea cookies were widely used on the web, and three out of four groups of users had vague knowledge of the malicious use of cookies and how to protect themselves [20]. McDonald et al. discovered that participants did not understand cookies or how Internet advertising worked, and a majority of participants erroneously believed that the sites they visited were legally barred from sharing their information. The study further revealed that the culprit was the browsers' user interfaces, which contributed to user confusion by mixing cookies, history, and bookmarks [33].

More recent studies have explored the effect of online tracking privacy practices on users' attitudes towards data sharing. Leon et al. investigated participants' willingness to share information based on four categories: length of data retention, view/edit access to data, range of websites on which advertising will be targeted based on data, and how well-known the website was [26]. Results showed that data retention time and scope of use significantly impacted willingness to share information; nearly half of the participants were unwilling to allow collection of any data. Furthermore, the majority of participants were not willing to pay any money to prevent data collection or remove advertising, believing that web privacy should be free.

In a sense, beacons are the “cookies" of the physical world [24]. Both can be used to personalize a user experience and track a user's path, both allow users to“opt-out" at any time (at the expense of reduced functionality and convenience), and the ethical use of both is largely up to the service provider and typically unknown to the consumer. Although the findings in these domains are relevant to beacons given these similarities in nature and use, there is yet to be a comprehensive study on the above issues in the context of physical BLE beacons in the real-world. Research studies specific to BLE beacon technology are imperative because the existing research on cookies and online tracking may not necessarily translate to the physical world, especially regarding information inference, identity management, and physical safety.

That is therefore a goal of our research, and such related studies serve as a guide or reference point for my beacon research.

2.3.2 Location-Based Services

In general, legal and constitutional privacy protections and policies have not kept pace with technological change [37]. The regulations regarding information collected, stored, and shared by the organizations providing location-based services (LBS) is often unclear, leading to distrust on the part of the consumer. As LBS become more popular and more central to the way individuals interact with technology, it has become imperative to take proactive approaches to ensure that consumers can use location-based services and still maintain control of their sensitive personal information [37].

Studies have been conducted to understand users' location sharing privacy preferences, as impacted by the location itself and how they are tracked [45]. Toch et al. found that location tracking patterns and techniques (laptop vs mobile) impact overall privacy preferences; highly mobile users, who visit a wider number of places, tend to also be the subject of more location requests, leading to more sophisticated privacy preferences. Other users appeared more comfortable sharing their presence at locations visited by a large and diverse set of people (“location entropy") as they considered these locations less private. Lastly, they found that rich privacy controls allow users to define preferences that they are comfortable with (such as time- and location-based restrictions).

2.3.3 User-regulated Tracking

Researchers have explored various approaches to alleviate users' privacy concerns and provide them with more control over the collection and subsequent dissemination of personal information. These approaches include enabling user-regulated tracking, providing compensation in exchange for shared information, using a trusted third party, and preventing tracking all together.

User-regulated tracking ensures that users are notified about any tracking and given the option to authorize the tracking or opt-out. For example, Bourimi et al.'s approach allows for more privacy-preserving evaluation by giving users the option to provide data of their accumulated paths during shopping when checking out [7]. In this scenario, retailers have the responsibility to preserve the privacy and security of the user by anonymizing identifiable information and analyzing only aggregated location information [7]. Myles et al. proposed a framework to specify privacy based on location, time, and the requesting organization/institution on behalf of the user. This addressed the challenge of enabling users to maintain control of their location privacy while minimizing the demands technology makes on them to accept or approve privacy related policies [35]. Researchers Riederer et al. explored an approach called 'transactional' privacy. Using this approach, users decide what aspects of their personal information can be sold in exchange for compensation and related ads. The interests of all parties in the transaction are aligned through an unlimited supply auction, which ensures truthfulness and efficiency [39].

Spreitzer and Theimer explored the use of a third-party user agent to collect and control all personal information pertaining to users [44]. In their work, requests for personal information were routed through the user agent, which enforced predetermined access policies [50]. This approach has also been explored by Confab [21] but extended to include more privacy mechanisms such as notifications, tags, logging, and interactive requests [50].

Other privacy preserving behaviors studied include false locations, which involves sending one or more fake locations that are related to the users' location [12]. This is accomplished by space transformation, which transforms the information about the user's location into another space where the spatial relationships among queries and data are encoded [12]. Lastly, some researchers have employed methods to modify radio parameters to prevent tracking all together [23, 27].

CHAPTER 3: PRIVACY PERCEPTIONS OF BLE BEACONS

In this chapter I proceed with an analysis of users' awareness and privacy perceptions toward Bluetooth Low Energy beacons. I hypothesize that (1) users are not aware of beacon technology, and naturally would have privacy concerns regarding its use, and (2) the disclosure of beacons would influence users' willingness to share beacon encounter and personal information. I outline the methodology used to study this domain, and present our findings as a contribution. I identify the privacy concerns user have, the related information they are willing to share, and the challenge in understanding context regarding beacon encounters. Our results showed that the majority of participants were largely unfamiliar with BLE beacon technology, as expected, and have a number of concerns that affect their willingness to disclose any location-related information associated with beacon encounters. Additionally, I found that participants' level of privacy concern proved to be an influential factor in their willingness to disclose this information.

3.1 Study Design

I conducted a two-part between-subjects study, where the first part of the study involved the use of a mobile application I created, called 49er Satisfier. At various designated locations around campus, users were provided a notification through the app to complete a brief location-specific questionnaire, which was triggered when the

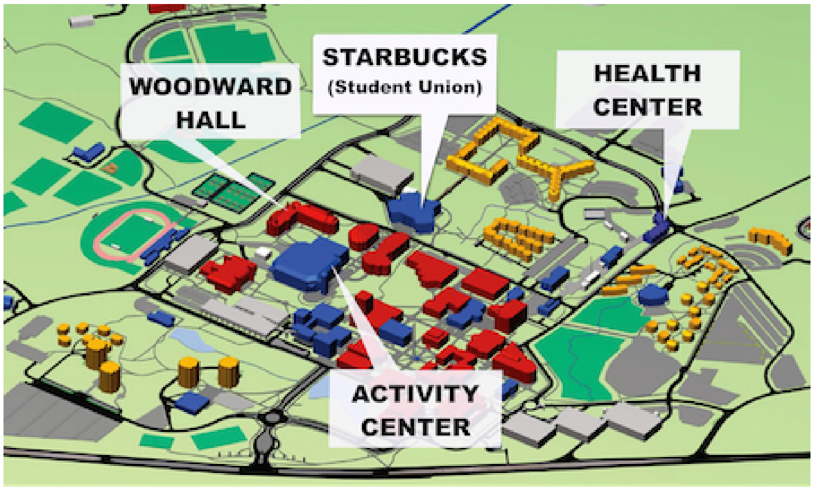


Figure 5: Participating beacon-equipped locations on the UNC Charlotte campus

user's device entered a beacon's region. Figure 5 indicates the participating locations in the study, which included Starbucks, the Student Activity Center (Gym), the Student Health Center, and Woodward. For each user, a certain condition was assigned based on the different privacy practice factors I was studying. The second part of this study consisted of an online survey, where participants answered a number of questions about their willingness to allow different types of beacon encounter information to be collected. Respondents were asked to keep in mind the condition to which they were assigned in the mobile app while they completed the survey. The University IRB approved the protocol to conduct the user study.

3.1.1 Recruitment

In order to recruit participants, I employed digital advertisements around the campus. I also sent out emails to various campus distribution lists. The study was a blind one, and therefore marketed as an endeavor to better understand the quality of experiences that people have on campus, through the use of a mobile app that prompted customer satisfaction feedback over the course of two weeks. This deception was required in order to properly compare the effects of the awareness of beacon usage without the presence of bias. Recalling our hypothesis for this study, I believed (1) that users are not aware of beacon technology, and naturally would have privacy concerns regarding its use, and (2) the disclosure of beacons would influence users' willingness to share beacon encounter and personal information. As a result, I masked the use of the beacon technology behind the deception of the "customer satisfaction" app; in this way, I could control for the effect of disclosure on participants' willingness to share related information by randomly allowing some participants to know in the beginning that the study will use beacons, while other participants would be kept in the dark until the end of the study.

After two weeks of using the app, users were asked to complete the post-survey, which took approximately 20 minutes to complete. During recruitment, no indication was provided that beacons or information privacy would be major components of the study, in order to avoid priming participants. A pre-survey was used to screen participants, in order to ensure that they were age 18 or over, students or faculty of the University, and owned a BLE-compatible Android device. As a base reward, all participants received $5 Amazon gift cards. A bonus reward was provided based on the number of in-app questionnaires users completed over the two-week period, up to an additional $5.

Table 1: Full-factorial of conditions for user study and survey

	Factors		
Conditions	*Scope of Use*	*Retention Time*	*Beacon Disclosure*
1	University only	One day	Disclosed
2	University only	One day	Not disclosed
3	University only	Indefinitely	Disclosed
4	University only	Indefinitely	Not disclosed
5	Univ. & others	One day	Disclosed
6	Univ. & others	One day	Not disclosed
7	Univ. & others	Indefinitely	Disclosed
8	Univ. & others	Indefinitely	Not disclosed

3.1.2 Conditions

Participants were each assigned round-robin style to one of 8 possible conditions based on the factors I was interested in studying regarding beacon providers' privacy practices. Table 1 reflects the details of these conditions. The study design for these conditions was full-factorial across three dimensions of privacy. The first dimension investigated scope of use and sharing policies by the beacon provider, who in this case was represented as the University. The second dimension involved retention time for collected data. The third dimension involved beacon disclosure. For each of these three factors, there were two levels each, which represented the factor's extremes. I only considered the extremes, under the assumption that if polar opposite policy practices did not impact participants, then there would be no need to investigate the impact of the varying degrees between these levels. As a result, the two levels for each of the three dimensions were represented as such:

- **Scope of data use:** Participants were either informed that the University was the sole identity that would use and share their information, or they were informed that third-party retailers also had access to the information.

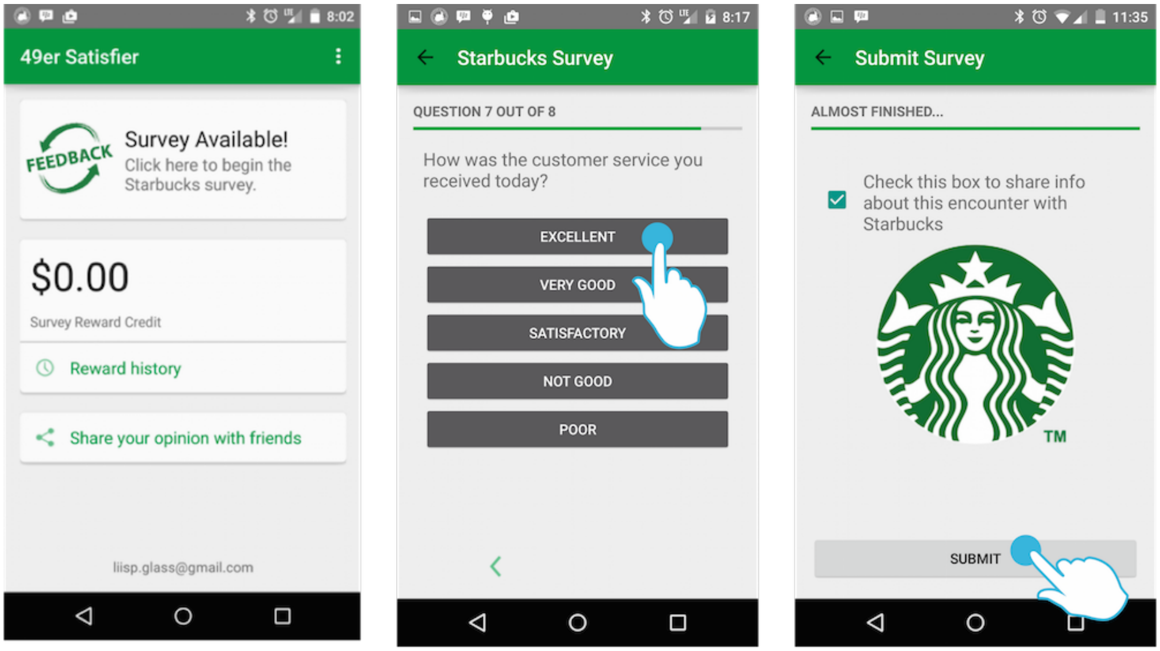
- **Data retention time:** Participants were either informed that their collected data would be kept for one day, or it would be kept indefinitely.
- **Beacon disclosure:** Participants were either informed of the use of Bluetooth Low Energy beacons as the means to trigger information collection, or they were not informed of the use of beacons at all. Those who were not explicitly made aware of the beacons were informed at the conclusion of the user study.

3.1.3 Motivating Factors

Additional key motivating factors which were investigated but which were not incorporated in the full-factorial design included view/edit access to data, entropy/context of location where data is collected, social network usage, general privacy concern, and general IT experience. With the exception of entropy/context of location, the remaining secondary factors were targeted solely by the post-survey, and not by use of the mobile app.

3.1.4 User Study Flow

Participants who were successfully screened and met the eligibility requirements for the study then downloaded the mobile app called "49er Satisifer" on their Android device. In this app, they were presented with a tutorial that explained the fictitious study goals and how to use the app. Figure 6 depicts the main interfaces of the app with which users interacted. Users were asked to explore the different locations on campus as part of the study, and whenever they entered one of the locations, the app



Survey Available! Click here to begin the Starbucks survey.

$0.00
Survey Reward Credit

liisp.glass@gmail.com

How was the customer service you received today?

☑ Check this box to share info about this encounter with Starbucks

Figure 6: Screenshots of 49er Satisfier Android app

would recognize the presence of a beacon and trigger a notification alerting them to take the corresponding questionnaire. This questionnaire had a few brief questions that related to the customer satisfaction experience that a user had while at that location. For example, at the Starbucks location, users would be presented with a questionnaire inquiring about things such as what coffee drink they ordered, the cost of the drink item, the length of the line to order, the demeanor of the barista, and so on. Each questionnaire was worth an additional $0.25, and each of the four location's questionnaires could be taken once a day. Once the user completed a questionnaire, the app would collect the provided responses and submit them to our Parse database, along with the information concerning the beacon encounter. This included the time and duration of encounter, and the beacon's UUID, Major and Minor values. This took place at every location. After the span of two weeks, all users were debriefed on the real intent of the study; they were shown a brief YouTube video about beacons and provided an explanation of how beacons were incorporated into the study, including the collection of aggregated and anonymized beacon encounter information. Then they were invited to complete the post-survey, which investigated their perceptions of BLE beacons and sharing various forms of related information.

3.1.5 Survey Flow

Users began the post-survey by completing a few general demographic questions, including age, gender, education, and technical expertise. Furthermore, the respondents were asked via Likert-scale questions about their general awareness/familiarity with standard Bluetooth, Bluetooth Low Energy, and BLE beacons. A few open-ended questions were included in order to glean some qualitative information about respondents' knowledge of Bluetooth and BLE beacons. Respondents were also asked to evaluate beacons on a 5-point Likert scale based on usefulness, relevance, and threat to privacy/security, to the best of their current knowledge. The survey progressed to quantitatively inquire about awareness of other tracking technologies, both physical and digital. These included browser cookies for in-app advertisement, GPS for geotracking, and cameras for surveillance.

The next part of the survey addressed the user study they participated in using the 49er Satisfier app. First they were asked to confirm each of the conditions they were assigned to for the scope of data use, data retention time, and beacon disclosure. They were also asked a question concerning what they believed were examples of beacon information that could be collected during an encounter. This included time, duration, frequency, and path taken of a visit, as well what clothes were worn and what words were said. These last two items were inaccurate, but used to determine users' understanding of the capability of beacons. Then, based on their assigned user study condition, respondents were asked a series of Likert-scale questions about their willingness to allow locations to collect and use various pieces of information related to beacon encounters. They were then prompted to respond to how much their overall willingness would change along different levels of retention time, and the ability to review/edit/delete collected information.

The last part of the survey dealt with beacons and privacy management. Since the ultimate goal of this research is to demonstrate the need for user-centric beacon privacy management, the responses to these questions were imperative, and were considered an initial phase of functional requirement gathering from prospective users. The first two questions under this section were Likert-scale questions evaluating respondents' willingness to allow the collection of anonymous information, as well as personal information, from beacon encounters if their mobile device allowed them certain levels of control. These include choosing in advance what information companies could learn about the user, controlling which companies can collect and use that information, controlling in what locations that information can be collected, and even having the ability to create different sharing “personas" or profiles. The last question was an open-ended question asking respondents to describe the features they would include in a tool or application that would help manage the privacy of their information regarding beacon encounters if they could design such a tool themselves.

3.1.6 Analysis Procedure

I was interested in investigating general awareness of BLE beacons and users' perceptions regarding the privacy implications of the technology. Furthermore, I wanted to reveal whether the motivating factors, including the privacy policies participants were told governed data collection, would influence users' willingness to share location information related to beacon encounters.

Using the participants' treatment for each dimension of privacy policy and the other identified potentially motivating factors as independent variables, and the beacon encounter information data types as dependent variables, I performed a multivariate multiple regression, evaluating the effect of multiple independent variables on multiple dependent variables. I confirmed any significant results by running ANOVA, to ensure that yielded similar results. For all statistical tests, the α-value was 0.05.

3.2 Descriptive Results

I had a total of 52 users who downloaded 49er Satisfier for the two-week study, but only 18 participants actively used the app through this time, and 34 participants who completed the post-survey at the end. I analyzed app usage for these 18 participants, and survey responses from 34 participants. The majority of data analysis comes from the survey respondents; the demographic breakdown for the 52 users overall can be seen in Table 2.

Table 2: Participants' demographic summary

Gender	%	Age	%	Education	%
Male	78.8	18-24	51.5	Bachelor's	42.4
Female	21.2	25-34	45.5	Graduate	36.4
		35-64	3	High School	12.1
				Some college	9.1

3.2.1 App Usage

Through the app I observed the locations most frequented by the 18 app users: Starbucks was visited the most, with a total of 1350 registered encounters and 19 satisfaction survey submissions, followed by Starbucks, with 1178 encounters and 28 survey submissions. The Gym had 917 beacon encounters and 0 submitted surveys, while the Health Center had 574 encounters and 5 submitted surveys. Of the 19 participants, only 6 visited Health Center and 5 visited the Gym, while 16 visited Woodward and 15 visited Starbucks. A summary of these results can be found in Table 3. While it was expected that a location like Starbucks would generate many beacon encounters by visitors, it is interesting that the location with the next most beacon encounters was Woodward Hall. However, assuming that the students who were most likely to participate in this study were those who already visit these locations as part of their normal routine, it is plausible that these same students are likely to visit Woodward daily, due to required class and meeting times. Regarding the higher number of submitted surveys at Woodward, perhaps students were more likely to spend an extended amount time in Woodward, and the location allowed for more of an opportunity to pause and complete questionnaires than in the campus Starbucks, which is a smaller environment and structured as a grab-and-go location.

Table 3: Summary of 49er Satisfier app usage

Location	Visitors	Encounters	Surveys
Starbucks	15	1350	19
Woodward	16	1178	28
Gym	5	917	0
Health Center	6	574	5

In contrast, the Health Center had the least amount of registered encounters, which was expected given its lower location entropy and the fact that it is visited on a need-to-go basis, yet it still triggered a few survey submissions. This is contrasts with the next least encountered location, the Student Activity Center (Gym), actually triggered 0 submitted surveys. One thing to note with these locations is that the lack of visitors may actually have been the result of a different coping mechanism to manage location privacy. In other words, users may have deliberately abstained from visiting these locations, or turned off Bluetooth while visiting, as a means of limiting the related location information shared. Regarding the difference in surveys submissions among the limited visitors, however, I believe this may have come from the fact the Health Center, like Woodward, allows for more time to stop and complete surveys while in that location. Between the waiting time after checking in or before being seen by a doctor, or perhaps while waiting for a prescription to be filled, there are several opportunities to complete a prompted survey. Students visiting the Student Activity Center, however, enter here with the intent to participate in some sort of exercise, and depending on the level of activity, may put away their phones upon coming in, and not bring them out out again until they've left the building.

Unfortunately there were not enough participants to conduct the full-factorial multivariate analysis I had intended, based on the various study conditions. Consequently, there was not enough data from the app usage to confidently make a claim about the significant impact of data-retention period, scope of use, and beacon disclosure on the participants' willingness to disclose related encounter information. Nonetheless, there is still value in reporting these results, it is my hope that the consideration to study these measures can serve as the basis for future research into understanding user behavior regarding beacon encounters.

3.2.2 Survey Responses

The remaining significant results that were gleaned from this study came from the post-survey that was administered after use of the 49er Satisfier app. The data analyzed from the 34 respondents served as indicators of the privacy perceptions users had towards BLE beacons, as well as the influential factors that affected their willingness to share when encountering these sensors.

3.2.2.1 Awareness and Perceptions of BLE Beacons

The majority of participants in our study proved to be largely unfamiliar with BLE beacon technology, which was our assumption going into the research study. As Figure 7 indicates, almost 60% were not familiar with Bluetooth Smart or BLE beacons, while only 30% claimed they were very familiar.When using the qualitative responses from the subsequent open-ended question to reinforce these results, I found even fewer had an understanding of the technology: only 11% (4 participants) provided an accurate answer.

Unfamiliar Responses

- *"I don't know much about beacons."*

- *"None" / "Nothing" / "Never used beacons"*

- *"They are transmitters. This is all what I know!"*

- *"I use bluetooth everyday for music in my car."*

Familiar Responses

- *"BLE beacons are transmitters that use low energy to broadcast signals that can be heard by smart devices."*

- *"Low energy beacons have been known to be used to in stores and malls to gather traffic patterns of customers and analyze shopping analytics."*

- *"A beacon broadcasts a signal and will communicate information to devices in range."*

As with other tracking technologies before beacons, the majority of users will base their opinions and perceptions on this lack of understanding, though these perceptions may change over time as beacons become more pervasive, and users' attention is drawn more to their presence. As a way to draw a comparison between users' perceptions of this beacon technology and that of other tracking technologies, I asked users to evaluate beacons, cookies, GPS/geotracking, and surveillance cameras on the basis of usefulness, relevance to their typical routine, threat to privacy & secu-

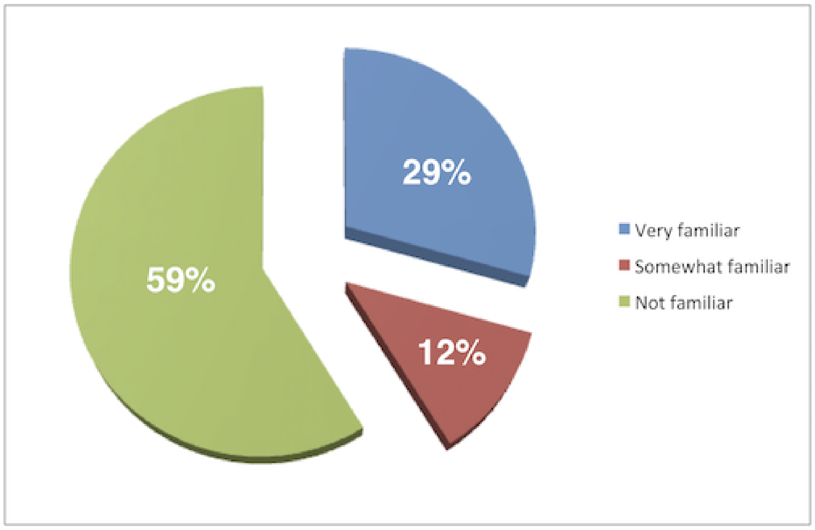


Figure 7: Participants' familiarity with BLE beacons

rity, and general necessity. As Figure 8 indicates, beacons rated lower on all of these categories. Repeated Measures ANOVA was performed for each factor, to compare the different technologies. Security and Necessity yielded significant results, with p-values of $< .0001$ and .017 respectively. For Security, post-hoc comparisons revealed that the significance lied between Cookies and Cameras, as well as between GPS and cameras, but there was not a real significant difference in perception of security between beacons and cameras. I interpret this to mean that users perceive beacons to be generally as secure as the other technologies. For Necessity, the difference lied between Cameras and all other technologies, including beacons. This would suggest users are not immediately aware of the potential applications of beacons.

3.2.2.2 Willingness to Disclose

The willingness of participants to share beacon encounter information varied between the types of information they would have to disclose, as shown in Figure 9. For instance, only about 45% of participants were willing to disclose the identity of the

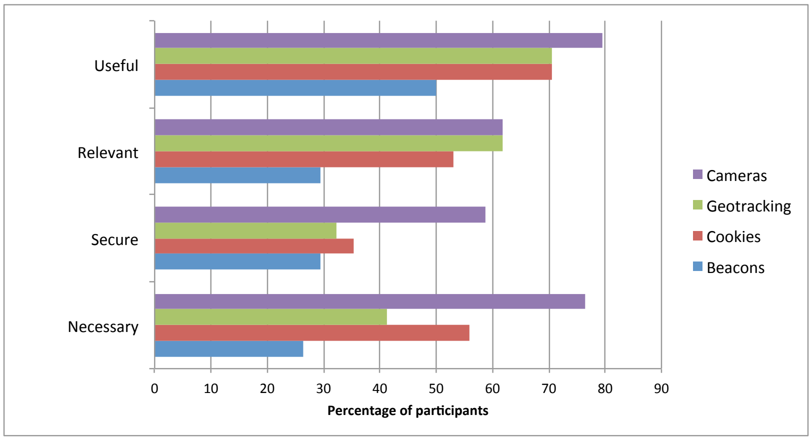


Figure 8: Participants' perceptions of BLE beacons and other online tracking and physical tracking technology

beacon they encountered, while over 70% were willing to share beacon travel path. The latter was an interesting trend, which seems to indicate that knowledge of the beacon travel path within a location is less sensitive to users than knowing each of the specific beacons that were visited. I believe a reasonable explanation for this is that the concept of "travel path" was not as clear to participants as the identity of a beacon, since the travel path was not a component of beacon encounters that they were exposed to through the user study. I did not collect that information, since the beacon-enabled locations on campus were too spread apart to gather any meaningful path data around campus, and furthermore, each location was not equipped with enough beacons to gather meaningful path data within each building. One might argue that knowledge of the path would imply knowledge of the beacons along the path. It is important to note, however, that all of these beacon encounter metrics were considered mutually exclusive in the survey. For example, the assumption was made that if users shared their travel path, it could not be used to identify the specific ID of the beacons along that path. Repeated measures ANOVA was conducted to

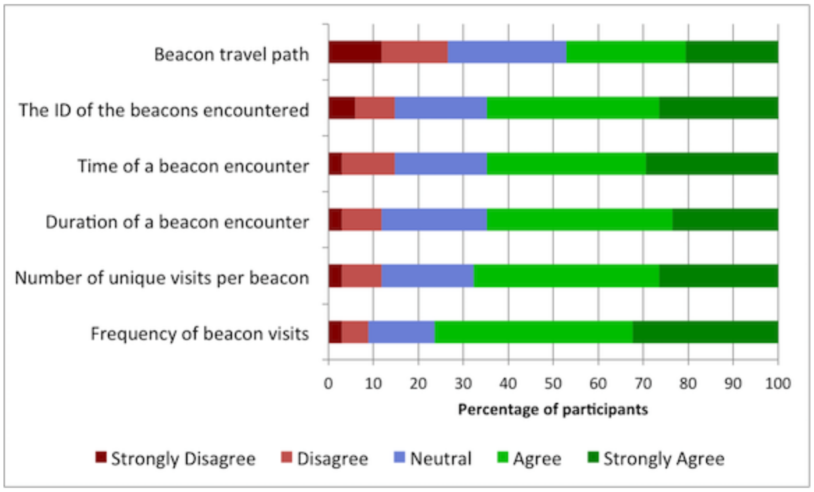


Figure 9: Participants' willingness to share different types of beacon encounter info

determine if there was any statistically significant difference between these responses, and what resulted was a p-value of .015. Hence I found that the significance lied between beacon path and time, duration, unique visits, and frequency. There was not a significant difference between beacon ID and path, so I concluded that in fact, the IDs of the individual beacons visited were considered as sensitive as travel path.

3.2.2.3 Impact of Privacy Concern

The levels of privacy concern reflected in this survey were inspired by Westin's Privacy Segmentation indexes of Pragmatist (balanced, or neutral), Fundamentalist (concerned), and Unconcerned [25]. These are determined based on responses to three pre-determined questions, in which users indicated how much they agreed with the following statements: (1) Consumers have lost all control over how personal information is collected and used by companies; (2) Most businesses handle the personal information they collect about consumers in a proper and confidential way; (3) Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today. Responses to each statement were captured on a Likert-Scale, ranging from Strongly Disagree, Somewhat Disagree, Somewhat Agree, to Strongly Agree. According to Westin, Privacy Fundamentalists are respondents who agreed (strongly or somewhat) with the first statement and disagreed (strongly or somewhat) with the second and third statements. Furthermore, Privacy Unconcerned are those that disagree with the first statement and agree with the second and third, while Pragmatists are all other respondents. Once I segmented participants based on responses to these questions, I used factor analysis to combine the responses of willingness to share the five individual elements of beacon encounter into a single score, and then I used a one-way ANOVA test to determine the impact of privacy concern on willingness to share for the concern three groups. This revealed a significant effect, with p=.021. Post hoc comparisons revealed that Unconcerned and Concerned were the two groups with significant difference in willingness to share, with p=.019.

3.2.2.4 Fine-Grained Control

Currently, there is a limitation of web browser tools in offering usable, fine-grained control over cookie management, data collection, or ad displays. Similarly, mobile device platforms and apps seldom offer the fine-grained control necessary to meet the expectation of users. Consequently, there has been sufficient research into tools that can satisfy users' privacy demands. Since this is a gap I want to fill for BLE beacon technology, I similarly need to explore whether the introduction of new, fine-grained controls would help users feel more comfortable sharing data. Hence I asked participants to consider six features of a hypothetical beacon privacy management app that would give the user control over and transparency into the information collected by beacon service providers.

For each feature, I asked users to indicate their level of agreement in being more willing to disclose information if they were able to take advantage of an app or device with this feature. The six included features were “choose ahead of time what information can learn,” “control which companies can collect and use the information,” “visualize information that companies already know,” “create different ‘personas’ to show companies,” “control in which locations information can be collected,” and “visualize in which locations’ information has already been collected.” Figure 10 highlights the survey responses regarding these features.

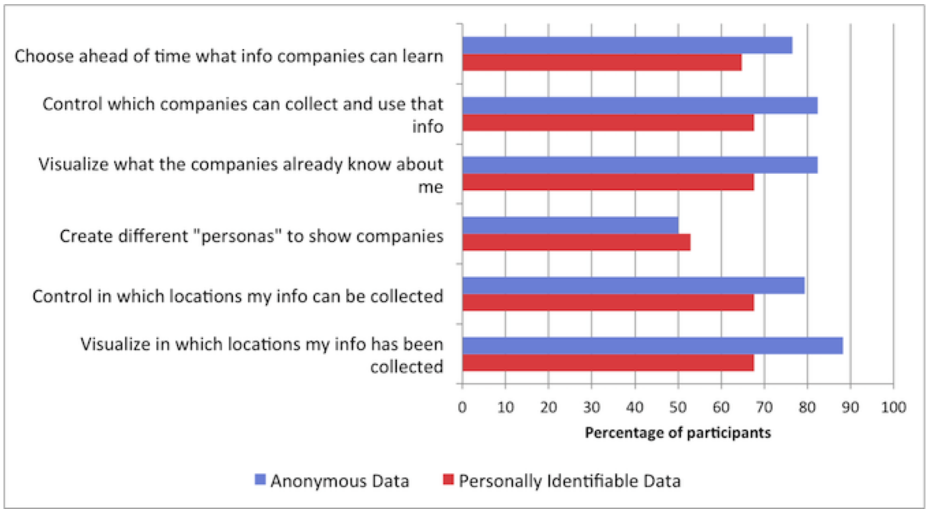


Figure 10: Percentage of users who would be more willing to share anonymous vs. personal information based on six different location privacy management features

The survey respondents reported that an app with the proposed features would generally make them more willing to share information with companies that use beacons, both when data was anonymous (an average of 84% of participants) as well as personally identifiable (74% of participants). This difference in willingness to share anonymous over personal data was consistent across five of our six proposed features. The singular exception was the feature regarding"create different personas," where the trend was reversed. This was in line with our expectations, since the concept of a persona is less relevant to anonymous data than to personally identifiable data. This feature also happened to be the least influential in making participants more willing to share location information; for anonymous data, 50% of participants said this would make them more willing, and for personal data, 53% agreed this would make them more willing.

Examining which app privacy management features would most increase willingness to share information, it appeared that most of the features were equally important regarding personally identifiable information. Regarding anonymous information, however, the ability to "visualize in which locations information has been collected" showed the most increase, with 88% of participants agreeing this would make them more willing. Repeated Measures ANOVA revealed that the most influential features, based on significant differences in willingness to share, existed for controlling which companies can collect information, as well as visualizing in which locations information has been collected.

Overall, these results confirm that offering more adequate, fine-grained control over beacon-related location information disclosure could mitigate some of their privacy concerns.

3.2.2.5 Qualitative Feedback

In addition to the quantitative responses obtained from the survey, I collected snippets of textual feedback from the open-ended question concerning features respondents would include in a beacon privacy tool if they could design it. These were valuable not only in reinforcing responses from the previous survey section, but also in gathering functional requirements for our framework. These snippets included:

> *"The ability to turn on or off sharing of individual identifiers (first name, last name, email, etc.) and companies, with 0 hoops to jump through."* [8 unique mentions related to "opting in/out of information sharing"]

> *"List of all information that has been shared about me ... as well as who is requesting, and the frequency at which each piece of information has been shared."* [5 unique mentions related to "visualization/analytics"]

> *"Check a box to allow the sharing of data with beacons or to delete the data from the beacons after a limited amount of time."* [3 unique mentions related to "controlling data retention time"]

> *"A delete button, where it is possible to ask companies to remove all the collected data about yourself in all their databases, servers, etc."* [2 unique mentions related to "edit access to data"]

> *"Having a type of 'firewall' that blocked specific information gatherings. If a beacon looks for a person's address, it could send back '*' instead to show that the person does not want this information collected."*

3.3 Discussion

Our results proved promising, but it is important to recognize areas of improvement that should be addressed in future studies. For example, this study was limited by the size and homogeneity of the sample. This was a result of the decision to limit the user study to a campus setting, which I did for a number of practical reasons. These included the need to keep track of the beacons, the convenience of having reliable access to the participants throughout the study, and the minimal overhead required to deploy the beacons and run the study. Consequently, our sample was not as large as anticipated, and the majority of our participants were homogeneous on certain levels, such as age and technical expertise. Furthermore, I experienced a higher than expected drop-out rate, with only 34% of participants completing the study in its entirety, from sign up to post-survey. I posit that this is a result of the timing of the study, which was conducted around the end of the academic semester, when students are preoccupied with final exams, among other things.

Although the results of this study implicitly point to the fact that certain locations are more acceptable to share beacon encounter information with than others, it is important to point out the study relied on the locations' overall "entropy," which is related to how public or private the entire location could be considered based on the amount of people that are typically present. For example, the entire Student Health Center building was considered a private location in this study. Yet in many settings, a single location may have various levels of “entropy" that exist within it. In other words, an entire location cannot always be considered entirely public or private, but rather is often comprised of sections that differ in levels of perceived privacy. A retail environment is a genuine example of this: a store like Wal-Mart has departments that vary from clothing to hardware to electronics. Consider how our male college student in the earlier Motivating Example may feel comfortable sharing details of beacon encounters when shopping in the video game section of the electronics department, but may refrain from sharing similar details from their beacon encounters when passing through the women’s lingerie section of the clothing department. If the information flow is not transparent to him, such as is the case with beacons, then the context in which information is gathered, associated, and shared is not clear to the user. The college student may as well consider the entire location as “private" and therefore refuse to disclose any beacon related information in any part of the store. Hence, this study is limited in its ability to evaluate the impact of context on users’ decision-making process with regard to sharing beacon encounter information. This limitation is the focus of a separate study, discussed in Chapter 4.

Regarding possible extensions to this work, a clear path to furthering the research here would be to conduct this beyond the college campus setting. Other studies should be conducted to compare the results with larger, more diverse or different sample populations. By doing so, we can better capture privacy perceptions of the population at large regarding BLE beacons, and incorporate these results into the framework upon which our BLE beacon privacy manager is being built. Furthermore, I believe it is worthwhile to pursue a framework that not only allows users to limit beacon information shared, but also incentivizes them to share this information when they determine it to be worthwhile. In this way, I encourage controlled information disclosure while still ensuring desired location privacy. As a result, another plausible extension would be to specifically explore the various types of incentives that are best suitable for the context-driven nature of beacon encounters.

3.4 Conclusion

This study marks the early stages of this research, and these results are pivotal in outlining the connection to related work and the need for further investigation. In some ways, the findings here are similar to what has been found in the research cited in Chapter 2. For example, I confirmed that users are largely unaware of how BLE beacons work, and uninformed about how privacy and security play a role in their interaction with this technology, as was the case for cookies [20, 33]. While this awareness will naturally increase with the pervasiveness of the technology, I determined that a user's privacy concern is still what plays a significant role in his willingness to disclose beacon related information. Furthermore, though our results were inconclusive regarding the impact of factors like scope of use, data retention time, and location entropy, which were found by Leon et al. to affect online tracking perceptions [26], I do suspect that location entropy plays a role in the privacy perceptions users have related to beacons, based on the observed patterns of app usage within the study. Still, in other ways, the findings here differ from the work done in related areas. This stems from the nuances in location data that can be gleaned from beacon encounters, including elements like the number and frequency of visits, as well unique travel paths. As a result, the amount of control desired by users is also more nuanced than that of the tracking technologies that precede BLE beacons [37, 45]. The next major research step and contribution of this dissertation involves the introduction of context in beacon encounters for users, so that they can make better privacy-preserving decisions when navigating these nuances.

CHAPTER 4: CROWDSOURCING FOR CONTEXT

Contextual integrity is a concept that suggests that people do not require absolute privacy but rather privacy that meets certain expectations and social norms. Research conducted by Helen Nissenbaum shows that contextual integrity is important to the privacy perceptions associated with technology; these perceptions are based on four elements: the context of a flow of information, the capacities in which those involved are acting, the type of information involved, and the principles of transmission [36]. From this I derive an emphasis on the context-dependence of privacy concerns, and I apply this to BLE beacons. Although they are used to provide precise location and contextual cues about users' interactions with the real world [19], the current identifiers that characterize a beacon encounter are actually not sufficient for ordinary users to make informed privacy decisions about the location information that could be shared for each encounter.

I envision a way to empower users with the means to control their privacy in beacon-enabled spaces. One solution would be to have standardized category and privacy labels associated with beacons, generated by beacon providers or an independent third-party. However, it would be difficult to ensure that all beacon providers abide by this policy. Moreover, their regard for privacy will likely differ from that of their users. Therefore, a novel approach is required to provide the necessary context, allowing users to form accurate mental models of beacon encounters before exercising appropriate privacy-preserving behaviors. This is where I provide a solution that does not previously exist. By designing, implementing, and deploying a beacon privacy manager that relies on crowdsourcing, I would empower users who have encountered beacons to contribute their understanding of the related context for other users to leverage in order to make informed privacy preserving decisions regarding what to share with beacon enabled mobile apps. With the proper incentives, I can also continually motivate users to contribute their input, which serves as a way to verify labels and separate the consistent, reliable input from the unreliable. Hence, my research led to "crowdsourcing" as a logical choice for this solution, and my results demonstrate it is also an effective and usable one.

4.1 Background

Crowdsourcing can be defined as "everyday people using their spare cycles to create content, solve problems, and even do corporate R&D" [22]. Rather than soliciting contributions from traditional employees or workers, crowdsourcing relies on a large number of average users, usually recruited via social networks or open calls online, to work together towards a common goal. Projects such as Wikipedia [49], Amazon Mechanical Turk [10], SETI@Home [2], and Threadless [8] are all the result of relying on the collective intelligence and input of the crowd to address a broad array of purposes, successfully demonstrating how large, loosely organized groups of people can use technology to contribute individual effort to address a larger purpose in surprisingly effective ways [32].

In the domain of security and privacy, crowdsourcing has seen similar effectiveness

[40, 31, 29, 41]. For example, Burguera et al. [11] utilized crowdsourcing to capitalize on dynamic analysis of application behavior to detect Android malware. Using their lightweight client called "Crowdroid," they were able to collect traces of applications' behavior-related data from real users, with experimental results showing that the system was able to provide a 100% detection rate for self-written malware, and 92.5% for two real malware specimens. Additionally, Lin et al. introduced a model for privacy, namely *privacy as expectations*, where crowdsourcing was employed through Amazon Mechanical Turk to capture users' expectations of what sensitive resources mobile apps tend to use, including unique device identifier, address book, network location, and GPS location [28].

Identifying expectation and purpose as two key factors that affect users' mental model of app privacy, Lin et al. go one step further to design and evaluate a privacy summary interface for Android apps that emphasize an app's behaviors that do not align with the crowd's expectations. They were able to show that this interface was both more accurate and efficient than the default Android permission interface in making users aware of the related privacy concerns. Lastly, Agarwal and Hall developed a system for iOS devices to detect an app's access to private data, such as unique device identifier, location data, address book, and music library, and it protects users by substituting anonymized data [1]. Their system used a crowdsourced recommendation approach to provide app specific privacy recommendations and was able to recommend settings for over 97.1% of the 10,000 most popular apps. Its effectiveness was also asserted through the acceptance of 67.1% of all privacy recommendations by users.

From the related work it is evident that the interaction of crowdsourcing and privacy is plausible, particularly with other tracking technologies. However, regarding beacons, the research presented here is the first of its kind. There is a need for this solution given the inherently context-driven nature of the technology. Since beacon providers decide the context of each beacon encounter [19], it is imperative that users are able to form accurate mental models of these encounters and exercise appropriate privacy-preserving behaviors when necessary. Our main objective is to build a privacy manager that leverages these mental models and equips users with policies that enforce the desired privacy-preserving behaviors based on the context of an encounter, characterized by more meaningful identifiers like the location or type of beacon, and the study I conducted is a critical first step towards this objective.

4.2 Study Design

For this study, I set out to determine whether users can come to a clear consensus through crowdsourcing regarding the specific context of a given beacon encounter, as well as the privacy perceptions associated with it. I believe users can leverage that consensus to aid them in making an informed privacy decision regarding future beacon encounters. In order to evaluate my problem statement, I conducted a between-subjects study involving the use of an Android mobile app I created called Beacon Buckets ("BknBkts"). Use of the app was accompanied by the completion of a post-survey. The study took place in the Barnes & Noble bookstore on campus, located in the Student Union, during normal business hours. I set up the beacons around the bookstore, and participants were instructed to find them in scavenger hunt fashion using the mobile app, and label them based on the category of items closest to them. Figure 11 indicates the sections of the bookstore where beacons were placed, each of which represented one of the following categories: Women's Athletic Apparel, Magazines, Men's Polo Ralph Lauren Apparel, Shot & Drinking Glasses, Clearance, Health & Beauty, Starbucks, Restrooms, and ATM machines. The University IRB approved the protocol to conduct this user study, and approval was also given by the Student Union building managers to deploy beacons in these locations around the bookstore.

Within the app, users were programmatically assigned in round-robin fashion to one of three conditions: either they were recommended the correct category associated with each beacon, the most popular categories selected for each beacon as crowdsourced by other users from all previous sessions, or they were not provided with any recommended labeling. Table 4 summarizes these study conditions: I represented the group of participants who were provided the correct category associated with each beacon as "TopCat," while the group provided with the most popular crowdsourced categories as "CrowdCat," and those not provided with any recommended categories as "NoCat." Decisions of the participants in the other groups, TopCat and NoCat, were not taken into account when providing CrowdCat suggestions, therefore preventing any leakage of correct category labeling. Participants used the information they were given to categorize each beacon and answer a few privacy-related questions for each. Then a post-survey was administered at the very end.

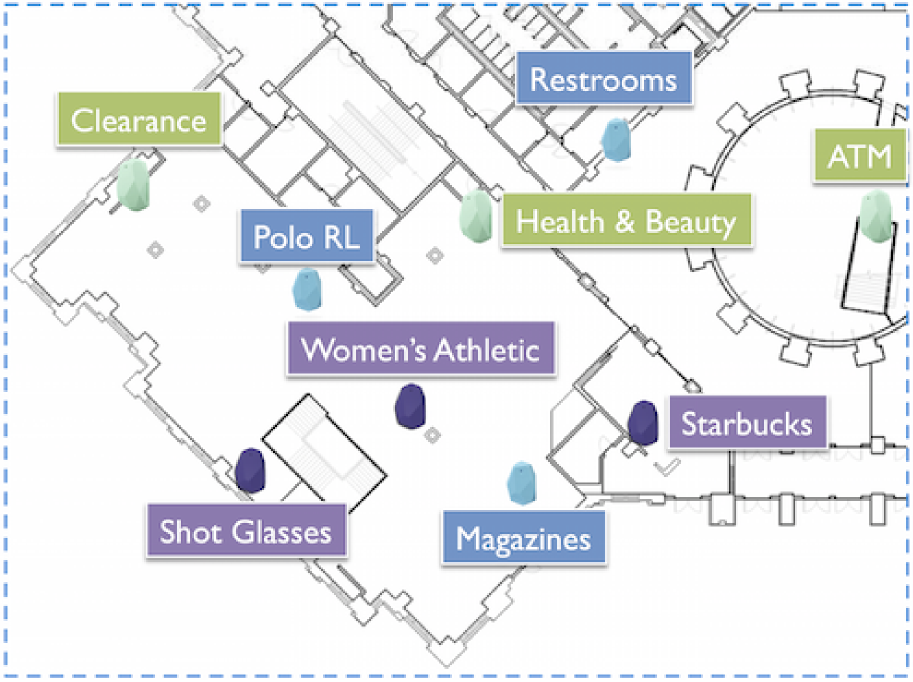


Figure 11: Map of beacon placement in campus bookstore for the BknBkts study

Table 4: Study conditions

Condition	Recommendation
TopCat	Correct category labels
CrowdCat	Crowdsourced category labels
NoCat	None

4.2.1 Recruitment

Random passers-by and visitors to the bookstore served as the random sample for the study. All participants were age 18 or over, and although the majority were students at the University, it was not a requirement. The study was advertised as a beacon scavenger hunt game, with a reward in the form of a $5 Starbucks gift card for anyone that played. Participants with a compatible Android device installed the app on their phone; otherwise, they were given a loaner device. A short pre-survey was administered within the app to assess awareness and perceptions of beacons. Overall, the scavenger hunt took an average of 30 minutes to complete, and the study was conducted over a span of three weeks.

4.2.2 User Study Flow

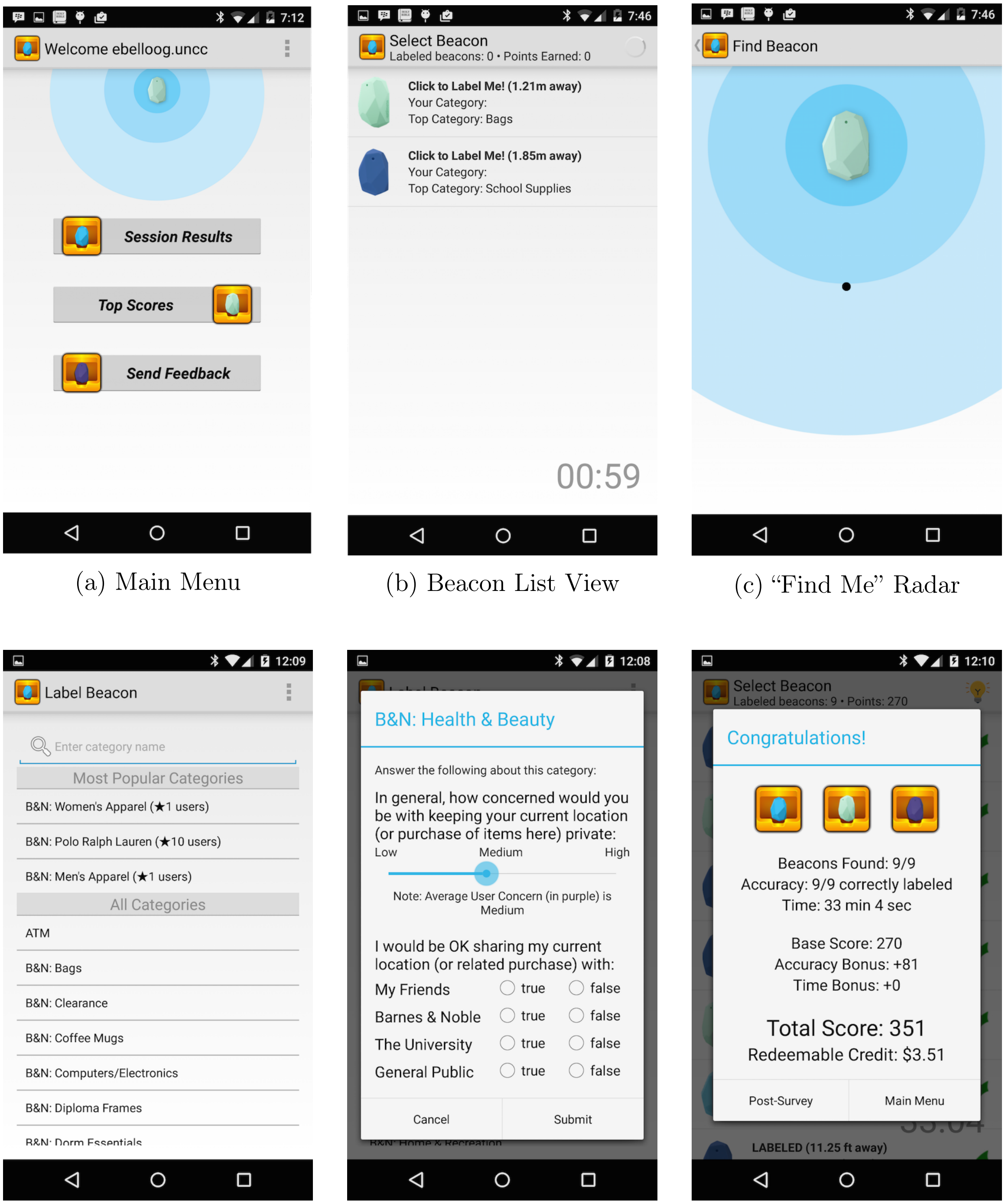
Participants began the user study by registering their profile in the BknBkts app, and proceeded through a brief tutorial with accompanying screenshots depicting how to use the app. Figure 12 represents screenshots of the app's interface, which was also presented to users during the tutorial. After registering, users were brought to the main menu, as seen in Figure 12a, where they would enable Bluetooth on the device and start the session. From here, users could view a dynamic list of BLE beacons within range of the device, shown in Figure 12b, sorted in order of distance from the user. From this view, the user also had the option to access hints for where beacons might be placed around the bookstore by selecting the light bulb icon in the top right corner. Selecting a beacon from the list provided two options: "Find Me," which displayed the radar view shown in 12c to help users determine their proximity to an unseen beacon, and "Label Me," which displayed a list of categories, as shown in Figure 12d, from which to choose and associate an observed beacon. Users were advised to visually locate the beacon in question before labeling it, to minimize incorrect labeling. The app actually required users to be within approximately 10 feet for the beacon to show up in the list of available beacons to label, and it was designed this way to limit the interference from other beacons when one was within view.

When choosing from a list of categories for a given beacon, participants in the Top-

Cat group were presented a subsection for an assigned “Top Category.” These participants were made aware through verbal instruction that the one category at the top represented a label as if provided by the bookstore itself. The CrowdCat participants were shown the three “Most Popular” categories, which were crowdsourced from other participants’ responses. These users were informed that the “Most Popular” category labels were the most popular choices for a beacon that were crowdsourced among participants across all previous sessions. The first CrowdCat user actually received no recommendation. All subsequent CrowdCat users received the top recommendations at the time (in particular, the second user is recommended whatever the first user chose, and so on), which may have included ties. The NoCat group did not see anything other than the standard list of all categories.

Figure 13 represents the view that participants were shown based on their condition. While on this screen, the app kept track of the amount of time taken to select a category, as well as whether the selected category was a recommended one, if applicable. The last step required users to provide a privacy label for a beacon, which involved a few questions, as shown in 12e, regarding the “sensitivity” based on the selected category. In this scenario, a “sensitive” beacon was described as “worth keeping my presence here, or purchase of related items here, as private.” Therefore for each beacon, users indicated the level of concern associated with the privacy/sensitivity of the beacon using a slider on a scale from 0 to 100. Here, those in the CrowdCat group would see “Average User Concern” level represented on the slider. This was done to again provide crowdsourced feedback on what other users had prescribed as a sensitivity level, though there were no a priori “correct” privacy labels. Participants also indicated which circles of people they would be willing to share this location with, including friends, the bookstore, the university, and general public, using radio buttons. These last few questions that pertained to the privacy label represented other levels of context to consider in location information sharing for each beacon found.

Users would repeat this process for each beacon they encountered as they explored the bookstore. Should they determine that they had inaccurately labeled any beacon, or they wanted to change their responses to the sensitivity-related questions, they simply had to click on the labeled beacon to redo the process. Since the app was designed as a Game With A Purpose [48], where every beacon labeled earned users a number of points contributing to a base score, this motivated users to provide truthful labels and gamified the labeling process. Additionally, users earned bonus points for labeling accuracy, as well as for completion time. The total possible score that could be earned was 500 points, which translated to the $5 gift card reward for participation. Although the app was structured this way to further incentivize participants to do their best in labeling, in the end all participants were equally paid a $5 gift card. Once all nine beacons had been found and labeled, or if the participant chose to quit early, the app would trigger the conclusion of the session and present the user with a report of the score earned, as seen in 12f. From the main menu, users were able to see a leaderboard of the top ten scorers and compare their scores with those of other participants. The purpose of the leaderboard was simply to contribute to making the app more like a game, and therefore incentivize users to complete the study. Participants were not able to redo the study in an effort to improve their



(a) Main Menu

Labeled beacons: 0 • Points Earned: 0

Click to Label Me! (1.21m away)
Your Category:
Top Category: Bags

Click to Label Me! (1.85m away)
Your Category:
Top Category: School Supplies

00:59

(b) Beacon List View

(c) “Find Me” Radar

Most Popular Categories
B&N: Women's Apparel (★1 users)
B&N: Polo Ralph Lauren (★10 users)
B&N: Men's Apparel (★1 users)

All Categories
ATM
B&N: Bags
B&N: Clearance
B&N: Coffee Mugs
B&N: Computers/Electronics
B&N: Diploma Frames
B&N: Dorm Essentials

(d) Category Label List

B&N: Health & Beauty

Answer the following about this category:

In general, how concerned would you be with keeping your current location (or purchase of items here) private:

Low Medium High

Note: Average User Concern (in purple) is Medium

I would be OK sharing my current location (or related purchase) with:

My Friends	○ true	○ false
Barnes & Noble	○ true	○ false
The University	○ true	○ false
General Public	○ true	○ false

(e) Privacy Label View

Labeled beacons: 9 • Points: 270

Congratulations!

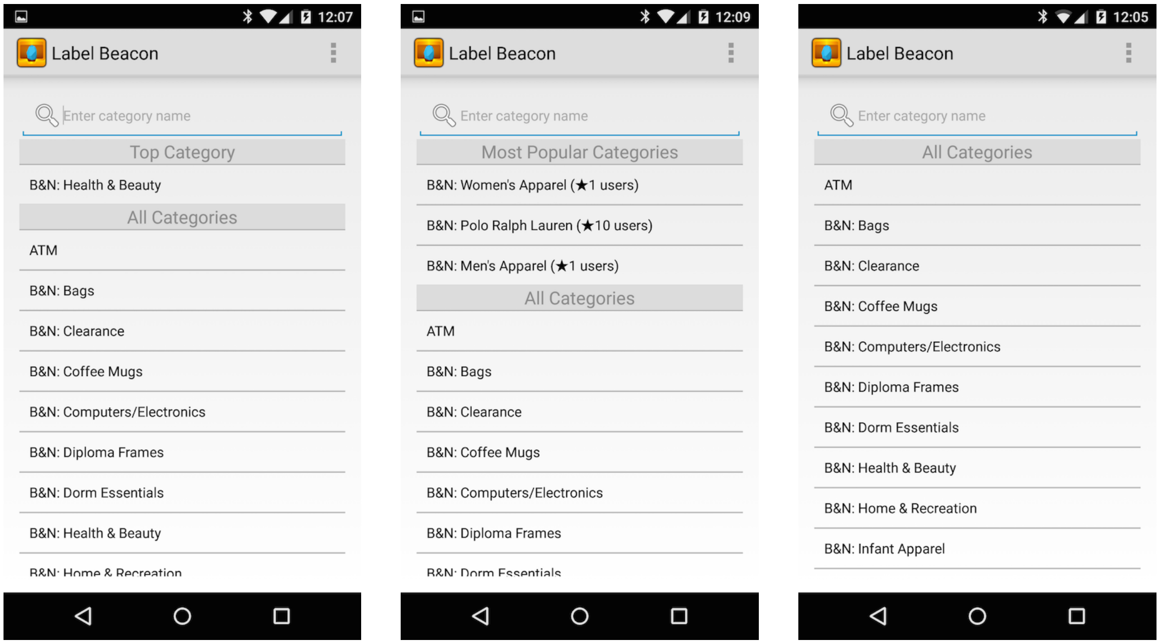
Beacons Found: 9/9
Accuracy: 9/9 correctly labeled
Time: 33 min 4 sec

Base Score: 270
Accuracy Bonus: +81
Time Bonus: +0

Total Score: 351
Redeemable Credit: $3.51

(f) Session Summary

Figure 12: Screenshots of BknBkts Android app



(a) TopCat (b) CrowdCat (c) NoCat

Figure 13: Category list views presented to users based on their study condition

score. Lastly, users were prompted to complete the post-survey, which was hosted on SurveyGizmo.com, after which they received their reward. In the end, all participants were given the full $5 reward.

4.2.3 Survey Flow

The post-survey for this study began with a few questions inquiring about demographic information for the participant, including age, gender, race/ethnicity, education, and technical expertise. These were followed by a series of 5-point Likert-scale questions evaluating the usability of the BknBkts mobile app. This subset of questions came directly from the System Usability Scale (SUS), a reliable tool and industry-standard in measuring usability [3, 9]. They captured items like complexity, consistency, confidence in use, likelihood of reuse, and technical expertise required to use. This was then followed by a question on the level of motivation by various forms of incentives to use the app for the function of providing beacon labels and privacy concern levels.

The subsequent section of the survey asked respondents about their general awareness/familiarity with standard Bluetooth, Bluetooth Low Energy, and BLE beacons using Likert-scale questions. A few open-ended questions were included to glean some qualitative information about respondents' knowledge of Bluetooth and BLE beacons. Respondents were also asked to evaluate beacons based on usefulness, relevance, and threat to privacy/security, to the best of their current knowledge. These questions were the same questions used in the pre-survey, and were asked again to determine any influence in perception that the study may have had on participants over the course of the study.

The remaining sections of the survey dealt with evaluating the level of trust that participants placed in the beacon category and privacy levels when they were provided through crowdsourcing, compared to assignment by a retailer/beacon provider and an independent third-party authority. These questions were on a 5-point Likert-scale, ranging from "No trust at all" to "Extreme trust." The goal of asking these questions was to go beyond the effectiveness of crowdsourcing and examine the users' trust in the approach to providing accurate contextual integrity. Respondents were then asked how much they agree that the context of information sharing impacts their willingness to share various information during a beacon encounter. The forms of information in question were beacon encounter information, mobile device information, demographic information, physical location, and personally identifiable information.

4.2.4 Analysis Procedure

In this study I was interested in the effectiveness of crowdsourcing as a method to incorporate user input and introduce contextual integrity regarding beacon encounters. This effectiveness was represented both by the accuracy (correctness) and efficiency (time/user burden) of beacon sensitivity and privacy concern labeling. For these factors, ANOVA was used to compare users between the three related conditions. I also reported on the percentage of recommended category labels that are selected by participants assigned to the respective conditions. Furthermore, I wanted to demonstrate the level of trust associated with these labels when crowdsourced by users for users, as compared to assignment by another party. Here I used split-plot repeated measures ANOVA tests to analyze responses to the corresponding survey questions, in order to determine the impact that the independent factors of condition and privacy concern had on the trust levels for labels crowdsourced by users, assigned by a beacon provider, or assigned by a third-party respectively.

Concerning usability of the crowdsourcing app, I used the provided SUS analysis procedure to generate a SUS score and interpret its meaning. Furthermore, I analyzed the impact of various levels of incentives on users' willingness to provide beacon category and privacy concern labels using ANOVA. As with the previous study, another important factor investigated involved general awareness of BLE beacons and users' perceptions regarding the privacy implications of the technology, this time examining how this changed before and after the user study. Hence I used repeated measures ANOVA tests to analyze the related pre- and post-survey questions. Lastly, I wanted to reveal how users explicitly believed context influenced their willingness to share various levels of beacon encounter information, and so repeated measures ANOVA was used here again. For all statistical tests, the α-value was 0.05.

4.3 Descriptive Results

I analyzed the app usage and survey responses from a total of 90 participants. The demographic breakdown of these participants can be seen in Table 5. Males made up 65.6% of participants and females were the remaining 34.4%. Regarding age, 62.2% were between 18-24, while 32.2% were ages 25-34, and then remaining 5.6% fell between 35-54. Lastly, the main levels of education that users completed included some college with 43.3% of participants, bachelor's degree with 22.2% of participants, and graduate degree with 26.7%.

Table 5: Participants' demographic summary

Gender	%	Age	%	Education	%
Male	65.6	18-24	62.2	Some college	43.3
Female	34.4	25-34	32.2	Graduate	26.7
		35-64	5.6	Bachelor	22.2
				High school	4.4
				Associate	3.3

4.3.1 Accuracy of Crowdsourcing

Of the 90 participants that were recruited, 30 were grouped into each condition, and the mean accuracy for each group is represented in Table 6. The TopCat group showed the highest accuracy of all the participants, at 94.074%, while the CrowdCat group had an accuracy of 92.592%, and the NoCat group was the least accurate in labeling, at 86.667%. This shows that without any recommended labels, participants are not as accurate, and it would appear that crowdsourcing labels provides an accuracy that is close to that of exact category recommendations. Furthermore, I note that the TopCat group arrived at 94% accuracy instead of 100%, even though they were informed that the one category at the top of their list represented a label generated by the bookstore itself, and therefore was the most correct one. This can be attributed to a number of reasons. First, participants were still free to choose whatever label they believed was correct, and in some cases, they did choose an incorrect label. Additionally, some beacon categories were more prone to erroneous labeling, due to their placement; for example, not all beacons were eye-level, and some were placed in between sections. Still, for those in the TopCat group, who were given the correct answer, I anticipated that they would not be as prone to incorrect labeling with these situations. Lastly, a few participants were not able to find and label all the beacons during their session; in the TopCat group, however, out of total possible 270 labels, 269 were provided, meaning only one label was missing from a single participant in this group. In the CrowdCat group, two labels were missing, and one label in the NoCat group. Hence, the major contributing factor that led to the 6% error in this condition was incorrect labeling.

Table 6: Mean accuracy percentage per condition

Condition	Mean (μ)	St. Dev	N
TopCat	94.074	9.103	30
CrowdCat	92.592	9.823	30
NoCat	86.667	10.275	30

In order to compare the effect of condition on the mean accuracy for the three groups, I used a one-way ANOVA test. This revealed a significant effect of condition on accuracy, with F(2,87) = 4.853, p=.010. Table 7 reflects the results of the post hoc comparisons performed, using the Tukey HSD test, with statistically significant results yielding a p-value less than .05. I found that there was no significant difference between the accuracy for the TopCat group and CrowdCat group, but there was between CrowdCat and NoCat (p=.05), as well as between TopCat and NoCat (p=.011). Logically I would expect the TopCat group to perform better in labeling beacons than the NoCat group, which was not given any labeling recommendation. However, these results also confirmed that crowdsourcing is more effective in accuracy than no recommendation at all, and that the crowd can be relied on to provide categorizations that are comparable in accuracy with the exact categories.

Table 7: Mean accuracy post hoc comparisons

Condition A	Condition B	μ_A-μ_B	p-value
TopCat	CrowdCat	1.481	.827
CrowdCat	**NoCat**	**5.925**	**.050**
TopCat	**NoCat**	**7.407**	**.011**

4.3.2 Time Efficiency of Crowdsourcing

In addition to accuracy, the other aspect of effectiveness that I sought to prove regarding our beacon labeling crowdsourcing approach was time efficiency. This was represented by the average amount of time users took to complete a labeling task for a beacon. Table 8 captures the mean time for each of the three groups, where N is the number of beacon labels captured that were attributed to that group. The TopCat group, as expected, had the fastest mean time, of 6.662 seconds, while the CrowdCat group had a mean label time of 8.349 seconds. The NoCat group had a mean label time of 11.280 seconds, meaning those who were not recommended any label had the slowest labeling time.

Table 8: Mean label time per condition, in seconds

Condition	Mean (μ)	St. Dev	N
TopCat	6.662	13.618	269
CrowdCat	8.349	18.440	268
NoCat	11.280	14.546	269

Since time measurements are not an unbounded normal variable, I performed a logarithmic transformation on the time, and then performed a one-way ANOVA to compare the effect of the study condition on time. This revealed a significant effect of condition on time, with F(2,87)=9.535, $p < .001$. Table 9 reflects the post hoc comparisons done using the Tukey HSD test. The results were similar to the findings related to labeling accuracy: I found that there was not a significant difference between the time efficiency for the TopCat group and CrowdCat group, but there was a significant difference between CrowdCat and NoCat (p=.024), as well as between TopCat and NoCat ($p < .001$). Taken together, this means that the crowd can be relied upon to quickly determine beacon labels with an efficiency that is comparable to users who are given the correct category. Another way to consider this outcome is that the user burden for crowdsourcing is sufficiently acceptable compared to being directly provided the category.

Table 9: Mean log time post hoc comparisons

Condition A	Condition B	μ_A-μ_B	p-value
TopCat	CrowdCat	-.1211	.223
CrowdCat	**NoCat**	**-.1978**	**.024**
TopCat	**NoCat**	**-.3190**	**.000**

With confidence in the accuracy and efficiency of the crowdsourcing approach established, I examine the acceptance of the crowdsourcing approach: of the 268 recommended labels generated for the CrowdCat group, 82% of the recommendations were taken by those participants. What I mean here is that 82% of participants in this group accepted some label recommendation that was provided by the crowd; this was not necessarily the response that was selected the most by the crowd. As Figure 13b indicates, labels recommended via the crowd had an accompanying count of users that chose this label. Compare the CrowdCat group's acceptance rate to the 94% acceptance of recommendations by users in the TopCat group. Again, one might expect the acceptance rate of the TopCat to be 100%, but as mentioned earlier, participants in this group did not always chose the top category, for various reasons. Participants were still able to make a selection beyond the recommendation, by choosing from the entire list. I observed that 3% of TopCat users noted the recommendation, but still searched through the whole list for a correct label, and though they may have ultimately selected the correct label, it was done so by choosing it from the main list, instead of choosing the recommended label at the top of the list.

4.3.3 Trust in Crowdsourcing

I analyzed trust in the beacon category labels as well as in beacon privacy labels when they are provided from a beacon provider/retailer, the crowd, and from an independent third-party respectively. I sought to answer the following questions:

- Is there a difference in trust of labels when provided by the retailer/beacon provider, the crowd, or an independent third-party? (within-subjects)

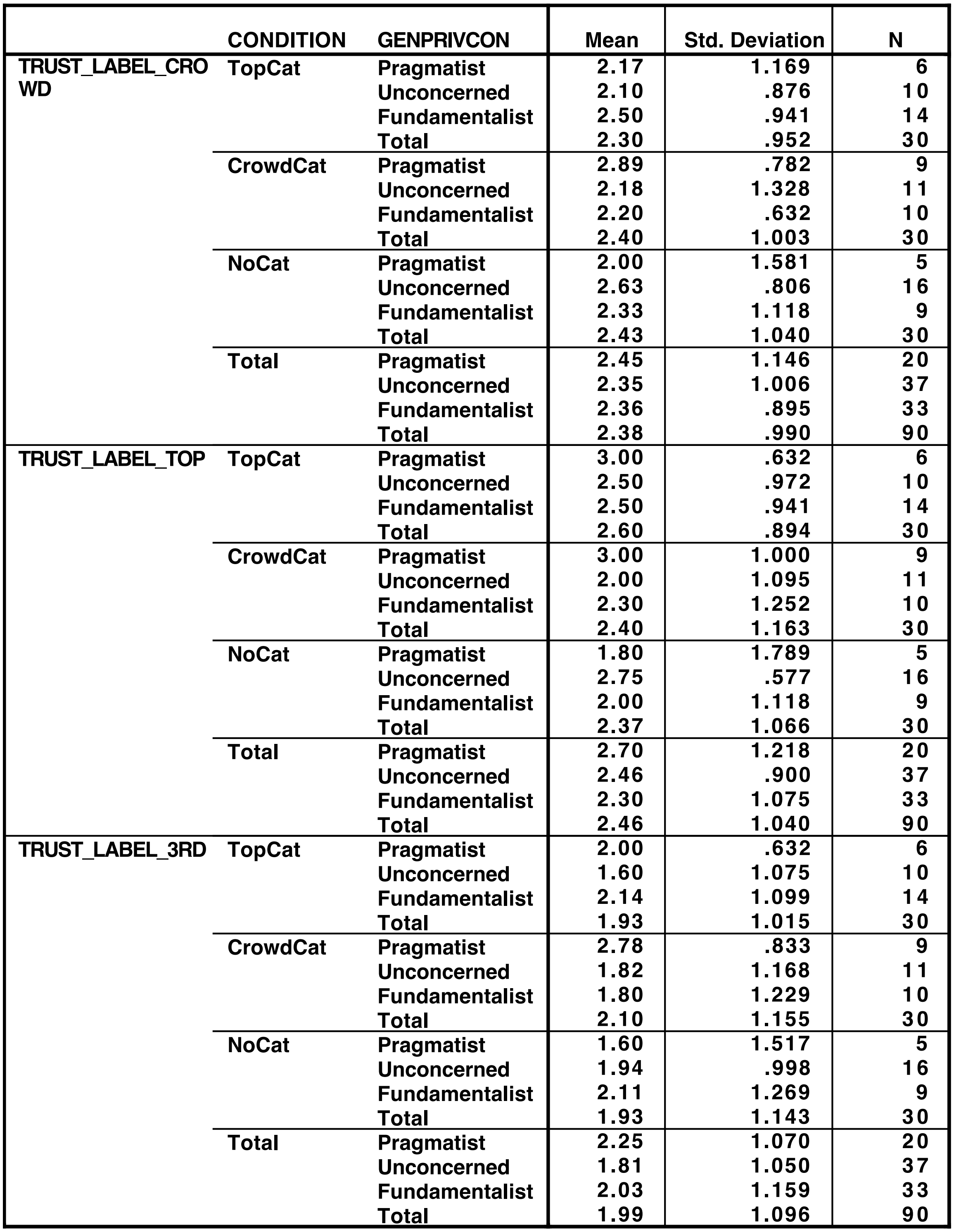
- Is there a difference in trust levels between condition groups? (between-subjects)

- Is there a difference in trust across privacy concern groups? (between-subjects)
- Is there an interaction between condition group and level of trust? (mixed)
- Is there an interaction between privacy concern and level of trust? (mixed)

In order to answer these questions, the three different groups of label providers were considered as within-subject independent factor terms, while the mean trust levels for both category and privacy were considered our dependent factors respectively. I also looked at the participants' determined privacy concern, as well as their assigned conditions of TopCat, CrowdCat, or NoCat, as independent factors. In this way, I performed a split-plot repeated measures ANOVA tests to analyze all the different interactions. Table 10 reflects the cross tabulation of mean category trust levels for each label provider, groups by condition group as well as privacy concern group, and Table 11 shows the same information for privacy label trust levels. I hypothesized that the trust levels would not differ among the various independent variables for beacon categories, as determining the categories can be seen as objective, but that trust in the privacy label would depend on the provider (in favor of the crowd) and on the privacy concern of the user.

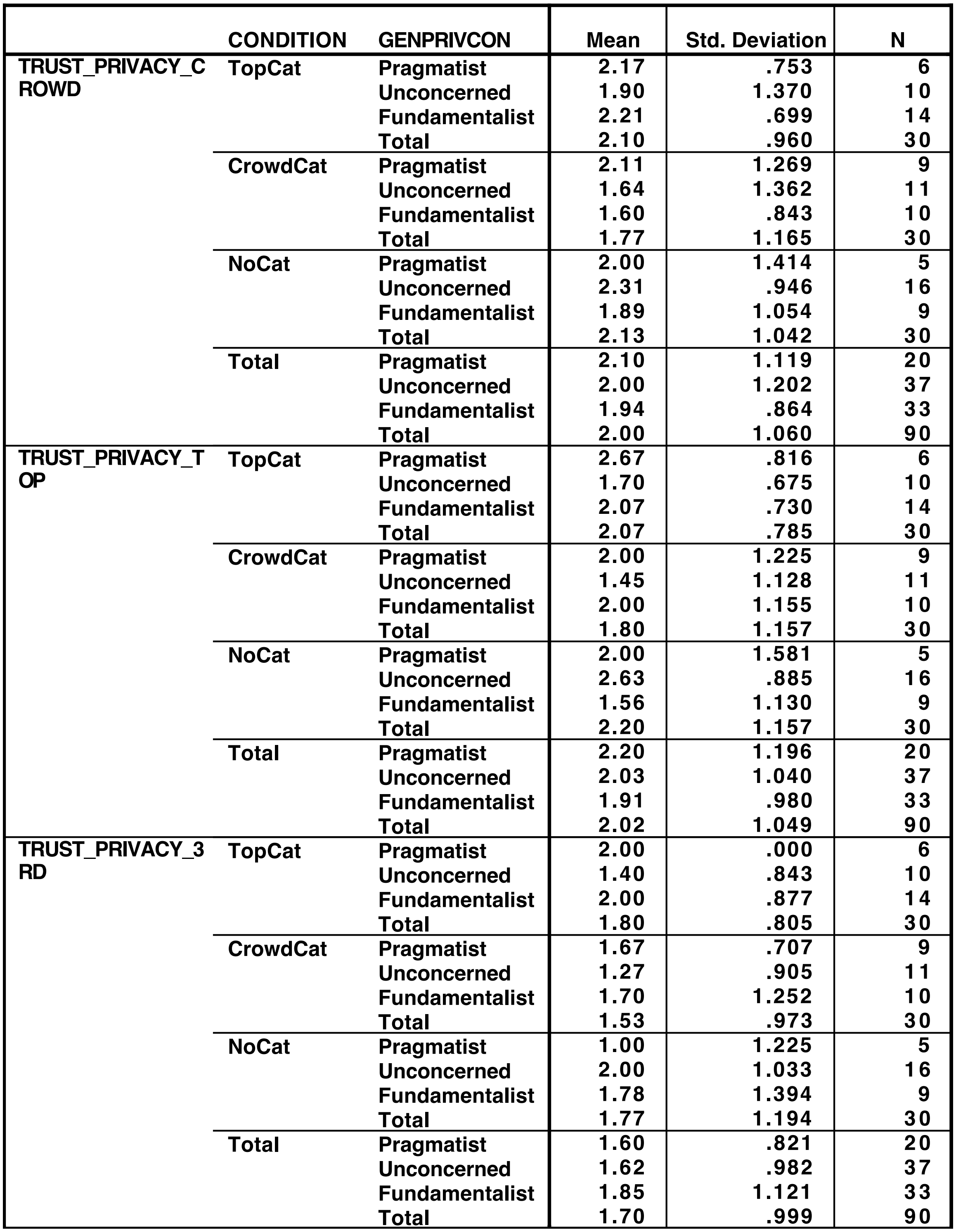
Based on the mixed ANOVA tests I ran, I found that the only factor that had a statistically significant influence on trust levels for both beacon category and privacy labels was the label provider, with $F(2,80)=8.206$, $p < .001$ for category labels and $F(2,80)=7.285$, $p < .001$ for privacy labels. That means I can say with certainty that the level of trust in the labels provided depends on who is providing them. To determine the amount of trust for each provider, I performed post hoc comparisons.

Table 10: Descriptive statistics for users' levels of trust in beacon **category** labels grouped by condition and general privacy concern



	CONDITION	GENPRIVCON	Mean	Std. Deviation	N
TRUST_LABEL_CROWD	TopCat	Pragmatist	2.17	1.169	6
		Unconcerned	2.10	.876	10
		Fundamentalist	2.50	.941	14
		Total	2.30	.952	30
	CrowdCat	Pragmatist	2.89	.782	9
		Unconcerned	2.18	1.328	11
		Fundamentalist	2.20	.632	10
		Total	2.40	1.003	30
	NoCat	Pragmatist	2.00	1.581	5
		Unconcerned	2.63	.806	16
		Fundamentalist	2.33	1.118	9
		Total	2.43	1.040	30
	Total	Pragmatist	2.45	1.146	20
		Unconcerned	2.35	1.006	37
		Fundamentalist	2.36	.895	33
		Total	2.38	.990	90
TRUST_LABEL_TOP	TopCat	Pragmatist	3.00	.632	6
		Unconcerned	2.50	.972	10
		Fundamentalist	2.50	.941	14
		Total	2.60	.894	30
	CrowdCat	Pragmatist	3.00	1.000	9
		Unconcerned	2.00	1.095	11
		Fundamentalist	2.30	1.252	10
		Total	2.40	1.163	30
	NoCat	Pragmatist	1.80	1.789	5
		Unconcerned	2.75	.577	16
		Fundamentalist	2.00	1.118	9
		Total	2.37	1.066	30
	Total	Pragmatist	2.70	1.218	20
		Unconcerned	2.46	.900	37
		Fundamentalist	2.30	1.075	33
		Total	2.46	1.040	90
TRUST_LABEL_3RD	TopCat	Pragmatist	2.00	.632	6
		Unconcerned	1.60	1.075	10
		Fundamentalist	2.14	1.099	14
		Total	1.93	1.015	30
	CrowdCat	Pragmatist	2.78	.833	9
		Unconcerned	1.82	1.168	11
		Fundamentalist	1.80	1.229	10
		Total	2.10	1.155	30
	NoCat	Pragmatist	1.60	1.517	5
		Unconcerned	1.94	.998	16
		Fundamentalist	2.11	1.269	9
		Total	1.93	1.143	30
	Total	Pragmatist	2.25	1.070	20
		Unconcerned	1.81	1.050	37
		Fundamentalist	2.03	1.159	33
		Total	1.99	1.096	90

Table 11: Descriptive statistics for users' levels of trust in **privacy** labels grouped by condition and general privacy concern



	CONDITION	GENPRIVCON	Mean	Std. Deviation	N
TRUST_PRIVACY_CROWD	TopCat	Pragmatist	2.17	.753	6
		Unconcerned	1.90	1.370	10
		Fundamentalist	2.21	.699	14
		Total	2.10	.960	30
	CrowdCat	Pragmatist	2.11	1.269	9
		Unconcerned	1.64	1.362	11
		Fundamentalist	1.60	.843	10
		Total	1.77	1.165	30
	NoCat	Pragmatist	2.00	1.414	5
		Unconcerned	2.31	.946	16
		Fundamentalist	1.89	1.054	9
		Total	2.13	1.042	30
	Total	Pragmatist	2.10	1.119	20
		Unconcerned	2.00	1.202	37
		Fundamentalist	1.94	.864	33
		Total	2.00	1.060	90
TRUST_PRIVACY_TOP	TopCat	Pragmatist	2.67	.816	6
		Unconcerned	1.70	.675	10
		Fundamentalist	2.07	.730	14
		Total	2.07	.785	30
	CrowdCat	Pragmatist	2.00	1.225	9
		Unconcerned	1.45	1.128	11
		Fundamentalist	2.00	1.155	10
		Total	1.80	1.157	30
	NoCat	Pragmatist	2.00	1.581	5
		Unconcerned	2.63	.885	16
		Fundamentalist	1.56	1.130	9
		Total	2.20	1.157	30
	Total	Pragmatist	2.20	1.196	20
		Unconcerned	2.03	1.040	37
		Fundamentalist	1.91	.980	33
		Total	2.02	1.049	90
TRUST_PRIVACY_3RD	TopCat	Pragmatist	2.00	.000	6
		Unconcerned	1.40	.843	10
		Fundamentalist	2.00	.877	14
		Total	1.80	.805	30
	CrowdCat	Pragmatist	1.67	.707	9
		Unconcerned	1.27	.905	11
		Fundamentalist	1.70	1.252	10
		Total	1.53	.973	30
	NoCat	Pragmatist	1.00	1.225	5
		Unconcerned	2.00	1.033	16
		Fundamentalist	1.78	1.394	9
		Total	1.77	1.194	30
	Total	Pragmatist	1.60	.821	20
		Unconcerned	1.62	.982	37
		Fundamentalist	1.85	1.121	33
		Total	1.70	.999	90

The post hoc comparisons revealed similar results regarding user trust for both beacon category and beacon privacy labels. Regarding the trust in beacon category labels, Table 12 shows the mean difference between trust in crowdsourced labels (μ=2.38) and third-party provided labels (μ=1.99) with a p-value of .003, and the mean difference between retailer-provided labels (μ=2.46) and third-party provided labels is also positive, with a p-value less than .0001. Regarding the trust in beacon privacy label, Table 13 shows that the mean difference between trust in crowdsourced labels (μ=2.00) and third-party provided labels (μ=1.70) had a p-value of .002, while the mean difference between retailer-provided labels (μ=2.02) also had a p-value of .002. There was no significant difference found between trust in crowdsourced labels and retailer-provided labels for either post hoc test. What this means is that for both beacon category and beacon privacy labels, users trust crowdsourced and retailer-provided labels over those provided by an independent third-party, and they consider crowdsourced and retailer-provided labels equally trustworthy.

Table 12: Post hoc pairwise comparison for users' levels of trust in **category** labels

Condition A	Condition B	μ_A-μ_B	p-value
Crowd	Retailer	-.095	.347
Crowd	**Third-party**	**.356**	**.003**
Retailer	**Third-party**	**.451**	**.000**

Table 13: Post hoc pairwise comparison for users' levels of trust in **privacy** labels

Condition A	Condition B	μ_A-μ_B	p-value
Crowd	Retailer	-.027	.810
Crowd	**Third-party**	**.335**	**.002**
Retailer	**Third-party**	**.362**	**.002**

It is interesting to note that even something objective like the beacon category labels are still trusted more when derived from the crowd over an independent party. Furthermore, though I had predicted that users would trust beacon privacy labels coming from the crowd over other sources, I speculate that the comparable trust in the retailer-provided labels may have been influenced by trust in the retailer of the user study, which was the campus Barnes & Noble bookstore. This could be considered an extension of the trust in the University in general that would be expected. Familiarity often breeds trust, and given that a majority of the participants were students at the University, that familiarity with the bookstore and/or the University in general may be what framed their perspective regarding trust of retailer-provided beacon category and privacy labels. Nonetheless, I can say with certainty that users do trust crowdsourced labels, making this an effective and trustworthy approach.

4.3.4 Usability of Crowdsourcing

Although usability is generally a subjective feature, assessing the general quality of appropriateness of an artifact is still imperative. Consider how even the most effective tool created can only be as useful as its users consider it to be. The same can be said for this crowdsourcing approach to beacon labeling: though quantitatively proven to be effective so far, if its implementation is not considered usable by users, then it is still rendered an ineffective approach. As a result, I used the industry-standard System Usability Scale (SUS) to evaluate the usability of our scavenger hunt game based on the responses to the provided Likert-scale questions. SUS yields a single number representing a composite measure of the overall usability of the system.

It is important to note that though it is tempting to interpret the score as a percentage, it is not such, nor is it meant to be diagnostic, but simply an evaluation of an application's ease of use [47]. Based on the given formula [9], I generated an overall SUS score of 66.1 for the BknBkts app. According to prior research, a SUS score above 68 is above average for general applications, but for cell phone applications, a score above 65.9 is acceptable. Figure 14 represents the SUS scale for general applications, with a marker indicating how the BknBkts app's score compares. There is room to improve, but since our app's score is above average for mobile phone applications, I am confident that it can be considered a usable approach.

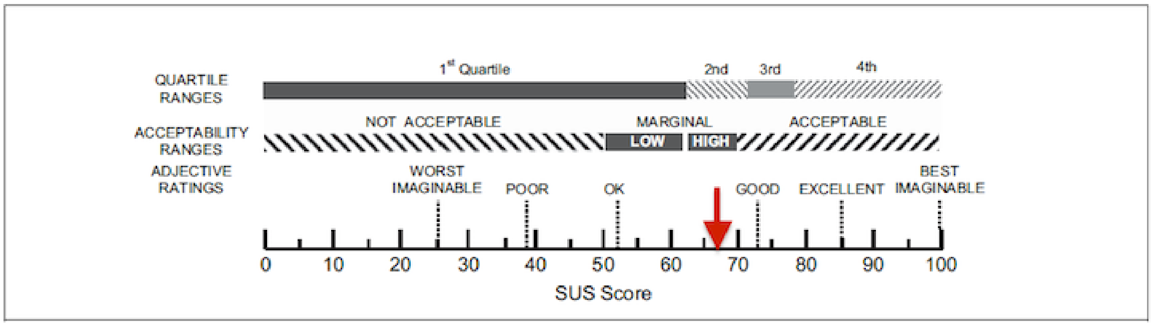


Figure 14: General SUS Scale, with red arrow indicating BknBkts' score

4.3.5 Motivating the Crowd through Incentives

In order to demonstrate the level of motivation that users associated with each the three forms of incentives, I performed a one-way repeated measures ANOVA, where the incentives were considered within-subject terms. The scale for the corresponding survey questions was a 5-point Likert from 0 to 4, where 0 represented "Not motivated at all" and 4 represented "Extremely motivated." The mean motivation levels for each incentive are shown in Table 14, and the ANOVA test resulted in F(2,88)=4.067, p=.020. Monetary/cash incentives had the highest mean motivation rating at 2.12, or "somewhat motivated," while Game Points had the lowest mean motivation rating of 1.70, closer to "slightly motivated." Since the p-value yielded was less than .05, there was a significant difference in motivation levels between incentives. In order to determine where the difference was, I computed post-hoc pairwise comparisons between the three incentive types, the results of which can be found in Table 15.

Table 14: Mean motivation levels for incentives

Incentive	Mean (μ)	St. Dev	N
Monetary/Cash	2.12	1.322	90
Coupons/Discount	1.94	1.239	90
Game Points	1.70	1.353	90

Table 15: Pairwise comparisons of different motivation levels for various incentives

Condition A	Condition B	μ_A-μ_B	p-value
Monetary	Coupons	.178	.081
Coupons	Points	.244	.070
Monetary	**Points**	**.422**	**.006**

What I found in the comparisons is a statistically significant difference in motivation rating between Monetary and Game Points incentives (p=.006). There was no difference found between Monetary and Coupon/Discounts, which makes sense, given that coupons/discounts still suggest pecuniary value, even if they it is not a literal cash value. Additionally, no difference was found in motivation between Coupons and Points. As expected, monetary/cash incentives are therefore the most influential motivator among the common forms of incentives; taking this one step further, additional research could be conducted to see what users feel is a fair amount to receive for contributing to a beacon label crowdsourcing campaign.

4.3.6 With Privacy, Context is King

Looking at the privacy labels generated by users, I recall that these reflected the perceived sensitivity of a beacon based on its assigned category label, as well as users' willingness to share their location with various circles of people. By averaging these responses, I got an aggregate view of the privacy labels, which is represented in Table 16. In this table, the Sensitivity column represents a rating between 0 and 100, where 0-32 is considered Low Sensitivity and therefore of minimal privacy concern, 33-65 as Medium, and 66-100 as High and therefore of highest privacy concern. Additionally, the values under the "Share with" columns in the Table represent the percentage of users who were willing to share their presence at that particular beacon location with the corresponding social circle: Friends, the University, the Bookstore, or the General Public.

Table 16: Averages for privacy label responses per beacon category: Sensitivity is on a scale from 0-100, and Sharing represents percentage of users willing to share; A plus (+) represents significantly different from ATM, and an asterisk (*) represents significantly different from Starbucks.

Beacon	Sensitivity	Friends	Bookstore	University	Public
ATM	87.84	$44\%^{*}$	$21\%^{*}$	$30\%^{*}$	$13\%^{*}$
Restrooms	72.00	$53\%^{*}$	$31\%^{*}$	$35\%^{*}$	$24\%^{*}$
Health/Beauty	64.37	$73\%^{+*}$	$68\%^{+}$	$47\%^{*}$	$33\%^{+*}$
Shot Glasses	63.57	$70\%^{+*}$	$68\%^{+}$	$46\%^{*}$	$36\%^{+*}$
Ralph Lauren	49.73	$83\%^{+}$	$87\%^{+*}$	$71\%^{+}$	$50\%^{+}$
Clearance	48.99	$76\%^{+*}$	$83\%^{+*}$	$66\%^{+}$	$51\%^{+}$
Women's Athl.	47.13	75%	70%	57%	38%
Magazines	46.23	$84\%^{+}$	$86\%^{+*}$	$70\%^{+}$	$55\%^{+}$
Starbucks	46.10	$91\%^{+}$	$62\%^{+}$	$71\%^{+}$	$58\%^{+}$

Based on Table 16, I found that the Sensitivity was highest for the ATM beacon, followed by the Restrooms beacon, which had an average rating of 87.84 and 71.88

respectively. Furthermore, the percentage of users willing to share their location here was lowest across the various social circles for these two beacon categories as compared to the others, as I expected. On the other end of the spectrum is the Starbucks beacon, which had a mean Sensitivity rating of 46.10. Even with this rating of Medium Sensitivity, it was the lowest of all the beacons, which was again as I expected. Similarly, the "Share with" percentages were the highest across most of the social circles for this beacon, with a reported 91.11% of participants willing to share their presence here with Friends, the highest amount of all the beacons and social circles.

For the remaining beacon categories, I observed a variation of sensitivity in the privacy labels reported. I note that none of them were regarded as Low Sensitivity beacons. Shot Glasses and Health & Beauty were the two categories with the next highest Sensitivity ratings, at 63.57 and 64.37 respectively. This would place them on the higher end of the Medium Sensitivity range (33-65), bordering High Sensitivity. For the Shot Glasses beacon, I believed it was perceived this way because of the association with alcohol and drinking; any indication of visiting this section of the bookstore too often might suggest the user engages in frequent drinking, which typically has negative connotations. Concerning the Health & Beauty category, I found that the Bookstore sold products here that included condoms, feminine care, and other personal hygiene items. It makes sense that users would consider this a sensitive beacon, as it is unlikely that they would be comfortable sharing their presence or purchase of these kinds of products with many others.

Lastly, the beacons with categories Clearance, Magazines, Polo Ralph Lauren, and

Women's Athletic all had a Medium Sensitivity rating that was similar to that of the Starbucks beacon, ranging between 46.23 and 49.73. Their respective percentages for users' willingness to share location information with different social circles were also comparable as well. This also makes sense, as three of the four categories were clothing-related, and furthermore, given the type of clothes and magazines sold at the campus bookstore, neither the related items nor a known proximity to these items would likely pose a privacy threat to visitors.

For these beacons that were observed, the ATM beacon was used as a "ground truth" for what I hypothesized would be regarded the most sensitive beacon, because I believed users would not feel comfortable sharing every time they visited an ATM, likely to withdraw money. It could be further hypothesized that this comes from more than just a desire for information privacy, but also a sense of physical safety/security when carrying money on themselves. On the other hand, the Starbucks beacon was used as the benchmark for the least sensitive beacon, given how public of a location Starbucks is generally considered. The remaining beacons could then be compared against these ground truths to determine what kind of privacy concern users associated with a beacon based on its category when sharing their encounter, as well as potential audiences of that information (Friends, Bookstore, University, and Public). Using the established ground truth beacons, my null hypothesis was that probability of a "Yes" response in willingness to share was the same for all categories of beacons, and my alternative hypothesis was that the probability that participants responded with a "Yes" in willingness to share was different depending on beacon, where they are more likely to respond "No" for the ATM beacon and more likely to respond "Yes" for the Starbucks beacon, in each of the different audiences.

In order to prove that these differences in privacy labels supported the existence of context as an influencer of privacy perceptions, I relied on statistical analysis to determine significant results. To do this, I used the Cochran's Q test for k-related samples. This provides a reliable way to test whether multiple matched sets of frequencies differ significantly among themselves. In this design, our "k" related samples are the beacons, and they are considered matched because each participant provides a response on willingness to share for each beacon, and for each audience. This test is particularly useful when the data are categorical or nominal, which was the case with our beacon data; the response for willingness to share was dichotomized as "Yes" or "No." With this test, the number of individual responses in each of the matched response sets (N=59) was less than the total 90 participants, because the test analyzes only the complete matched sets, those being where a response was provided for all beacons. Not every participant provided 9 beacon labels, and not every participant that did so was able to correctly identify the 9 beacons in question; hence, the test dropped the Women's Athletic Apparel beacon, the beacon that was missed the most (either incorrectly labeled or not labeled at all), and considered "k" to be the 8 remaining beacons, thereby causing N to be 59.

Looking at participants' willingness to share beacon location information among the Friends audience first, I found that the Cochran's Q test resulted in Q = 76.245, with a p-value less than .001. With an alpha of .05, I rejected my null hypothesis in favor of the alternative hypothesis. Similarly, making the same comparisons within the Bookstore audience, I generated Q = 129.284 with a p-value less than .001. For the University audience, the test resulted in $Q = 87.062$, p-value less than .001. Lastly, for the Public audience, I generated $Q= 78.821$, with p less than .001. Consequently, on the basis of these data, I conclude that the probability that participants are willing to share their presence at a beacon differs significantly between the beacons, for each audience.

I conducted multiple post hoc pairwise tests using the McNemar test to determine where the difference was in willingness to share for different beacons for each audience. Cochran's Q test is an extension of McNemar, which is a nonparametric test specifically for two-sample cases, making the latter an appropriate test for post hoc comparisons. For the purpose of simplicity, instead of conducting McNemar on every pairing of beacons, I only used our ground truth beacons of ATM ("most sensitive") and Starbucks ("least sensitive"), and I conducted the McNemar test between each of these beacons respectively and the remaining seven beacons. This resulted in 14 pairwise comparisons under each audience, seven with the ATM beacon and seven with the Starbucks beacon. Our alpha was .0035 (.05/14), which was Bonferroni corrected, to counteract the issue of multiple testing. The pairings that resulted in significant differences are represented in Table 16, where a plus (+) represents significantly different from ATM, and an asterisk (*) represents significantly different from Starbucks. Through examination of crosstabs for each comparison, I confirmed that participants were more likely to respond "No" in willingness to share for the ATM beacon than any beacon from which it was significantly different, and "Yes" for the Starbucks beacon versus any others.

With these results, I confidently assert that context does impact the privacy perceptions of users in their willingness to share beacon information.

4.4 Discussion

As the first work of its in kind in the domain of BLE beacons, it is important to identify both strengths and weaknesses of this crowdsourcing approach, so that it can continually be refined and improved. One clear strength is that users did not have a difficult time in expressing privacy labels for beacons. Yet, as Lin et al. admitted in a similar approach [28], one limitation is the realization that users may often weigh utility over privacy and security when making decisions. An extension to this research could include explicitly investigating the role of utility to maintain a more honest level of context. Security of a crowdsourcing approach is an angle that was outside the scope of this study, but is certainly worth researching a future iteration, such as when exploring how to best incorporate this approach into the beacon privacy manager this research is moving towards.

Furthermore, while using the concept of contextual integrity as inspiration for this study, admittedly this applies in a limited scope. When considering the privacy labels for beacons, the study primarily examines the "context of flow of information" aspect of contextual integrity, specifically the per-beacon and per-audience context of flows of information, as well as the capacities in which the participants were acting in choosing to share. An extension to the study could additionally focus on the other components of contextual integrity, such as type of information involved. For example, I could expand the concept of beacon information involved to include the different beacon metrics, such as beacon encounter frequency, duration, or travel path. Another logical extension is to explore the principles of transmission. Here, I could investigate on what basis the beacon information could be collected and shared, be it legal requirement, in exchange for an incentive, or the promise of anonymity. This could lead to more comprehensive results from the crowd, based on a more accurate representation of context. Concerning the user study design, another limitation was the presence of "Average User Concern" in the user interface for those in the CrowdCat group. This may have somewhat artificially inflated the findings of the privacy label analysis, and more extensive experiments are required to make truly conclusive results.

In this study there is also concern for confounding variables within our study design. For example, participants were instructed about where the labels came from; TopCat users were told that the recommended label could be considered as if "provided by the bookstore itself," which may have made TopCat participants question the point of labeling. Additionally, it would appear that the study confounds the number of recommended labels provided with the type of labels, although I defend this design decision with the justification that the number of labels is actually an integral part of the different conditions. There is only one correct category for each beacon, and so the TopCat should only see one recommended label. For the CrowdCat group, on the other hand, there may be a tie in recommended labels, particularly in that initial period where there are not sufficient contributions for any label to pull ahead as the top label. So it is important to reveal more than one option in this condition. Furthermore, users are still able to come to a reasonable decision regarding the top choice among the crowdsourced labels, given that these labels were marked with a count of the number of users who had selected that label before them. Yet this count in itself could be considered a confounding variable. Lastly, it is possible that participants could have encouraged their friends to take part in the study and coach them on the correct answers, this was not something for which I controlled.

One of the more critical limitations to acknowledge is the lack of a proper bootstrap or seeding mechanism, in order to address the “cold start” problem that is typical of early-stage recommender and crowdsourcing systems. This study did not address the negative implications, such as potential of information cascading, where users may observe incorrect beacons labels provided from the crowd, and despite their own inclinations, follow the same labeling. This would lead to a waterfall of incorrect labels, thereby weakening the accuracy of the crowdsourcing approach. Fortunately I did not observe any evidence of this in our study results, but I recognize that this is something for which I would have to account and correct in a future application of this approach. For example, I could implement a heuristic where recommendations are not made for beacons until at least 3 labels in agreement have been provided. Alternatively, I could collect some manual input, or use another set of heuristics to generate likely labels. In the end, the purpose of this study was to show what was possible with crowdsourcing for context and privacy, and I achieved this goal. Going forward, this provides the confidence to rely on these findings to implement a more stable and robust crowdsourcing approach.

4.5 Conclusion

The long term vision of this research is to design a beacon privacy management framework that leverages crowdsourcing to incorporate context into privacy policy configuration for beacons. In this way, I can empower users to manage their own location information privacy during beacon encounters. I intend to achieve this framework by defining beacon privacy policy creation in such a way that both the beacon provider and the user can benefit from the data gleaned from location-based profiling, without putting users at risk of privacy invasion. Through the results of the study addressed in this paper, I have demonstrated the feasibility of crowdsourcing as a critical component of this vision. As future research, these crowdsourced considerations can be used to extend the beacon privacy framework, moving from a pure management system to a recommender-based system, suggesting privacy policies based on similar beacon categories and configurations, as well as users' general privacy concern profile.

CHAPTER 5: BEACON PRIVACY FRAMEWORK

Given the previous research mentioned in Chapter 4 demonstrating the feasibility of the crowdsourcing approach as a way to introduce greater context during beacon encounters, the next step is to leverage this context to develop a general model that will allow users to create informed privacy policies. Consequently, in this chapter I propose the first privacy framework BLE beacons. This is a novel and significant contribution to the domain of BLE beacons, particularly with respect to privacy policy frameworks. Because of this, it is important to have a firm grasp on the current state of privacy policy guidelines and paradigms in information privacy, in order to understand the design decisions incorporated. As a result, in this section I first present an overview of existing literature related to information privacy policies, and then I describe the general framework design and recommended policy models.

5.1 Background

Many researchers across the field of computer science have explored the notion of privacy and the reasonable expectation of it that users may have when interacting with technology. Most notably, a wealth of research exists with regards to privacy-related issues on the Internet, especially in online social networks (OSN). A broad set of solutions have been offered to address these issues, ranging from tangible software tools to design principles of guidelines. For example, Besmer et al. investigated the third-party social applications developed for Facebook in order to formally define the current access control model applied to them [5]. In this model, Facebook allows user-to-user policies to be set, but adopts an all-or-nothing policy when it comes to these applications, meaning either an application is granted all request attributes of a user's profile or it can not be installed at all. Besmer et al. then improved upon this model by introducing a new user-to-application policy that strikes a balance between protecting and sharing, all while trying to preserve as much of the current architecture as possible. To do this, they introduced an interface design by which to apply this policy, and evaluated their framework through a user study. Ultimately, they concluded that the model and interface are successful for users who are already more privacy-conscious, but is ineffective for those who are less concerned.

In a future study, Besmer et al. revisited privacy policies regarding third-party Facebook applications, this time exploring the impact of social navigation on these policies by adding relevant cues to their policy interface [6]. Social navigation, defined as "the use of social information to aid a user's decision," has already been applied to several privacy and security systems, including peer-to-peer file sharing, cookie management, and firewalls, but there is little empirical evaluation of its impact on in said systems, particularly when creating privacy policies. Through an experiment where users had to set policies for a number of applications with varying social cues, they found that social navigational cues can impact users' decisions, but only when those visual cues are sufficiently strong. Related to this focus on visual representation, Lipford et al. further compared the impact of two different interfaces, "Audience View" and "Expandable Grids," on the privacy policies users created for

Facebook profiles [30]. Specifically, they recruited participants to complete 17 individual tasks on the two interfaces, rate their confidence in these tasks, and then be interviewed about their preference for each interface. Though the interfaces were very different, performance between the two did not vary, but their findings resulted in very clear and distinct preferences. Acknowledging the tradeoffs between both visual representations, Lipford et al. recommended a combination to best appeal to a wider audience.

In the first study by Besmer et al. previously mentioned [5], they contemplated methods by which to introduce their new user-application policy configuration; they considered asking users to indicate all of their preferences the first time they access or install an application, though they recognized this takes time, especially for complex policies. Alternatively, an application could request permission for each individual access to a user's data item, but research shows that timing is everything, and users tend to ignore frequent pop-up messages, which would diminish the quality of privacy decisions made by users over time [13]. Lastly, they could provide users with special settings for each application in order to view or modify their policies at any time. Ultimately, they settled on users' setting all preferences upon installation. Nonetheless, all of these considerations are examples of design choices for privacy configurations, each appropriate for difference audiences or situations. While there is limited guidance available for designers and developers regarding best practices in this area, Shaub et al. surveyed existing literature and mapped out the current design space in order to provide a useful taxonomy by which related research, including that which I contribute in this dissertation, can be informed when constructing privacy

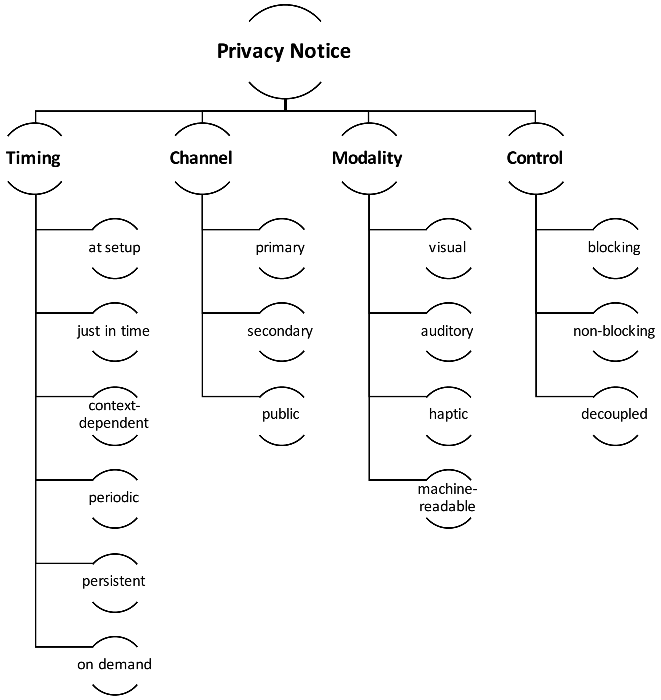


Figure 15: Schaub et al.'s privacy notice design space

policy-driven frameworks [42]. Figure 15 highlights the design space they created. As a result of exploration of this taxonomy, the development of the beacon privacy framework I contribute primarily explores the dimension of Timing, specifically the guidelines related to "At setup" and "Just in time" notifications.

5.2 Framework Overview

5.2.1 Framework Design

Regarding framework implementation, I propose an extension to the current Bluetooth framework in the Android open source architecture by incorporating a middleware layer that manages and enforces beacon privacy policies created by the user. Furthermore, I propose a beacon privacy service that executes as a system service in the Android framework; the beacon privacy service manages and enforces the user's beacon privacy policies. The Android Bluetooth discovery protocol will be extended to monitor beacon discovery and communicate with the beacon privacy service to enable the enforcement of the user beacon privacy policy, depicted in Figure 16.

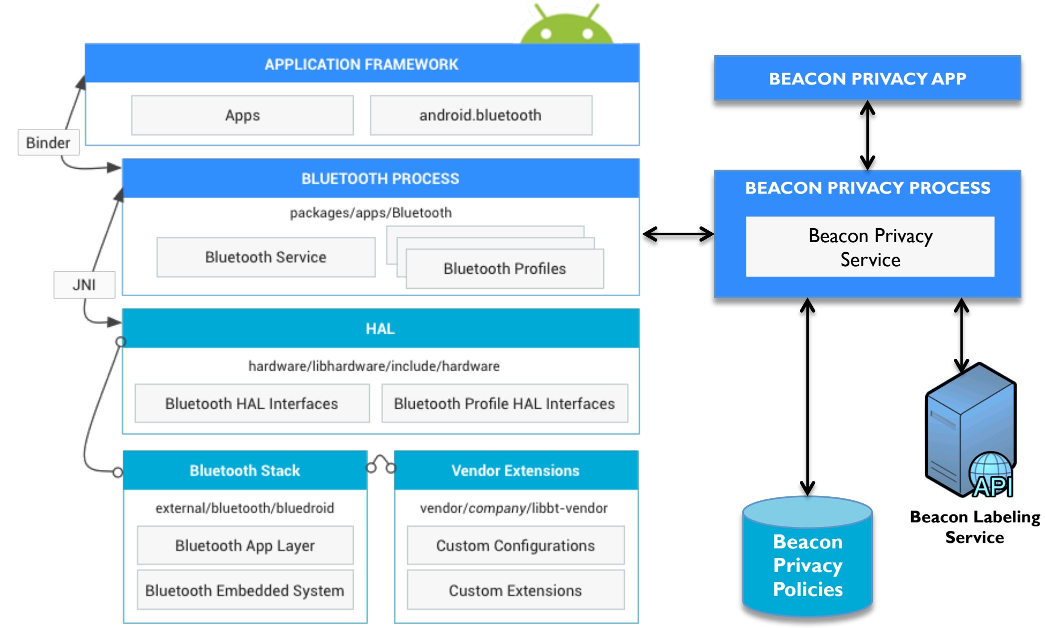


Figure 16: Beacon privacy extension to Bluetooth architecture

The user should be able to setup beacon privacy policies through a mobile app, which communicates with the background service to update and store the beacon privacy policies. Each privacy policy is stored in a device-level or cloud database, accessible only through the privacy process. In addition the privacy process accesses an online database that includes beacon descriptions, which provides information about different beacon encounters. This beacon information can include information about where the beacon is located and the context of the beacon, such as a beacon present in the retail store's mens shoe department.

The beacon privacy application also interacts with the user through the notification and alert dialog framework. For example, when a new beacon is encountered the beacon privacy application will alert the user and will request the user's consent before the beacon encounter information is released to the Bluetooth service. The privacy service acts as a reference monitor, controlling the release of beacon encounter information through the Bluetooth service. For example, if the user decides not to release a specific beacon encounter to the Bluetooth service, then the beacon encounter will be deleted from the beacon discovery stack and will not be made available to other beacon enabled apps on the device.

5.2.2 Framework Policies

A user's privacy preferences with respect to beacon encounters express his willingness to share pieces of information that describe the discovered beacons. Formally, I represent a beacon that a user encounters as b, where $b \in B$, and B is the set of all beacons. In addition, I represent a piece of information related to a beacon encounter as i, where $i \in I$, with I being the set of all beacon encounter information items. Consequently, a user's privacy preferences can be represented in terms of the function $pref : IxB \rightarrow \{allow, deny\}$. If a user specifies a policy $pref(i, b) = allow$, then this means that it is the user's preference to allow information item i to be shared when b is encountered. Figure 17 depicts a typical user's ideal policy set. In this depiction, our example user Alice specifies the policies for all beacons encountered, where the hexagons represent the set of beacons B and the rectangles drawn over the arrows represent the set of policies that capture a user's privacy preferences for each beacon b. Within each rectangle is a letter representing each of the individual elements of a beacon encounter i. Note that the privacy policies vary for each beacon, based on implicit rules and contexts of the beacon encounters; the beacon privacy framework would support this variability.

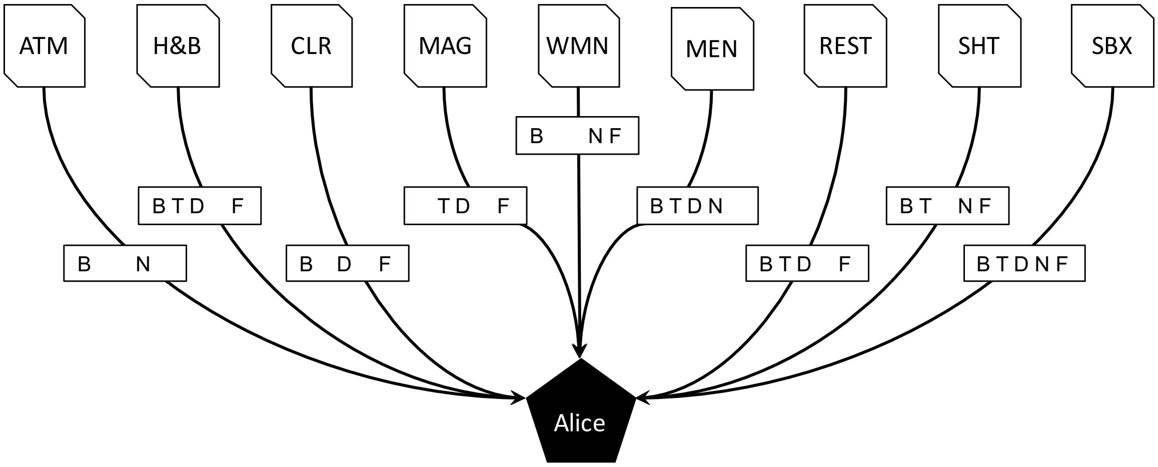


Figure 17: Representation of a user's ideal policy in the beacon privacy framework

The proposed types of supported beacon encounter policies include:

- Simple Beacon Encounter Policy (B): This is a simple policy that enable the user to specify if he would like to opt-in or opt-out of the sharing the beacon ID of a specific encounter.

- Beacon Encounter Time Policy (T): This enables the user to opt-in or opt-out of sharing the timestamp associated with a beacon encounter. For example, a user could decide to share the beacon they encountered, but not what date or time they discovered this beacon.

- Beacon Encounter Duration Policy (D): This policy enables the user to control the length of time for an encounter being reported. For example, the user can limit the reported encounters to a specific time limit, such as sharing the encounters for up to 5 seconds. This enables the user to control the derived activity time by the beacon enabled apps.

- Beacon Encounter Number Policy (N): This enables the user to opt-in or opt-out of sharing the number of times they have encountered a specific beacon. For example, a user may opt to share the fact that they discover a particular beacon a total of 3 times.

- Beacon Encounter Frequency Policy (F): This enable the user to control the reporting of the rate of repeated visits for a specific beacon. For example, the user could opt-out of sharing that they discover a particular beacon at a rate of 3 times a day.

CHAPTER 6: EVALUATION OF THE BEACON PRIVACY FRAMEWORK

The purpose of evaluating the beacon privacy framework was to compare and contrast different styles of a beacon privacy manager, based on the privacy notice design guidelines that informed the established framework. During the design phase, I had planned to build a privacy manager that extended the Android architecture, specifically incorporating a middleware layer that manages the BLE signals received and enforces beacon privacy policies created by the user. After exploring design options, however, I determined a full implementation was not necessary to test its effectiveness, specifically from a user perspective.

Consequently, the prototype that I built did not extend the Android Bluetooth architecture, and any policies created would only have the appearance of being enforced in the study. Instead, the prototype emphasized the user experience involved in interacting with the privacy manager, exploring what kind of policies users created and how they reacted to the provided feedback within the privacy manager. As one instance of the generalized framework, I developed a proof-of-concept Beacon Privacy Manager app, and I evaluated this in an empirical user study, the design of which was influenced by the same principles that inform other common access control and privacy policy configuration solutions.

6.1 Study Design

Participants in the user study were provided a mobile device with the Beacon Privacy Manager (BPM) application installed, which they used to create privacy policy rules regarding the information that could be shared. The study was conducted in the campus Barnes & Noble bookstore, where Estimote [14] beacons were placed in various sections of the bookstore. Figure 18 indicates the sections where beacons were placed, each of which represented one of the following categories: Women's Athletic Apparel, Magazines, Men's Apparel, Shot & Drinking Glasses, Clearance, Health & Beauty, Starbucks, Restrooms, and ATM (Automated Teller Machine). These sections corresponded to the same locations that were used in the crowdsourcing study discussed in Chapter 4. The category and privacy sensitivity labels that were accumulated from this previous study were aggregated and averaged to generate the category and sensitivity rating that participants would see for each beacon encountered. The University IRB approved the protocol to conduct this user study, and approval was also given by the Student Union building managers to deploy beacons in the bookstore.

6.1.1 Recruitment

A combination of random passers-by/visitors to the bookstore, students recruited by emails sent out to the different departments, and word-of-mouth served as methods of recruitment. All participants were at least 18 years or older. The study was advertised as a beacon scavenger hunt game, with a reward in the form of a $10 Amazon gift card for anyone that participated. Each session took an average of 30

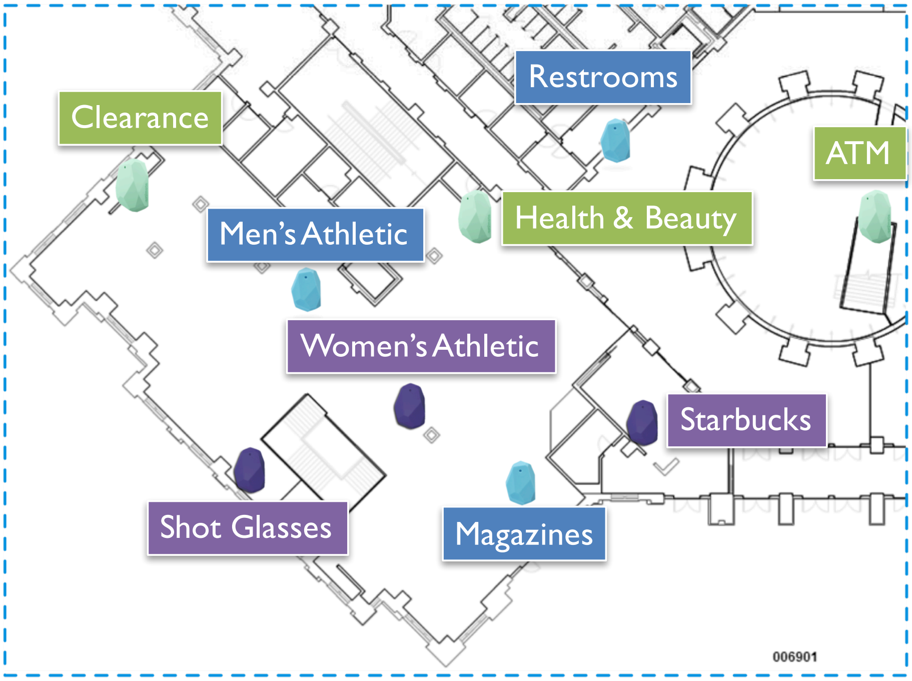


Figure 18: Map of beacon placement in campus bookstore for BPM study

minutes to complete: in addition to performing the main activity of setting policies, this allotted time also included completing a short pre-survey assessing awareness and perception of beacons, receiving a verbal description of the intent of the study and some background information on the beacon technology, and completing the post-survey administered at the end. The study was conducted over a span of one week.

6.1.2 User Study Flow

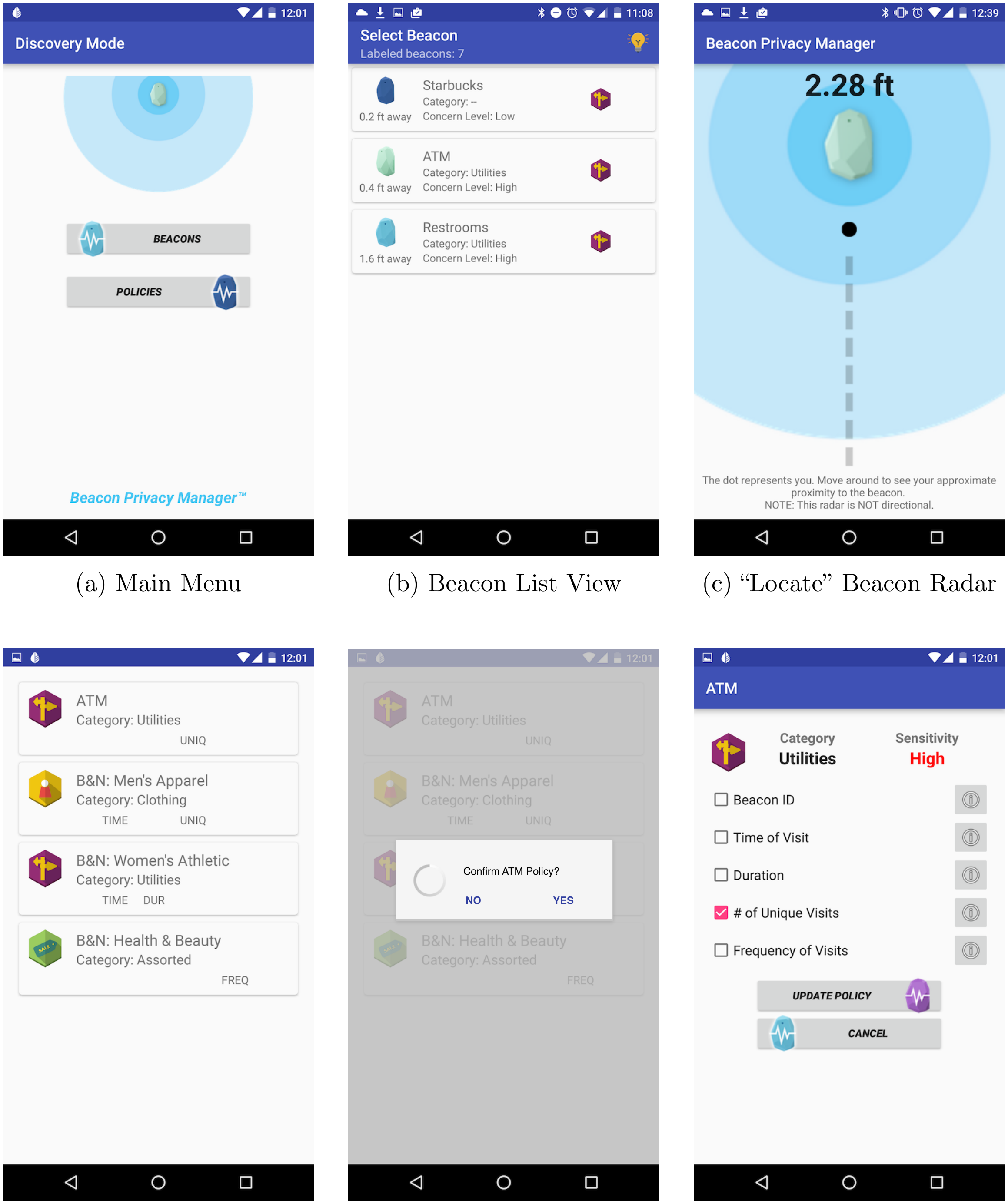
Following the pre-survey, participants clicked through a brief tutorial with accompanying screenshots of the app's main features. Figure 19 highlights the screenshots of the app, which were also displayed to the user during the tutorial. After the tutorial, users were brought to the main menu of the app, as seen in Figure 12a, where they would start the session and either set their beacon policies upfront, or begin exploring the bookstore and setting beacon policies on the fly, depending on their assigned condition. Participants were randomly assigned in round-robin style to one of two conditions in the study. One condition, the “At Setup” group, required users to set all of the privacy policies for the related beacons in the beginning, when the app is first run, before they explored the bookstore. The other condition, the “Just In Time” group, required users to set their beacon policies on the fly, specifically at the moment they actually visited each beacon in the bookstore.

These conditions were inspired by the privacy notice options outlined in the best practices for effective privacy policies [42]. The advantage of “just-in-time” notices is that it gives the user a chance to examine the actual data that would be considered, thereby giving them more immediate context by which to make a privacy decision. However, this convenience has to be balanced by the potential for notice fatigue and annoyance, where prompts to set new policies are displayed too often. Furthermore, some users simply prefer to make their privacy related decisions at “first run” or installation time, yet a disadvantage here is that users may not understand the features or the information in question enough to make a properly informed decision at this stage.

Within the BPM app, the “At Setup” group pressed the Beacons button from the Main Menu screen in order to view a dynamic list of BLE beacons within range of the device, as shown in Figure 19b. These were sorted in order of distance from the user. Selecting a beacon from the list provided two options: “Locate,” which displayed the radar view shown in 19c to help users determine their proximity to an unseen beacon, and “Set Policy,” which displayed the interface shown in Figure 19d. The “Just In

Time" group pressed the Policies button first from within the Main Menu, and selected each beacon one at a time from a list of known beacons. Again, the identities of these beacons are known as a result of the crowdsourced beacon data from the previous study, which is why these could be considered known and therefore associated with a privacy policy in advance. This detail was explained to the participants as part of the study instructions. As policies were created, they would be viewed in a list as seen in Figure 19d. Once policies had been set for all nine beacons, then these users were asked to explore the bookstore. In this way, when they encountered a beacon, a notification would pop up, as seen in Figure 19e, indicating the previously created policy corresponding to this beacon was being enforced. At this point, they had the opportunity to update the policy, making it more open or closed, or leave it the same, based on actual observation of the section for which they had created the beacon policy.

Leveraging the crowdsourced beacon category and sensitivity information, all users would set a privacy policy indicating what they wanted to share for a given beacon. Figure 19d is the view seen by users when creating a policy. The process of configuring privacy policies involved selecting from five options: Beacon ID, Time of Visit, Duration of Visit, Unique Visits, and Frequency of Visits. A more detailed explanation was provided within the app for each item: Beacon ID referred to the "identity and category of the beacon," for example "I am willing to share that I visited the Men's Apparel (Clothing) beacon." The Time of Visit simply referred to "the exact date and time that a particular beacon was visited," i.e. "I am willing to share that I visited a beacon at 12pm on Saturday." Additionally, Duration referred to the "length



(a) Main Menu

Labeled beacons: 7

Starbucks
Category: --
Concern Level: Low
0.2 ft away

ATM
Category: Utilities
Concern Level: High
0.4 ft away

Restrooms
Category: Utilities
Concern Level: High
1.6 ft away

(b) Beacon List View

The dot represents you. Move around to see your approximate proximity to the beacon.
NOTE: This radar is NOT directional.

(c) "Locate" Beacon Radar

ATM
Category: Utilities
UNIQ

B&N: Men's Apparel
Category: Clothing
TIME UNIQ

B&N: Women's Athletic
Category: Utilities
TIME DUR

B&N: Health & Beauty
Category: Assorted
FREQ

(d) Policy List View

Confirm ATM Policy?

(e) Set Policy Notification

Category
Utilities

Sensitivity
High

□ Beacon ID
□ Time of Visit
□ Duration
☑ # of Unique Visits
□ Frequency of Visits

(f) Privacy Policy View

Figure 19: Screenshots of the "BPM" Android app

of time spent within a beacon's zone," while Number of Unique Visits referred to the "total number of beacon encounters"' (each entry/exit of a beacon's region counts as a unique visit), and Frequency of Visits referred to the rate of encounters, or "how often a user visits a given beacon," i.e. "I am willing to share that I visit this beacon at a rate of 5 times a week" or "2 times a day." A user could optionally select one, many, all, or none to share when setting a policy. While in this view, the app kept track of the amount of time taken to create a policy. Users would repeat this process for each beacon they encountered as they explored the bookstore. Should they determine that they had inaccurately set a policy for any beacon, or they wanted to change their responses to the sensitivity-related questions, they simply had to click on the labeled beacon to redo the process. Once all nine beacons had been found and set with a policy, the app would trigger the conclusion of the session and present the user with the option to complete the post-survey.

6.1.3 Post-Survey Flow

The post-survey for this study began with a few questions inquiring about demographic information for the participant, including age, gender, race/ethnicity, education, and technical expertise. This was then followed by a series of questions on their general privacy concern levels. These levels were inspired by Westin's Privacy Segmentation indexes of Pragmatist (balanced, or neutral), Fundamentalist (concerned), and Unconcerned [25]. The next 10 questions regarded the usability of the Beacon Privacy Manager app. These 5-point Likert-scale questions came from the System Usability Scale (SUS), a reliable tool and industry-standard in measuring usability

[3, 9]. They captured items like complexity, consistency, confidence in use, likelihood of reuse, and technical expertise required to use.

Additionally, the post-survey evaluated the users' perceptions of level of control in setting privacy policies, as well as the level of trust in enforcement of privacy policies, respectively, using 5-point Likert-scale questions. Lastly, the survey finished with an open-ended question for any final comments.

6.1.4 Analysis Procedure

The goal of the analysis was to evaluate the merits of a Beacon Privacy Manager that is based on two different types of policy configurations: "At Setup" and "Just in Time." Regarding the use of the BPM app, I considered the measures of policy openness, time efficiency, and trend of policy changes. Given the two groups, I used independent t-tests in order to determine any significant difference in usage. From the post-survey that was administered after use of the app, I was able to learn more about the usability, trust, and control of the privacy manager, again comparing responses between the two groups. These served as artifacts by which I could demonstrate that this approach is both a quantitatively and qualitatively effective implementation. Concerning usability, I used the provided SUS analysis procedure to generate a SUS score and interpret its meaning. For trust and control, I again relied on independent t-tests to determine significant difference. For all statistical tests, the α-value was 0.05.

6.2 Descriptive Results

I analyzed the app usage and survey responses from a total of 90 participants. The demographic breakdown of these participants can be seen in Table 17. Males made up 72.2% of participants and females were the remaining 27.8%. Regarding age, 43.3% were between 18-24, while 53.3% were ages 25-34, and the remaining 3.3% fell between 35-54. Lastly, the main levels of education that users completed included bachelor's degree at 42.2% of participants and graduate degree at 38.9%, while 18.9% completed an Associate's degree or lower.

Table 17: Participants' demographic summary

Gender	%	Age	%	Education	%
Male	72.2	18-24	43.3	High school	6.7
Female	27.8	25-34	53.3	Some college	8.9
		35-64	3.3	Associate	3.3
				Bachelor	42.2
				Graduate	38.9

6.2.1 App Usage

6.2.1.1 Openness of Policies

I define openness of privacy policies to be the amount of beacon encounter-related information that users are willing to share for a given policy, based on the beacon metrics that users marked in the BPM app. For example, if a user marks "Beacon ID" and "Time of Visit" as information that they are willing to share with apps requesting this information about a specific beacon encounter, then their openness for this specific beacon policy is rated 2. These metrics are weighted equally, so with five possible elements of a beacon encounter to mark in a policy, openness can range from 0 (where nothing is marked) to 5 (where everything is marked). If a policy is more open, then that encounter is more transparent, and the user is likely less concerned about preserving their location privacy with regard to visiting that beacon. By averaging the openness of policies created for all beacons, I can evaluate the level of openness, and therefore the level of location privacy concern, for all the study participants. For our between-subjects study, I hypothesized that the two groups would have a significant difference in levels of openness. Here I express this hypothesis as follows:

$$H1_0 : \mu_{O1} = \mu_{O2}$$

$$H1_a : \mu_{O1} \neq \mu_{O2}$$

In the above, $_{O1}$ represents the mean policy openness for the "At Setup" group and $_{O2}$ represents the mean policy openness for the "Just In Time" group. Each time a user created or updated a policy for a given beacon, a new policy record was stored in the database; the latest version of a policy was always flagged as such, in order to determine what the final policy for each beacon for every user. As a result, there were a total of 1301 policy records, but the total number of policies that were considered final for all users was 799. These final policies were used to calculate the mean openness. Table 18 captures the mean policy openness for the two groups, where N is the number of final policies created for users in each group. The "At Setup" group had a mean policy openness of 3.10 while the "Just In Time" group had a mean openness of 2.69.

Table 18: Mean policy openness per condition

Condition	Mean (μ)	St. Dev	N
At Setup	3.10	1.559	405
Just In Time	2.69	1.647	394

In order to compare the mean accuracy for the two groups, I used independent t-tests to compare the means. First checking for homogeneity of variance using Levene's Test for Equality of Variances, I found that our group variances were not equal. Conducting an independent t-test with this in mind, I found that there was a statistically significant difference between the openness for the two groups (t=-3.619, p $<$ .001). Based on this result, I conclude that the users in the "Just In Time" group created policies that were less open, and therefore more privacy-preserving, than the "At Setup" group. This would suggest that the users are more likely to set a more conservative, privacy-preserving policy the first time when making the decision at encounter time, as compared to users who make a decision at setup and then revisit that decision at encounter time.

6.2.1.2 Time Efficiency of Policies

In addition to openness, the Beacon Privacy Manager app measured the amount of time taken by users to create each policy. Unlike with openness, where I only used the final version of policies set for each beacon, here I acknowledged the amount of time taken for every single policy record created, a sum total of 1301 entries. Because the "At Setup" group had to spend time creating an initial policy entry at setup and at least one updated policy entry at encounter time for all beacons, this group created more policies, and I hypothesized that there would be a significant difference in average amount of time spent setting policies between the two groups. Here I express the hypothesis as the following:

$$H2_0 : \mu_{T1} = \mu_{T2}$$

$$H2_a : \mu_{T1} \neq \mu_{T2}$$

In the above, $_{T1}$ represents the mean policy time for the “At Setup” group and $_{T2}$ represents the mean policy time for the “Just In Time” group. Table 19 reflects the mean time for the two groups, where N is the number of beacon policies records captured by the app that was attributed to each group. Since the time measurements are not an unbounded normal variable, I performed a logarithmic transformation on the values to stabilize the variance. As a result, the “At Setup” group had a mean log time of 3.77, while the “Just In Time” group had a mean log time of 3.81.

Table 19: Mean policy time per condition

Condition	Mean (μ)	St. Dev	N
At Setup	3.77	.4165	803
Just In Time	3.81	.4336	498

I then performed an independent t-test to compare the effect of the study condition on time. This revealed no significant difference in time between the two conditions (t = -1.399, p = .162). This means that there is actually no significant difference in average amount of time spent making a privacy decision for each policy.

6.2.1.3 Trend of Policy Changes

While the design of the user study was such that the “At Setup” group had to create initial policies in the beginning and then were prompted to verify or update these policies at beacon encounter time, the users in the “Just In Time” group were also able to update created policies, which in turn could result in a policy change on the spot. Consequently, both groups could make policy changes, and I wanted to compare the trend of policy changes under both conditions. In other words, I wanted to observe whether policy updates trended towards more open or more closed depending on condition, believing that there would be a significant difference between the two groups. I express this hypothesis as such:

$$H3_0 : \mu_{\Delta 1} = \mu_{\Delta 2}$$

$$H3_a : \mu_{\Delta 1} \neq \mu_{\Delta 2}$$

Here, $_{\Delta 1}$ represents the mean openness delta for the “At Setup” group and $_{\Delta 2}$ represents the mean openness delta for the “Just In Time” group. Table 20 reflects the mean delta for the two groups, where N is the number of beacon policies records captured by the app that was attributed to that group. These policy records were a subset of the 1301 total policies records, generated by taking all policies that were flagged as “initial” only and matching these up with the identical policy records that were flagged as “final” only, and calculating the difference in their openness score. Note that this disregards any policy records that were both flagged as “initial” and “final,” as these would indicate policies that were created once and not updated (most certainly generated by users in the “Just In Time”) and therefore would not ever have any openness change. For the “At Setup” group, the mean change in policy openness was .0741, while the “Just In Time” group had a mean change of -.0584.

Table 20: Mean change in policy openness per condition

Condition	Mean (μ)	St. Dev	N
At Setup	.0741	1.076	405
Just In Time	-.0584	.556	394

An independent t-test was conducted in order to determine if condition had any significant effect on the trend of policy openness changes. First checking for homogeneity of variance using Levene's Test for Equality of Variances, I found that our group variances were not equal. The resulting t-test provided a statistically significant difference (t = 2.194, p = .029). The positive mean value of the "At Setup" group indicates that policies updated by this group trended towards being more open, whereas the negative value of the latter indicates the "Just In Time" group, when they happened to update their policies, trended towards more closed policies.

6.2.2 Survey Responses

6.2.2.1 Usability

I used the industry-standard System Usability Scale (SUS) to evaluate the usability of the Beacon Privacy Manager app based on the responses to the corresponding Likert-scale questions. SUS yields a single number representing a composite measure of the overall usability of the system being studied. I note that this score is not a percentage nor diagnostic, but simply an evaluation of an application's ease of use [47]. Based on the formula provided [9], I calculated a SUS score of 77.75, well above the accepted average of 68 for general applications, and 65.9 for cell phone applications. When breaking this down by condition group, the "At Setup" group provided an average SUS score of 77.05, and the "Just In Time" group generated a

SUS score of 78.44. Figure 20 represents the SUS scale for general applications, with a marker indicating how the BknBkts app's score compares. As the figure shows, this lands the BPM app in the 3rd quartile, with a SUS rating between "Good" and "Excellent," therefore providing confidence in the app as a usable implementation of the beacon privacy framework.

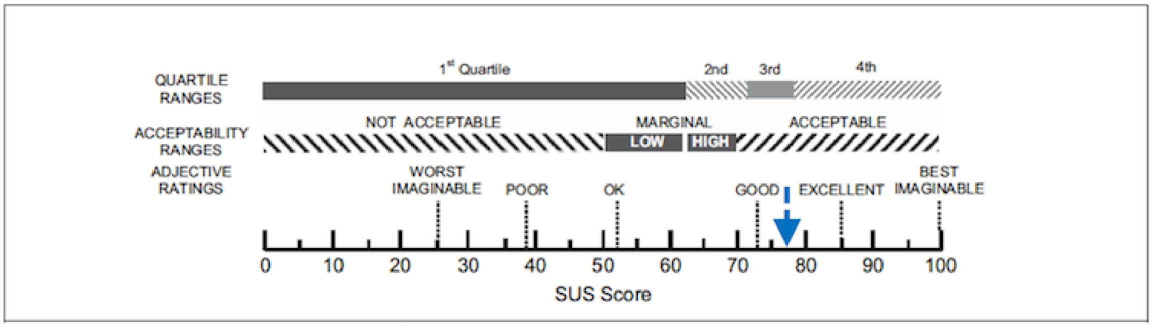


Figure 20: General SUS Scale, with blue arrow indicating BPM's score

6.2.2.2 Trust & Control

I used survey responses to evaluate the level of control users felt they had in setting policies, with regard to what they were able to configure concerning location privacy, as well as the level of trust they had in the fact that policies they set were being enforced. The latter is particularly of interest, considering that in this prototype, there is no feedback demonstrating that policies are being enforced for either condition, other than a view of the list of the policies they created. For both of these variables, I express the hypotheses as follows:

$$H4_0 : \mu_{Tr1} = \mu_{Tr2} \mid\mid H4_a : \mu_{Tr1} \neq \mu_{Tr2}$$

$$H5_0 : \mu_{C1} = \mu_{C2} \mid\mid H5_a : \mu_{C1} \neq \mu_{C2}$$

For $H4$, $_{Tr1}$ represents the mean policy trust level for the "At Setup" group and

$_{Tr2}$ represents the mean policy time for the “Just In Time” group, while for $H5$, $_{C1}$ and $_{C2}$ represent the mean policy control level for the “At Setup” and “Just In Time” groups respectively. The mean trust and control levels for both groups are found in Tables 21 and 22. In both cases, the “At Setup” condition resulted in a higher mean.

Table 21: Mean policy control level per condition

Condition	Mean (μ)	St. Dev	N
At Setup	3.09	.701	45
Just In Time	2.73	.809	45

Table 22: Mean policy trust level per condition

Condition	Mean (μ)	St. Dev	N
At Setup	2.91	.821	45
Just In Time	2.51	.757	45

Running an independent t-test on both sets of means resulted in a statistically significant difference between groups for both policy control (t = 2.228, p = .028) and policy trust (t = 2.402, p = .018). Consequently, this shows that the “At Setup” group felt more control and more trust in enforcement than the “Just In Time” group.

6.3 Discussion

As a result of our studies, I have established that setting and updating beacon policies “Just in Time” leads to more appropriate policies being created. I surmise this to be the result of the immediate visual context of the encounter that is being taken into consideration when policies are created in this manner. This additional information allows users to form a concrete representation of a scenario where they would be willing to share certain information when encountering a given beacon.

This provides enough evidence to make an informed decision immediately. On the other hand, users felt more control and trust when they were able to create policies "At Setup." This could be because this configuration actually encourages multiple opportunities to evaluate a privacy policy, prompting users both at the beginning as well as during an actual encounter of the relevant beacon. While this might be considered extraneous effort, the repetition may act as needed confirmation, helping to reinforce every decision made.

This issue of trust and control may be mitigated as users continue to use a tool like the Beacon Privacy Manager app, allowing them to become more comfortable with the process and therefore more empowered with their data. Furthermore, combining the "just in time" configuration with periodic notices or reminders of set policies can act as nudges that achieve the same feeling of confirmation while ensuring appropriate configuration from the outset. However, it is important to note that with either configuration, there is the risk of annoyance or fatigue that results from repetitive notices. Though it was not observed within the context of this user study, in general this could potentially lead to desensitization over time, which could become a barrier to adoption of the framework overall. This is not a problem unique to this framework, but rather inherent in systems that employ similar notification structures. Solving this issue requires further research, in order to optimize user experience.

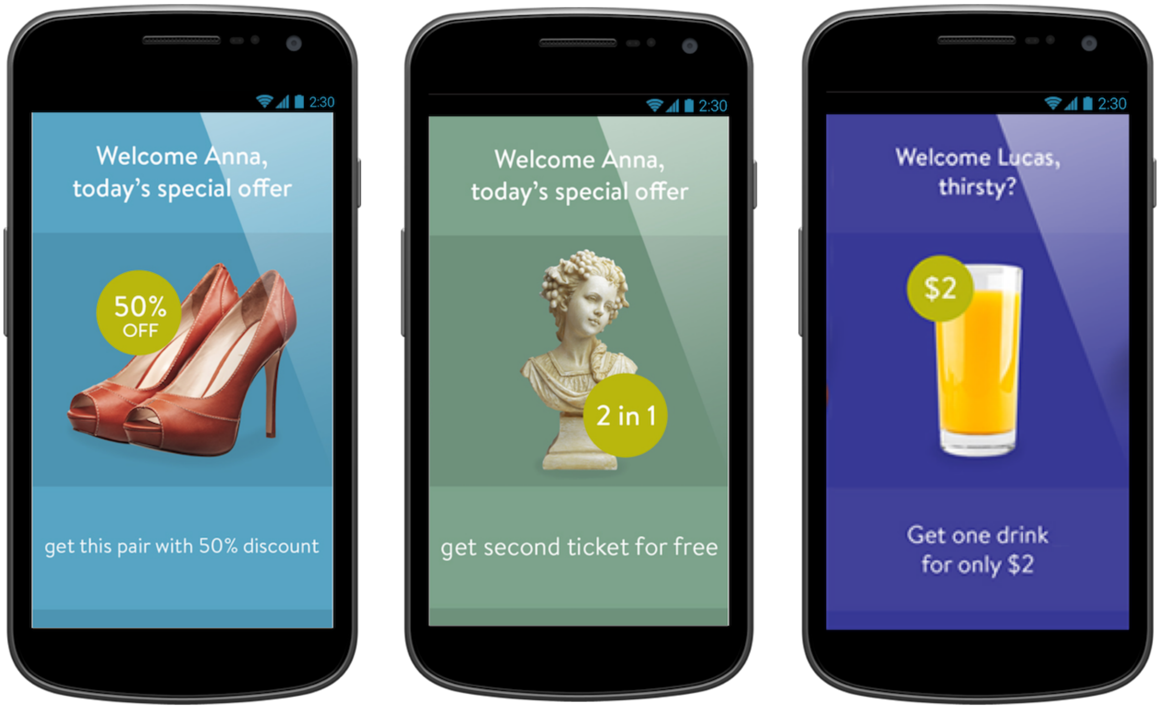
One clear solution to the risk of configuration fatigue, however, would be to automate the process of applying policies by allowing BPM to make recommendations for beacons that are encountered. Fang and LeFevre constructed a similar privacy wizard, based on a framework they proposed for social networking sites [15]. By relying on an active learning paradigm known as uncertainty sampling, this wizard iteratively allowed users to assign privacy labels for selected friends, and then built a classifier which was then used to assign privileges to the remaining unlabeled friends in a user's social networks. Similarly, as a recommender system, the Beacon Privacy Manager could construct a machine learning model to reflect users' privacy policy preferences, and then use this to automatically configure or apply policies.

Another interesting observation from the study results comes from the analysis of trends in policy changes. I noted that participants who set beacon policies "just in time" had a surprising number of policy changes. While this was expected of "at setup" users, this was not a trend we expected from the "just in time" users. The number of changes made by the two groups were very similar (N=405 for "at setup" and 394 for "just in time"), which led me to ponder why these users were compelled to make so many changes to policies. I surmise that this was partly due the study design; by allowing users to set policies for all nine beacons all at once while exploring the bookstore space, it is possible that users felt the need to continually reconfigure policies with each re-encounter of beacons, until all of them had been located and accounted for. Even with this assumption, I acknowledge that being able to know with certainty why users made changes to policies is a limitation in the study; an extension to this work would focus on extrapolating these reasons, either through interviews with users or through additional prompts as users set beacon policies.

6.4 Users as Beacons

In addition to using the Beacon Privacy Manager to investigate the privacy policies that users set when discovering beacons, I also sought to explore another scenario, where users themselves act as beacons. By this I mean that a user's device enters a broadcast state, relying on the peripheral mode of BLE to continuously send a signal representing a small piece of information. Neighboring devices would be able to detect this signal, just as they would from any normal beacon within range. Consider when a consumer walks into a department store, purchases an item, and exits with a bag containing the item in hand. This bag would likely have the name or logo of the store on the bag, and the consumer could therefore be considered a walking advertisement for that store. Translating this scenario to beacon technology, the information that a user would broadcast could be related to the beacon encountered, or perhaps ads for other products related to the ebacon or owning location, thereby broadcasting the discovery to other users. I envision this will become a commonplace use case for BLE beacons, and consequently, I aimed to incorporate this use case as a feature of the BPM app. The goal was to use the same user study in order to measure whether users would exhibit varying levels of information control, including their identity and beacon discovery.

The study design for this "beacon broadcast" experiment was constructed like the "beacon discovery" study previously described: as a between-subjects design, there were two independent conditions, "At setup" and "Just in time." Similar to the broadcast study, these two conditions represented the point in time at which participants



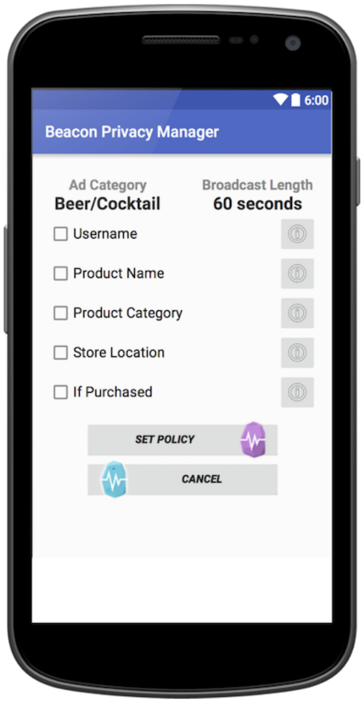
(a) Shoe advertisement (b) Museum advertisement (c) Beer advertisement

Figure 21: Different advertisements displayed to the user as broadcasts

set the policy parameters for the advertisements they were to broadcast. The participants recruited were the same 90 users in the beacon discovery part of the study; they were actually asked to complete this broadcast part of the study immediately after the discovery part, before moving on to the post-survey. Participants were randomly assigned to one of the two conditions; those in the former group were instructed to configure their policies for all advertisements before traveling around the bookstore to broadcast them at predetermined intervals (60 seconds), while the latter group configured their advertisements on the fly. There were three ads for which participants had to configure settings, each in the form of a coupon. Screenshots of these advertisements can be seen in Figure 21; one corresponded to clothing, another to a museum, and the last one to beer/cocktails.

The process of configuring privacy policies for each of the three advertisements involved selecting from five options to broadcast, which can be seen in Figure 22: Username, Product Name, Product Category, Store Location, and If Purchased. Overall, this beacon broadcast study was designed to be more exploratory compared to the beacon discovery part, and therefore its scope was limited, with less emphasis placed on the specific broadcast policies created and more placed on the user comprehension/behavior regarding the overall scenario. In other words, we wanted to convey to the users when and why a store would ask them to act as advertisements on their behalf, in order to drive comprehension when making privacy-preserving policy decisions related broadcasting. Unfortunately, when analyzing the results of app usage for this part of the study, we found that participants were generally open in the advertisement policies, with no statistically significant difference found with respect to the two groups.

While the overall results were non-significant, I conclude that there is still value in having conducted this exercise. The study highlights the disconnect between the real-world scenario of customers acting as advertisements by way of the physical products they purchase/carry around, and this forward-thinking scenario of customers advertising by way of their mobile phones as beacons. This information is useful in recreating the study in a way that matches users' mental models regarding acting as moving advertisements. Still, greater care needs to be taken in furthering this study in order to produce meaningful results. One clear improvement that would need to be made is an expansion of the number of advertisements observed, as well as their variety. It is likely that the provided advertisements were too conservative or



6:00

Beacon Privacy Manager

Ad Category
Beer/Cocktail

Broadcast Length
60 seconds

□ Username

□ Product Name

□ Product Category

□ Store Location

□ If Purchased

SET POLICY

CANCEL

Figure 22: Broadcast policv configuration

similar in category/intent to warrant any concern with respect to users' willingness to broadcast these ads.

Additionally, in a real-world scenario, customers are often compensated for advertising on behalf of a company, in the form of a discount on the product they purchased or a future transaction. Hence, an extension to this particular study would require further exploration into the impact of varying forms of incentives provided to users. This would certainly add to the authenticity of the scenario explored in the study, and it would likely draw out more conclusive results regarding the broadcast policies created. Additional measures that warrant further investigation include the user reactions triggered from broadcasting different ads, as well the impact that ad influence, or number of views by other users, might have on the broadcast policies created. Perhaps the measured influence would motivate users to be more or less open in broadcast policy creation, interacting with the potential impact of any incentive provided. All in all, this study of users as beacons was intended to complement the results found in the beacon discovery study, yet ultimately it serves as a springboard for a tangential yet independent line of future research in the area of BLE beacon privacy management.

6.5 Conclusion

In this chapter, I presented the Beacon Privacy Manager, a tool developed as a prototype and used to implement the framework for beacon privacy management offered in Chapter 5. Through a quantitative and qualitative analysis with 90 users, I evaluated this prototype by providing users with the ability to create privacy policies for beacons, based on crowdsourced information and personal privacy preferences, and compared different methods by which to set these policies. I note that this prototype differs from a real-world implementation of the suggestion framework in a few ways. For example, a full implementation should override the Android Bluetooth protocol in order to intercept BLE broadcasts and enable the enforcement of policies. Furthermore, unlike in the user study, real users would not set policies with the intention of discovering every single beacon in an environment, but simply the ones they had encountered while going about their normal routine. Nonetheless, I made a critical first step towards solving impending beacon privacy management issues. This work was done in response to the need for mechanisms to enable consent of information sharing and privacy management during beacon encounters, which comes largely from the lack of consumer information regarding usage, degree of threat, and control of Bluetooth Low Energy beacons. My research does more than highlight this void, but makes an attempt to fill it, through the development of the framework and evaluation of prototype using real user input, and inspire future researchers to contribute additional solutions.

CHAPTER 7: CONCLUDING REMARKS

In this dissertation, I argued that researchers must begin to take proactive steps towards impending BLE beacon privacy management issues, considering the rapid growth in the use of beacon technology to track users and provide personalized experiences/content. To this end, I sought to enhance user awareness of BLE beacon technology and empower users with tools to control their privacy in beacon-enabled areas. I started on this task by designing and conducting a user study to investigate user awareness of the beacon technology. I found that users did not understand the difference in the underlying BLE protocol, and that participants lacked an awareness of the privacy implications or degree of threat that can result from use of technology. By breaking down a beacon encounter into various attributes, including time, duration, frequency of visits, and travel path, I recognized that privacy concern is a significant factor when it comes to sharing these pieces of information. Furthermore, I also noted in particular that willingness to share beacon encounter information depended on the metric being shared, with less participants willing to share travel path, and most willing to share individual beacon IDs encountered. In light of this, I presented qualitative and quantitative evidence that users do desire fine-grained control of information that is shared.

As a next step, I sought to find a way to make the context of beacon encounters more clear and understandable, so that users can better express when and where they are willing to share each piece of information. By exploring mechanisms to incorporate context into matters involving privacy, I hypothesized that crowdsourcing would be a sufficient method with regard to beacon encounters. Through a separate user study, I confirmed that crowdsourcing allows for users to collectively consider appropriate category and privacy information as they determine what they are willing to share. It proved to be effective, in both accuracy and time efficiency, as well usable, based on a quantitative industry-standard scale and qualitative user feedback. Equally important, I revealed that context when provided by the crowd is trusted as much as when generated by retailers or beacon providers. All this demonstrated the feasibility of crowdsourcing and reinforced it as a critical component of my approach to beacon privacy, where information disclosure is both user-driven and context-based.

My dissertation research culminated in the development of a beacon privacy management framework, which offered guidelines for creating and supporting privacy policies related to beacon encounters. Furthermore, I implemented a proof-of-concept in order to put such technology in the hands of actual users and derive meaningful feedback. Users created policies for beacons encountered, leveraging the crowdsourced information from the previous study to make informed privacy decisions. I found that users created more conservative policies when done “just in time,” demonstrating a greater level of conservativeness in configuration than policies initially created “at setup.” On the other hand, I found that users felt more control and trust with the latter setup option, likely due to confirmation of each policy created, which would suggest a hybrid solution would improve the ability of wider adoption.

I believe there exists a balance between the privacy of users and the social and economic value of users' beacon encounter data. Through my research, I have investigated a new model for beacon platforms regarding privacy management, and have done so in the interest of fostering that balance while encouraging early recognition of impending privacy concerns. Regarding this objective, no such tools exist for users yet, nor is there any framework for researchers to create said tools. My research aims to fill that gap, and the completed work presented here is a pivotal first step towards that goal. It is my hope that through the findings and proposed extensions presented here, other researchers in the community can have a greater understanding of how users interact with BLE beacons in the context of privacy. With this knowledge, they can continue to explore more advanced privacy management methods and build out the beacon ecosystem with relevant privacy enhancing tools for users.

REFERENCES

[1] Y. Agarwal and M. Hall. Protectmyprivacy: detecting and mitigating privacy leaks on ios devices using crowdsourcing. In *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*, pages 97–110. ACM, 2013.

[2] D. P. Anderson, J. Cobb, E. Korpela, M. Lebofsky, and D. Werthimer. Seti@ home: an experiment in public-resource computing. *Communications of the ACM*, 45(11):56–61, 2002.

[3] A. Bangor, P. Kortum, and J. Miller. Determining what individual sus scores mean: Adding an adjective rating scale. *Journal of usability studies*, 4(3):114–123, 2009.

[4] J. Bernstein, J. Singer-Vine, and S. Ryley. Exclusive: Hundreds of devices hidden inside new york city phone booths, 2014. http://www.buzzfeed.com/josephbernstein/exclusive-hundreds-of-devices-hidden-inside-new-york-city-ph.

[5] A. Besmer, H. R. Lipford, M. Shehab, and G. Cheek. Social applications: exploring a more secure framework. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, page 2. ACM, 2009.

[6] A. Besmer, J. Watson, and H. R. Lipford. The impact of social navigation on privacy policy configuration. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, page 7. ACM, 2010.

[7] M. Bourimi, G. Mau, S. Steinmann, D. Klein, S. Templin, D. Kesdogan, and H. Schramm-Klein. A privacy-respecting indoor localization approach for identifying shopper paths by using end-users mobile devices. In *Information Technology: New Generations (ITNG), 2011 Eighth International Conference on*, pages 139–144. IEEE, 2011.

[8] D. C. Brabham. Moving the crowd at threadless: Motivations for participation in a crowdsourcing application. *Information, Communication & Society*, 13(8):1122–1145, 2010.

[9] J. Brooke. Sus-a quick and dirty usability scale. *Usability evaluation in industry*, 189(194):4–7, 1996.

[10] M. Buhrmester, T. Kwang, and S. D. Gosling. Amazon's mechanical turk a new source of inexpensive, yet high-quality, data? *Perspectives on psychological science*, 6(1):3–5, 2011.

[11] I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani. Crowdroid: behavior-based malware detection system for android. In *Proceedings of the 1st ACM workshop*

on Security and privacy in smartphones and mobile devices, pages 15–26. ACM, 2011.

[12] C.-Y. Chow and M. F. Mokbel. Trajectory privacy in location-based services and data publication. *ACM SIGKDD Explorations Newsletter*, 13(1):19–29, 2011.

[13] S. Egelman, J. Tsai, L. F. Cranor, and A. Acquisti. Timing is everything?: the effects of timing and placement of online privacy indicators. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 319–328. ACM, 2009.

[14] Estimote. Estimote beacons, 2015. http://estimote.com/.

[15] L. Fang and K. LeFevre. Privacy wizards for social networking sites. In *Proceedings of the 19th international conference on World wide web*, pages 351–360. ACM, 2010.

[16] N. Gagliordi. Macy's rolls out retail's largest beacon installation, 2014. http://www.zdnet.com/article/macys-rolls-out-retails-largest-beacon-installation/.

[17] Gartner. Gartner says 4.9 billion connected "things" will be in use in 2015, 2014. http://www.gartner.com/newsroom/id/2905717.

[18] C. Goodwin. A conceptualization of motives to seek privacy for nondeviant consumption. *Journal of Consumer Psychology*, 1(3):261–284, 1992.

[19] G. Grumen. What you need to know about using bluetooth beacons, 2014. http://www.infoworld.com/article/2608498/mobile-apps/what-you-need-to-know-about-using-bluetooth-beacons.html.

[20] V. Ha, K. Inkpen, F. Al Shaar, and L. Hdeib. An examination of user perception and misconception of internet cookies. In *CHI'06 Extended Abstracts on Human Factors in Computing Systems*, pages 833–838. ACM, 2006.

[21] J. I. Hong and J. A. Landay. An architecture for privacy-sensitive ubiquitous computing. In *Proceedings of the 2nd international conference on Mobile systems, applications, and services*, pages 177–189. ACM, 2004.

[22] J. Howe. The rise of crowdsourcing. *Wired magazine*, 14(6):1–4, 2006.

[23] T. Jiang, H. J. Wang, and Y.-C. Hu. Preserving location privacy in wireless lans. In *Proceedings of the 5th international conference on Mobile systems, applications and services*, pages 246–257. ACM, 2007.

[24] R. Kerr. Are ibeacons cookies for the physical web?, 2015. http://mobiletoolworks.com/are-ibeacons-cookies-for-the-physical-web/.

[25] P. Kumaraguru and L. F. Cranor. Privacy indexes: a survey of westin's studies. 2005.

[26] P. G. Leon, B. Ur, Y. Wang, M. Sleeper, R. Balebako, R. Shay, L. Bauer, M. Christodorescu, and L. F. Cranor. What matters to users?: factors that affect users' willingness to share information with online advertisers. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, page 7. ACM, 2013.

[27] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran. Swing & swap: user-centric approaches towards maximizing location privacy. In *Proceedings of the 5th ACM workshop on Privacy in electronic society*, pages 19–28. ACM, 2006.

[28] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, pages 501–510. ACM, 2012.

[29] J. Lin, G. Xiang, J. I. Hong, and N. Sadeh. Modeling people's place naming preferences in location sharing. In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing*, UbiComp '10, pages 75–84, New York, NY, USA, 2010. ACM.

[30] H. R. Lipford, J. Watson, M. Whitney, K. Froiland, and R. W. Reeder. Visual vs. compact: A comparison of privacy policy interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1111–1114. ACM, 2010.

[31] B. Liu, J. Lin, and N. Sadeh. Reconciling mobile app privacy and usability on smartphones: could user privacy profiles help? In *Proceedings of the 23rd international conference on World wide web*, pages 201–212. ACM, 2014.

[32] T. W. Malone, R. Laubacher, and C. Dellarocas. The collective intelligence genome. *IEEE Engineering Management Review*, 38(3):38, 2010.

[33] A. M. McDonald. Cookie confusion: do browser interfaces undermine understanding? In *CHI'10 Extended Abstracts on Human Factors in Computing Systems*, pages 4393–4398. ACM, 2010.

[34] A. D. Miyazaki. Online privacy and the disclosure of cookie use: Effects on consumer trust and anticipated patronage. *Journal of Public Policy & Marketing*, 27(1):19–33, 2008.

[35] G. Myles, A. Friday, and N. Davies. Preserving privacy in environments with location-based applications. *IEEE Pervasive Computing*, 2(1):56–64, 2003.

[36] H. Nissenbaum. Privacy as contextual integrity. *Washington law review*, 79(1), 2004.

[37] N. Ozer, C. Conley, D. H. O'Connell, T. R. Gubins, and E. Ginsburg. Location-based services: time for a privacy check-in. *ACLU of Northern California*, 2010.

[38] T. Pick. 21 vital mobile marketing facts and statistics for 2014, 2014. http://www.business2community.com/mobile-apps/21-vital-mobile-marketing-facts-statistics-2014-0850425.

[39] C. Riederer, V. Erramilli, A. Chaintreau, B. Krishnamurthy, and P. Rodriguez. For sale: your data: by: you. In *Proceedings of the 10th ACM WORKSHOP on Hot Topics in Networks*, page 13. ACM, 2011.

[40] J. L. B. L. N. Sadeh and J. I. Hong. Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings. In *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[41] N. Sadeh, A. Acquisti, T. D. Breaux, L. F. Cranor, A. M. McDonalda, J. R. Reidenbergb, N. A. Smith, F. Liu, N. C. Russellb, F. Schaub, et al. The usable privacy policy project. Technical report, Tech. report CMU-ISR-13-119, Carnegie Mellon University, 2013.

[42] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor. A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 1–17, 2015.

[43] B. SIG. Are ibeacons cookies for the physical web?, 2015. http://www.bluetooth.com/Pages/Consumer-Electronics-Market.aspx.

[44] M. Spreitzer and M. Theimer. *Providing location information in a ubiquitous computing environment (panel session)*, volume 27. ACM, 1994.

[45] E. Toch, J. Cranshaw, P. H. Drielsma, J. Y. Tsai, P. G. Kelley, J. Springfield, L. Cranor, J. Hong, and N. Sadeh. Empirical models of privacy in location sharing. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*, pages 129–138. ACM, 2010.

[46] D. Tynan. What are bluetooth beacons, and why are they following you?, 2014. https://www.yahoo.com/tech/what-are-bluetooth-beacons-and-why-are-they-following-99522970424.html.

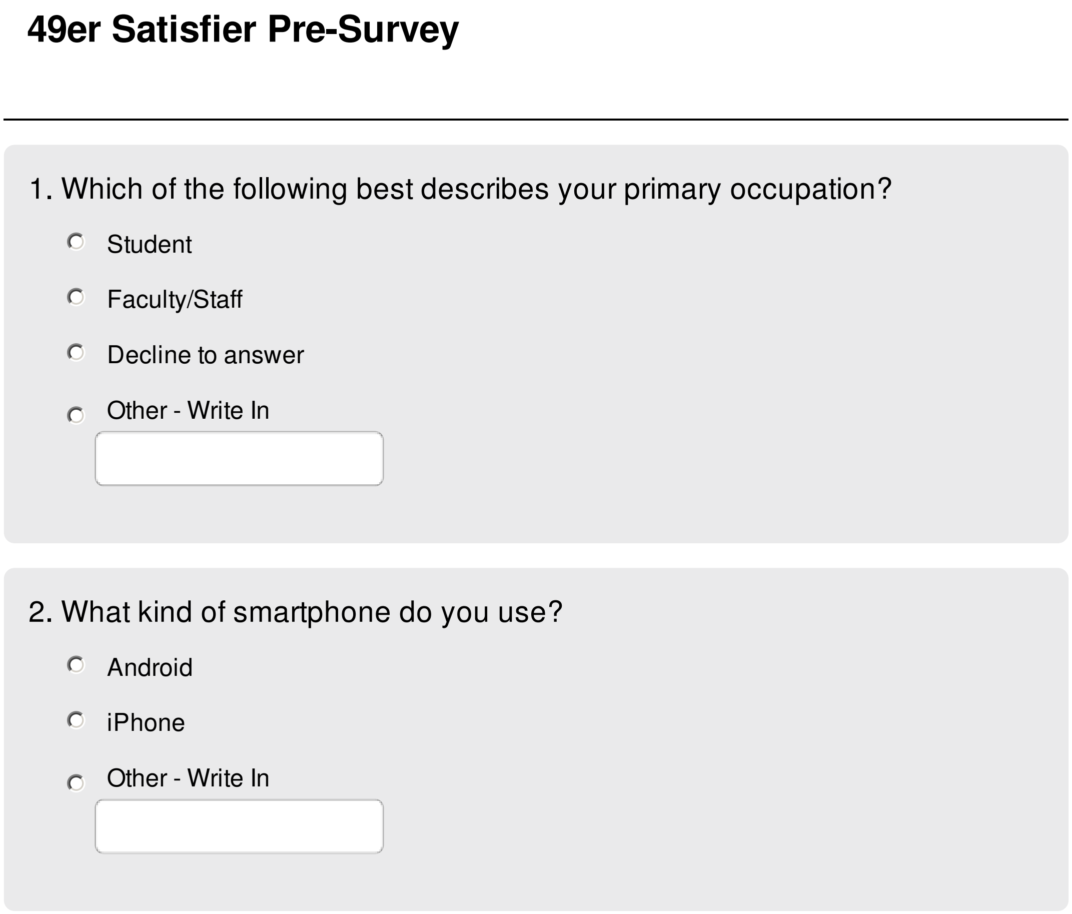
[47] usability.gov. System usability scale, 2015. http://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html.

[48] L. Von Ahn. Games with a purpose. *Computer*, 39(6):92–94, 2006.

[49] J. Voss. Measuring wikipedia. 2005.

[50] S. Zhong, L. Li, Y. G. Liu, and Y. R. Yang. Privacy-preserving location-based services for mobile users in wireless networks. *Department of Computer Science, Yale University, Technical Report ALEU/DCS/TR-1297*, 2004.

APPENDIX A: 49ER SATISFIER USER STUDY PRE SURVEY



49er Satisfier Pre-Survey

1. Which of the following best describes your primary occupation?

○ Student

○ Faculty/Staff

○ Decline to answer

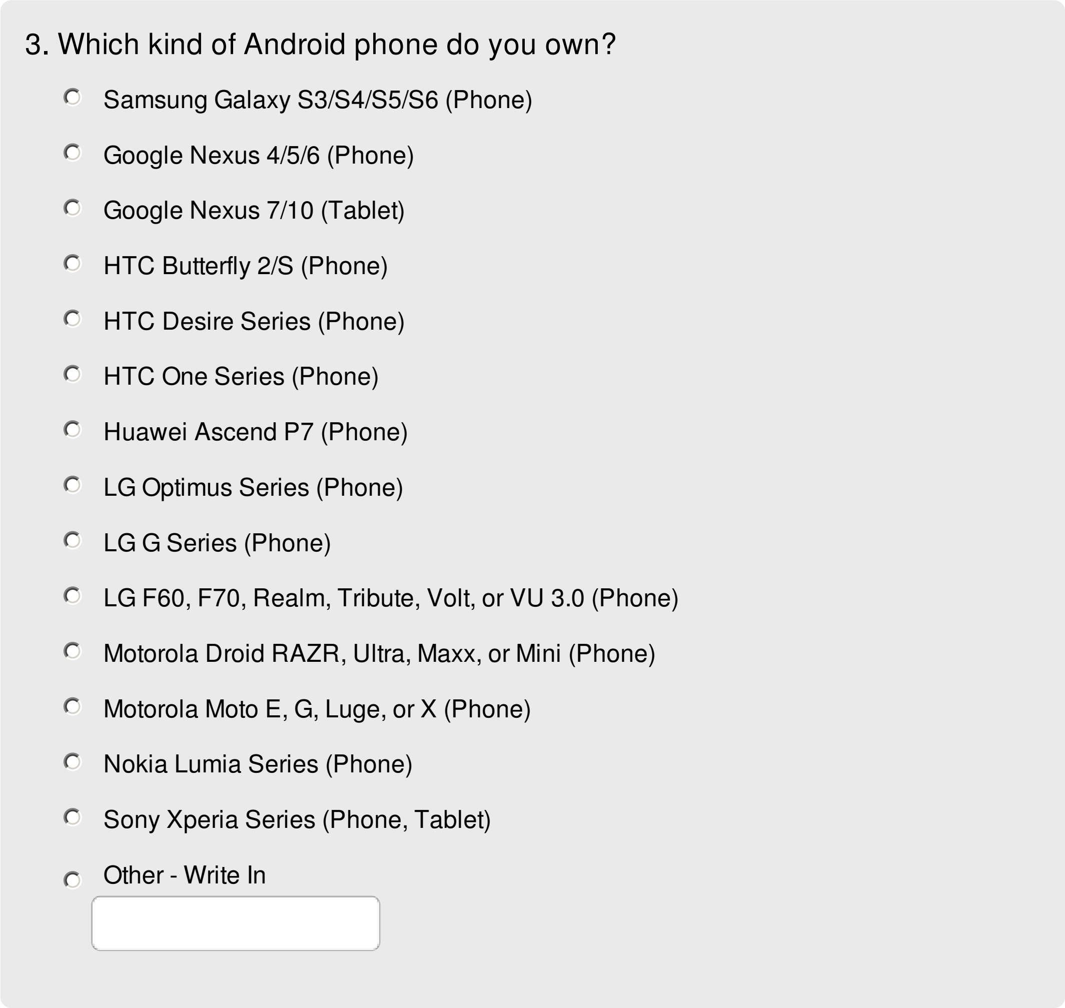
○ Other - Write In

2. What kind of smartphone do you use?

○ Android

○ iPhone

○ Other - Write In



3. Which kind of Android phone do you own?

○ Samsung Galaxy S3/S4/S5/S6 (Phone)

○ Google Nexus 4/5/6 (Phone)

○ Google Nexus 7/10 (Tablet)

○ HTC Butterfly 2/S (Phone)

○ HTC Desire Series (Phone)

○ HTC One Series (Phone)

○ Huawei Ascend P7 (Phone)

○ LG Optimus Series (Phone)

○ LG G Series (Phone)

○ LG F60, F70, Realm, Tribute, Volt, or VU 3.0 (Phone)

○ Motorola Droid RAZR, Ultra, Maxx, or Mini (Phone)

○ Motorola Moto E, G, Luge, or X (Phone)

○ Nokia Lumia Series (Phone)

○ Sony Xperia Series (Phone, Tablet)

○ Other - Write In

4. What version of Android is on your device? (Go to Settings > About Phone > Android version.)

○ Lollipop (5.0-5.1)

○ KitKat (4.4)

○ Jellybean (4.3)

○ Jellybean (4.2) or below

○ Other - Write In

5. What kind of iOS device do you own?

○ Apple iPad Tablet (Air, Mini, 3rd & 4th gen)

○ Apple iPad Tablet (1st or 2nd generation)

○ Apple iPhone (6 Plus, 6, 5s, 5c, 5 & 4s)

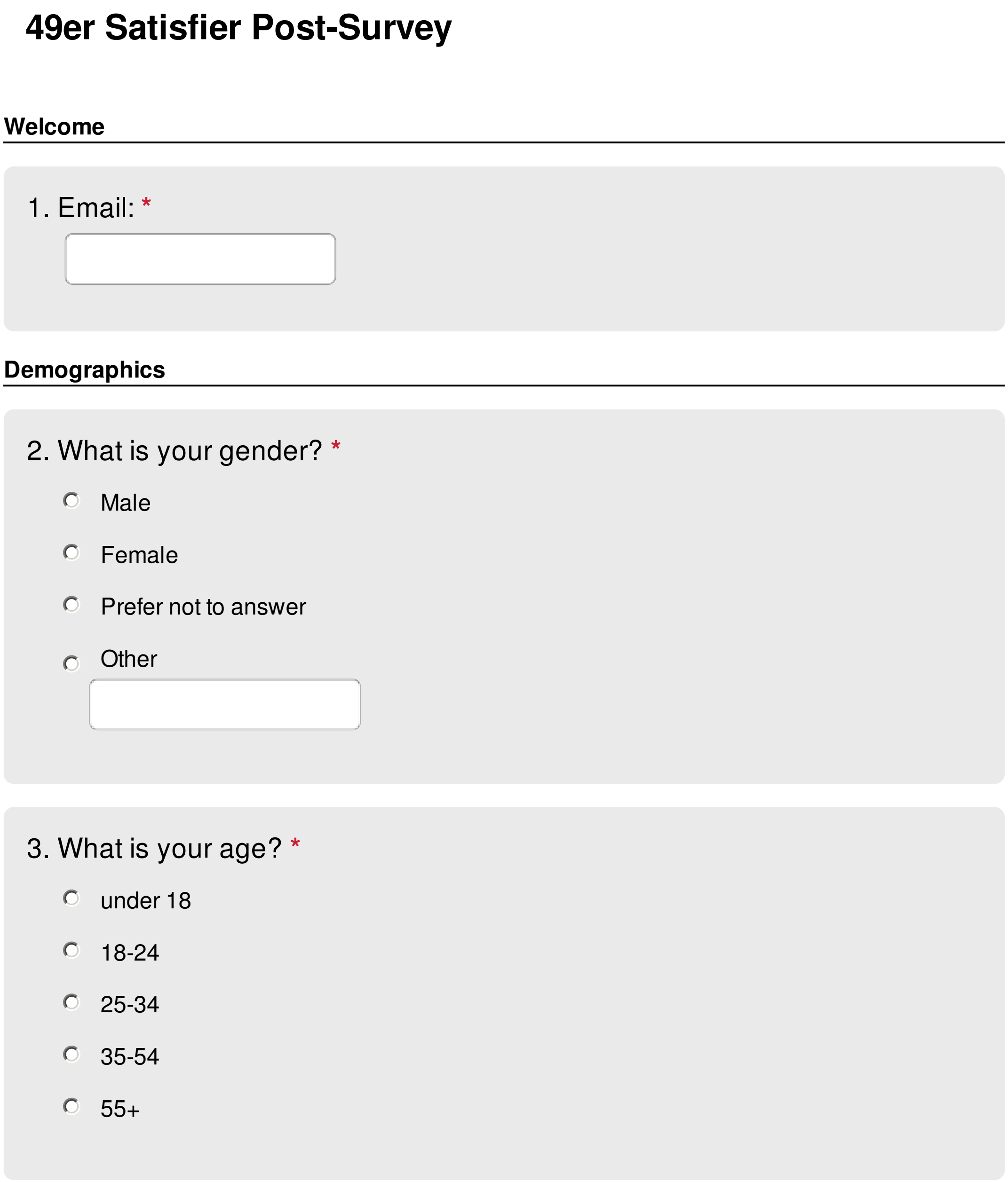
○ Apple iPhone (4 and below)

○ Apple iPod touch (5th generation)

○ Apple iPod touch (4th generation and below)

○ Other - Write In

APPENDIX B: 49ER SATISFIER USER STUDY POST SURVEY



49er Satisfier Post-Survey

Welcome

1. Email: *

Demographics

2. What is your gender? *

○ Male

○ Female

○ Prefer not to answer

○ Other

3. What is your age? *

○ under 18

○ 18-24

○ 25-34

○ 35-54

○ 55+

4. Which of the following best describes your highest achieved level of education? *

12th grade or less
Graduated high school or equivalent
Some college, no degree
Associate degree
Bachelor's degree
Post-graduate degree

5. Which of the following best describes your primary occupation? *

○ Student

○ Employed

○ Unemployed

○ Prefer not to answer

○ Other

Technical Expertise

6. Do you have a college degree or work experience in computer science, software development, mobile app development, web development or similar computer-related fields? *

○ Yes

○ No

7. How often do you spend time on the Internet each day? *

○ Never

○ A few times per month or less

○ Once per week

○ Several times per week

○ Once per day

○ Several times per day

8. Approximately how often do you use Facebook, Instagram, or other social media apps on your smartphone? *

○ Never

○ A few times per month or less

○ Once per week

○ Several times per week

○ Once per day

○ Several times per day

9. Have you ever done the following? (Select all that apply) *

- □ Purchased a product or service online using your mobile phone (e.g., music, books, clothing, etc.)
- □ Used a social networking app (e.g., Facebook, Twitter, LinkedIn, MySpace, etc.)
- □ Clicked on an ad that appeared in an app to get more information about the advertised product
- □ Accidentally clicked on an ad that appeared in an app
- □ Used health, wellness, or medical information apps (e.g., MayoClinic, MyFitnessPal, Men's Health, etc.)
- □ Used retail apps (e.g. Starbucks, Macy’s, Best Buy, etc.)
- □ None of the above

10. Have you ever done the following? *

	Yes	No
Refused to give information to an app because you felt it was too personal or unnecessary	○	○
Decided not to download an app or not to purchase something using an app because you were not sure how your personal information would be used	○	○
Read an app's privacy policy	○	○
Cleared the cache of an app on your phone	○	○

11. How much do you agree or disagree with the following statements: *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
When websites ask for personal information, I usually think twice about providing it	○	○	○	○	○
Consumers have lost all control over how personal information is collected and used by companies	○	○	○	○	○
I feel that as a result of my visiting websites, others know more about me than I am comfortable with	○	○	○	○	○

Awareness of Bluetooth Beacons

12. This user study you participated in employed the use of Bluetooth Low Energy (BLE) beacons. How familiar are you with Bluetooth Low Energy (BLE), or "Bluetooth Smart"? *

Very Unfamiliar	Unfamiliar	Unsure	Familiar	Very Familiar
○	○	○	○	○

13. How familiar are you with BLE beacons? *

Very Unfamiliar	Unfamiliar	Unsure	Familiar	Very Familiar
○	○	○	○	○

14. How much do you agree or disagree with the following? *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Bluetooth beacons are necessary to enjoy free mobile apps.	○	○	○	○	○
I find beacons useful.	○	○	○	○	○
I find beacons to be relevant to my interests/activities.	○	○	○	○	○
I find beacons to be safe and secure.	○	○	○	○	○
I find beacon technology pointless.	○	○	○	○	○
I find beacons to be intrusive on my interests/activities.	○	○	○	○	○
I find beacons to be a threat to my privacy and security.	○	○	○	○	○

15. (Optional) In a few sentences, tell us what you know about Bluetooth, and Bluetooth Low Energy. What do you know about each? How do they relate/compare?

16. (Optional) Briefly tell us what you know about **beacons**. What is your past experience with them, if any?

Awareness of Tracking Technology

17. We are interested in understanding how you experience things online, particularly concerning "**in-app advertising.**" Here, "in-app advertising" refers to ads that are displayed within the mobile apps you use.

How much do you agree or disagree with the following? *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
In-app advertising is necessary to enjoy free mobile apps.	○	○	○	○	○
I find in-app advertising useful.	○	○	○	○	○
I find in-app advertising to be relevant to my interests/activities.	○	○	○	○	○
I find in-app advertising to be safe and secure.	○	○	○	○	○
I find in-app advertising to be unnecessary.	○	○	○	○	○
I find in-app advertising distracting.	○	○	○	○	○
I find in-app advertising to be a threat to my online privacy and security.	○	○	○	○	○
I usually don't look at the ads that appear in the apps I use.	○	○	○	○	○

18. (Optional) In a few sentences, please tell us what you know, and what you think about in-app advertising?

19. **"Browser cookies"** refers to small pieces of information that web browser use to track your online location. Online ads often rely on these cookies to provide ads based on site you visit on your mobile device or computer.

How much do you agree or disagree with the following? *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Browser cookies are necessary to enjoy web browsing.	○	○	○	○	○
I find browser cookies useful.	○	○	○	○	○
I find browser cookies to be relevant to my interests/activities.	○	○	○	○	○
I find browser cookies to be safe and secure.	○	○	○	○	○
I find browser cookies to be pointless.	○	○	○	○	○
I find browser cookies to be irrelevant to my browsing.	○	○	○	○	○
I find browser cookies to be a threat to my online privacy and security.	○	○	○	○	○
I usually don't notice the use of browser cookies in the sites I visit.	○	○	○	○	○

20. (Optional) In a few sentences, please tell us what you know, and what you think about browser cookies?

Awareness of Tracking Technology (cont'd)

21. **"Geotracking"** refers to the use of GPS in mobile apps to monitor your physical location while providing provide location-based services.

How much do you agree or disagree with the following? *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Geotracking is necessary to enjoy most free mobile apps.	○	○	○	○	○
I find geotracking useful.	○	○	○	○	○
I find geotracking to be relevant to my interests/activities.	○	○	○	○	○
I find geotracking to be safe and secure.	○	○	○	○	○
I find geotracking to be pointless.	○	○	○	○	○
I find geotracking distracting.	○	○	○	○	○
I find geotracking to be a threat to my online privacy and security.	○	○	○	○	○
I usually don't notice the use of geotracking in the apps I use.	○	○	○	○	○

22. (Optional) In a few sentences, please tell us what you know, and what you think about geotracking?

23. We are also interested in understanding how you experience things "offline," particularly concerning "**surveillance cameras.**" Here, "surveillance cameras" refers to the video cameras that are in place to monitor people. Many businesses have them installed for security purposes.

How much do you agree or disagree with the following? *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Surveillance cameras are a necessary tool in many locations.	○	○	○	○	○
I find surveillance cameras useful.	○	○	○	○	○
I find surveillance cameras to be relevant to my interests/activities.	○	○	○	○	○
I find surveillance cameras to be safe and secure.	○	○	○	○	○
I find surveillance cameras to be pointless.	○	○	○	○	○
I find surveillance cameras distracting.	○	○	○	○	○
I find surveillance cameras to be a threat to my privacy and security.	○	○	○	○	○
I usually don't notice the use of surveillance cameras in the locations I visit.	○	○	○	○	○

24. (Optional) In a few sentences, please tell us what you know, and what you think about surveillance cameras?

User Study

25. Based on the information that you just read, which of the following are examples of the types of information you think can be collected from your beacon encounters? (Choose any that apply) *

- □ The time you entered the location
- □ The length of time you spent at the location
- □ How many times you visit the location
- □ What path you took as you walked around the location
- □ What you were wearing during your visit to the location
- □ What you said while you were inside the location

26. Based on **your assigned user study scenario** (open the 49erSatisfier app and click "User Study Details" under the Main Menu to refer to the scenario details), for who will your information be collected? *

- ○ University only
- ○ University and other 3rd party retailers

27. Based on **your assigned user study scenario** (open the 49erSatisfier app and click "User Study Details" under the Main Menu to refer to the scenario details), how long may the participating locations use the information collected about you? *

○ One day

○ One week

○ One year

○ Indefinitely

28. Based on **your assigned user study scenario** (open the 49erSatisfier app and click "User Study Details" under the Main Menu to refer to the scenario details), can this information about you be collected WITH or WITHOUT your consent? *

○ With consent only

○ Without consent

User Study (cont'd)

29. I would be willing to allow the locations to use and store the following information about my mobile device. *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The type of operating system (e.g., Android, iOS, etc.) of my mobile device	○	○	○	○	○
The IP address of my mobile device (i.e., a identifier assigned by your Internet service provider)	○	○	○	○	○
The name and version of my device (e.g., Google Nexus 5, Samsung Galaxy S5, etc.)	○	○	○	○	○
The cell carrier of my device (e.g., T-Mobile, AT&T, Verizon, etc.)	○	○	○	○	○

30. I would be willing to allow the locations to use and store the following demographic and preference information. *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
My gender	○	○	○	○	○
My highest level of education	○	○	○	○	○
My income bracket	○	○	○	○	○
My religion	○	○	○	○	○
My political preferences	○	○	○	○	○
My sexual orientation	○	○	○	○	○
My marital status	○	○	○	○	○
My hobbies	○	○	○	○	○
My credit score bracket	○	○	○	○	○

31. I would be willing to allow the locations to use and store the following information related to my interactions with the beacons in their space. *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The beacons I encounter	○	○	○	○	○
The time I visited/encountered a beacon	○	○	○	○	○
Duration of a beacon visit	○	○	○	○	○
Number of unique visits to a beacon	○	○	○	○	○
Frequency of visits to a beacon	○	○	○	○	○
The path I took around these beacons	○	○	○	○	○

32. I would be willing to allow the businesses to use and store the following information related to my present location. *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Current country	○	○	○	○	○
Current state	○	○	○	○	○
Current city	○	○	○	○	○
Current zip code	○	○	○	○	○

33. I would be willing to allow the locations to collect the following information. *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
My name	○	○	○	○	○
My email address	○	○	○	○	○
My phone number	○	○	○	○	○
My address	○	○	○	○	○
My social security number	○	○	○	○	○
My credit card number	○	○	○	○	○

34. How would your willingness to allow locations to collect your information change if it retained your information for the following length of time: *

	I would be less willing	No difference	I would be more willing
only for the duration of a single visit	○	○	○
for one day	○	○	○
for one week	○	○	○
for one month	○	○	○
for six months	○	○	○
for one year	○	○	○
indefinitely	○	○	○

35. How would your willingness to allow locations to collect your information change, if you could review, edit, and delete the information that is being collected? *

○ I would less willing

○ No difference

○ I would more willing

User Study (cont'd)

36. Imagine that you are offered an incentive in exchange for your beacon encounter information, which **will NOT be used to show you any ads, but may still be used for other purposes (like marketing).**

How much do you agree or disagree with the following as motivating incentives? *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Monetary (cash) rewards	○	○	○	○	○
Coupons/Discounts directly related to the item(s) near the encountered beacon	○	○	○	○	○
Coupons/Discounts NOT directly related to the items near the encountered beacon	○	○	○	○	○
Game Points/Badges	○	○	○	○	○

37. Imagine that you are offered an incentive in exchange for your beacon encounter information, which **WILL be used to show you <u>general ads</u>, but NOT <u>targeted ads</u>.**

How much do you agree or disagree with the following as motivating incentives? *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Monetary (cash) rewards	○	○	○	○	○
Coupons/Discounts directly related to the item(s) near the encountered beacon	○	○	○	○	○
Coupons/Discounts NOT directly related to the item(s) near the encountered beacon	○	○	○	○	○
Game Points/Badges	○	○	○	○	○

38. Imagine that you are offered an incentive in exchange for your beacon encounter information, which **WILL be used to show you <u>targeted ads</u>.**

How much do you agree or disagree with the following as motivating incentives? *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Monetary (cash) incentives	○	○	○	○	○
Coupons/Discounts directly related to the item(s) near the encountered beacon	○	○	○	○	○
Coupons/Discounts NOT directly related to the item(s) near the encountered beacon	○	○	○	○	○
Game Points/Badges	○	○	○	○	○

39. How much do you agree or disagree with the following statement:
I am interested in receiving targeted ads on a mobile app based on beacon encounters for the following: *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
health apps	○	○	○	○	○
banking apps	○	○	○	○	○
travel apps	○	○	○	○	○
employment apps	○	○	○	○	○
arts and entertainment apps	○	○	○	○	○
dating apps	○	○	○	○	○
news apps	○	○	○	○	○
photo sharing apps	○	○	○	○	○
social networking apps	○	○	○	○	○

40. Overall, how do you feel about receiving ads that are targeted based on your beacon encounters? *

Very Dissatisfied	Dissatisfied	Neutral	Satisfied	Very Satisfied
○	○	○	○	○

41. What do you consider the main benefit, if any, of receiving targeted ads that are based on your beacon encounters?

42. What do you consider the main disadvantage, if any, of receiving targeted ads that are based on your beacon encounters?

43. Explain what, if anything, would make you feel more comfortable with receiving location-based ads based on beacon encounters?

Beacons & Privacy Management

44. Please state how much you agree or disagree with the following statements:

I would be more willing to allow collection of **ANONYMOUS** information (i.e., information that cannot be used to identify me or contact me) using beacons if my device did the following: *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
allowed me to choose ahead of time what information companies can learn about me	○	○	○	○	○
allowed me to control which companies can collect and use that information	○	○	○	○	○
allowed me to visualize what the companies already know about me	○	○	○	○	○
allowed me to create different "personas" (i.e., fake or real characterizations of me) to show to these companies at different points in time	○	○	○	○	○
allowed me to control in which locations my information can be collected	○	○	○	○	○
showed me in which locations my information has been collected	○	○	○	○	○

45. Please state how much you agree or disagree with the following statements:

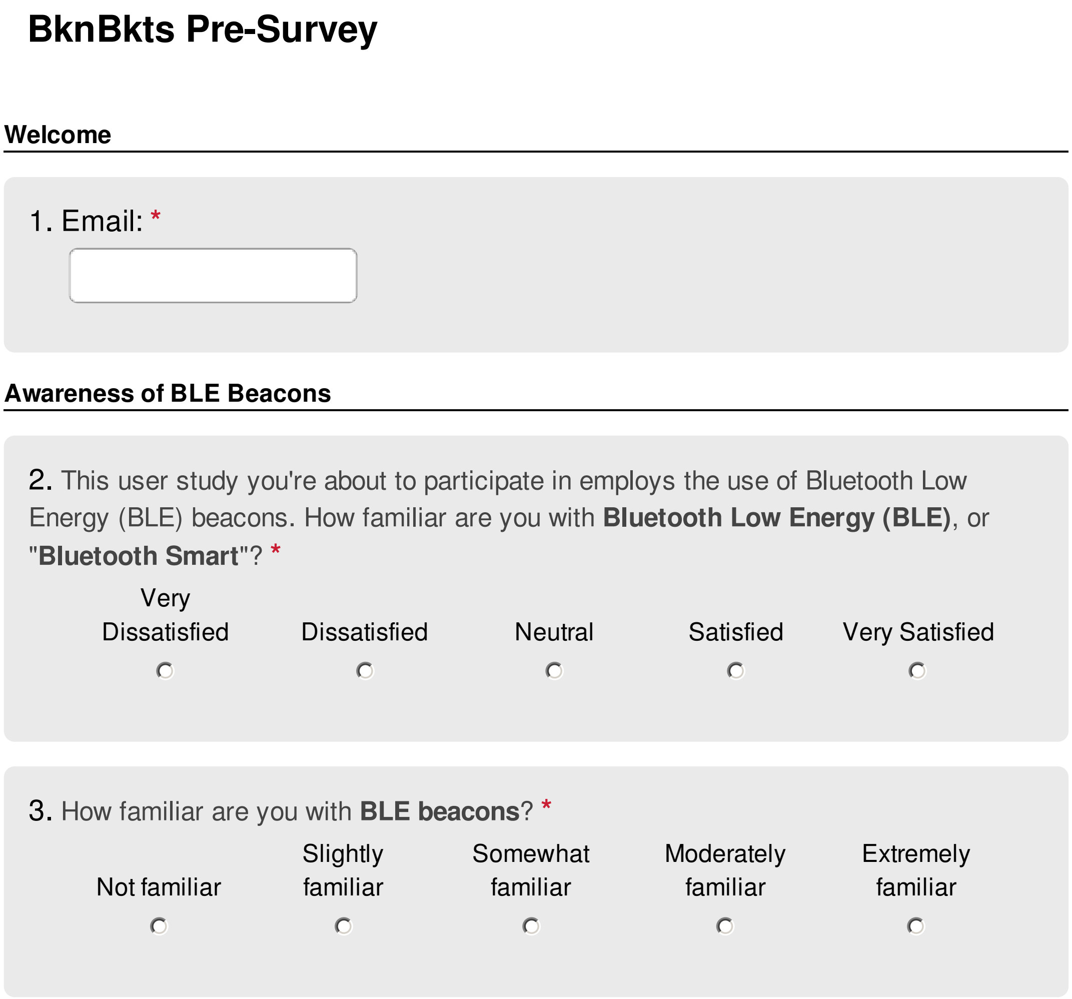
I would be more willing to allow collection of **PERSONAL** information (i.e. information that can be used to identify me and contact me) using beacons if my device did the following: *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
allowed me to choose ahead of time what information companies can learn about me	○	○	○	○	○
allowed me to control which companies can collect and use that information	○	○	○	○	○
allowed me to visualize what the companies already know about me	○	○	○	○	○
allowed me to create different "personas" (i.e., fake or real characterizations of me) to show to these companies at different points in time	○	○	○	○	○
allowed me to control in which locations my information can be collected	○	○	○	○	○
showed me in which locations my information has been collected	○	○	○	○	○

46. Imagine you could design a tool or application to help manage the privacy of your information regarding your beacon encounters. What features would it include? *

47. Do you have any further comments?

APPENDIX C: BKNBKTS USER STUDY PRE SURVEY



BknBkts Pre-Survey

Welcome

1. Email: *

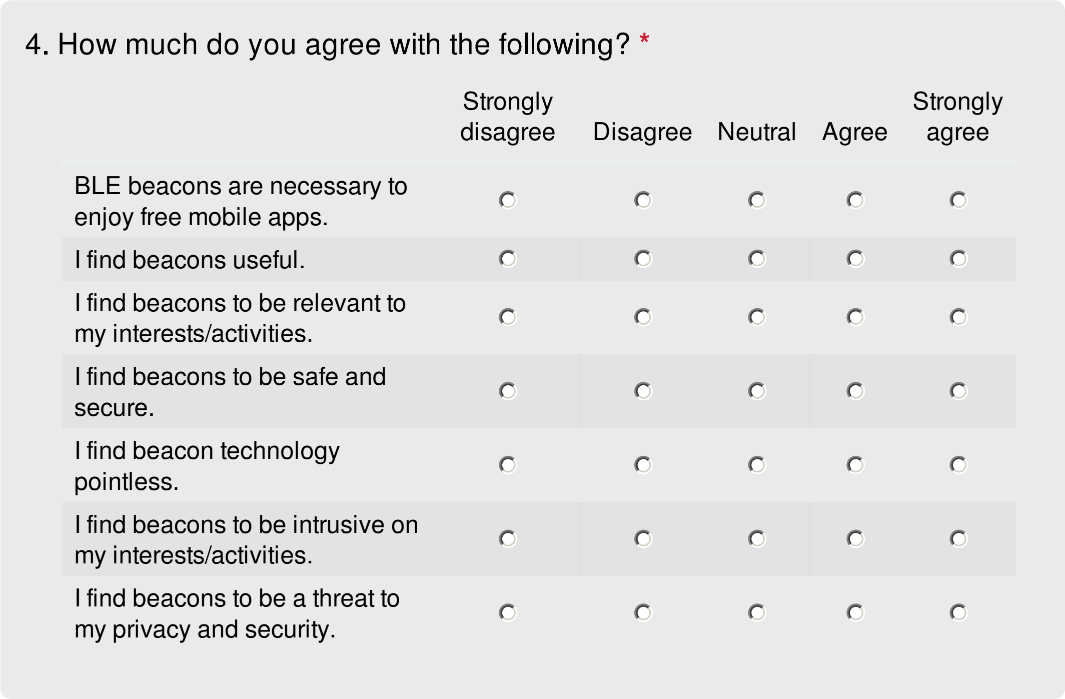
Awareness of BLE Beacons

2. This user study you're about to participate in employs the use of Bluetooth Low Energy (BLE) beacons. How familiar are you with **Bluetooth Low Energy (BLE)**, or "**Bluetooth Smart**"? *

Very Dissatisfied	Dissatisfied	Neutral	Satisfied	Very Satisfied
○	○	○	○	○

3. How familiar are you with **BLE beacons**? *

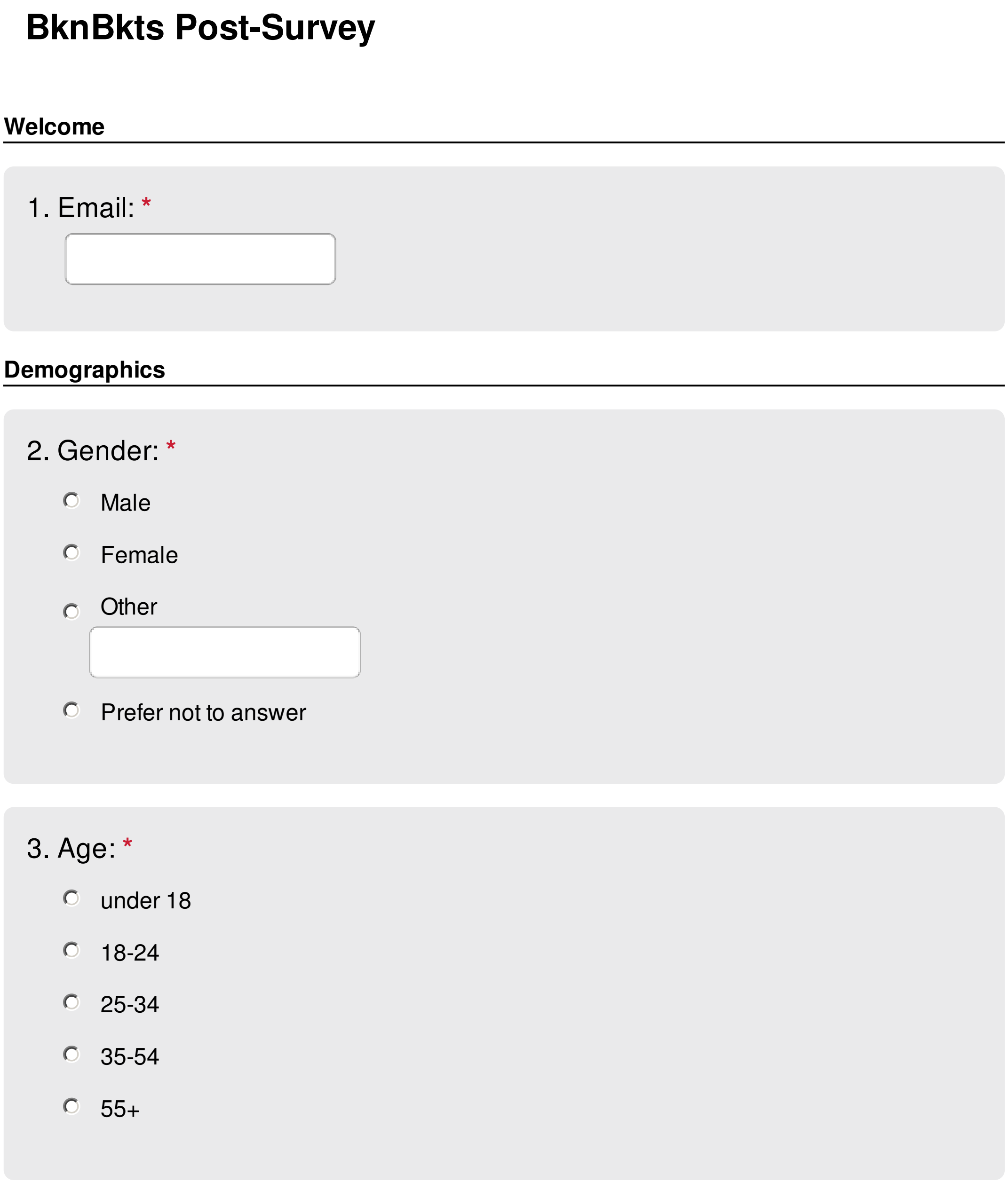
Not familiar	Slightly familiar	Somewhat familiar	Moderately familiar	Extremely familiar
○	○	○	○	○



4. How much do you agree with the following? *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
BLE beacons are necessary to enjoy free mobile apps.	○	○	○	○	○
I find beacons useful.	○	○	○	○	○
I find beacons to be relevant to my interests/activities.	○	○	○	○	○
I find beacons to be safe and secure.	○	○	○	○	○
I find beacon technology pointless.	○	○	○	○	○
I find beacons to be intrusive on my interests/activities.	○	○	○	○	○
I find beacons to be a threat to my privacy and security.	○	○	○	○	○

APPENDIX D: BKNBKTS USER STUDY POST SURVEY



BknBkts Post-Survey

Welcome

1. Email: *

Demographics

2. Gender: *

○ Male

○ Female

○ Other

○ Prefer not to answer

3. Age: *

○ under 18

○ 18-24

○ 25-34

○ 35-54

○ 55+

4. Race/Ethnicity: *

○ Native Hawaiian or Other Pacific Islander

○ Black/African-American

○ White

○ Hispanic/Latino

○ American Indian/Alaska Native

○ Other

5. Which of the following best describes your highest achieved level of education? *

12th grade or less
Graduated high school or equivalent
Some college, no degree
Associate degree
Bachelor's degree
Post-graduate degree

6. Which of the following best describes your primary occupation? *

○ Student

○ Employed

○ Unemployed

○ Prefer not to answer

○ Other

Technical Expertise

7. Do you have a college degree or work experience in computer science, software development, mobile app development, web development or similar computer-related fields? *

○ Yes

○ No

8. How often do you spend time on the Internet each day? *

○ Never

○ A few times per month

○ Once per week

○ Several times per week

○ Once per day

○ Several times per day

9. Do you own a smartphone? *

○ Yes - Android

○ Yes - iPhone

○ Yes - Other

○ No

10. How often do you spend time on your mobile phone each day? *

○ Never

○ Rarely

○ Sometimes

○ Often

○ Always

11. Have you ever done the following? (Select all that apply) *

□ Purchased a product or service online using your mobile phone (e.g., music, books, clothing, etc.)

□ Used a social networking app (e.g., Facebook, Twitter, LinkedIn, Instagram, etc.)

□ Clicked on an ad that appeared in an app to get more information about the advertised product

□ Accidentally clicked on an ad that appeared in an app

□ Used health, wellness, or medical information apps (e.g., MayoClinic, MyFitnessPal, Men's Health, etc.)

□ Used retail apps (e.g. Starbucks, Macy’s, Best Buy, etc.)

□ None of the above

12. Have you ever done the following? (Select all that apply) *

□ Refused to give information to an app because you felt it was too personal or unnecessary

□ Decided not to download an app or not to purchase something using an app because you were not sure how your personal information would be used

□ Read an app's privacy policy

□ Cleared the cache of an app on your phone

□ None of the above

13. How much do you agree or disagree with the following statements: *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
When websites ask for personal information, I usually think twice about providing it	○	○	○	○	○
Consumers have lost all control over how personal information is collected and used by companies	○	○	○	○	○
I feel that as a result of my visiting websites, others know more about me than I am comfortable with	○	○	○	○	○

App Usability

14. Please rate the follow statements about the usability of the "BknBkts" app. *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I think that I would like to use this app frequently.	○	○	○	○	○
I found the app unnecessarily complex.	○	○	○	○	○
I thought the app was easy to use.	○	○	○	○	○
I think that I would need the support of a technical person to be able to use this app.	○	○	○	○	○
I found the various functions in this app were well integrated.	○	○	○	○	○
I thought there was too much inconsistency in this app.	○	○	○	○	○
I would imagine that most people would learn to use this app very quickly.	○	○	○	○	○
I found the app very difficult to use.	○	○	○	○	○
I felt very confident using the app.	○	○	○	○	○
I needed to learn a lot of things before I could get going with this app.	○	○	○	○	○

15. Indicate your level of motivation by the following incentive to provide a label & privacy concern level for beacons with this app: *

	Not at all motivated	Slightly motivated	Somewhat motivated	Moderately motivated	Extremely motivated
Monetary (cash/gift card) rewards	○	○	○	○	○
Product coupons/discounts	○	○	○	○	○
Game points / Competitive rank	○	○	○	○	○

Awareness of BLE Beacons

16. This user study you participated in employed the use of Bluetooth Low Energy (BLE) beacons. How familiar are you with Bluetooth Low Energy (BLE), or "Bluetooth Smart"? *

Not familiar	Slightly familiar	Somewhat familiar	Moderately familiar	Extremely familiar
○	○	○	○	○

17. How familiar are you with BLE beacons? *

Not familiar	Slightly familiar	Somewhat familiar	Moderately familiar	Extremely familiar
○	○	○	○	○

18. How much do you agree with the following? *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
BLE beacons are necessary to enjoy free mobile apps.	○	○	○	○	○
I find beacons useful.	○	○	○	○	○
I find beacons to be relevant to my interests/activities.	○	○	○	○	○
I find beacons to be safe and secure.	○	○	○	○	○
I find beacon technology pointless.	○	○	○	○	○
I find beacons to be intrusive on my interests/activities.	○	○	○	○	○
I find beacons to be a threat to my privacy and security.	○	○	○	○	○

19. In a few sentences, tell us what you know about standard Bluetooth, as well as Bluetooth Low Energy. What do you know about each? How do you think they compare or contrast?

20. Briefly tell us what you know about **BLE beacons**. What is your experience with them, if any, other than this study?

□

Beacon Labels

21. How much would you trust the **top category/label** that were assigned to beacons **if they were based on crowdsourced consensus?** *

No trust at all	Very little trust	Somewhat trust	Moderate trust	Extreme trust
○	○	○	○	○

22. How much would you trust the **top category/label** that were assigned to beacons **if they were assigned by the retailer/beacon provider?** *

No trust at all	Very little trust	Somewhat trust	Moderate trust	Extreme trust
○	○	○	○	○

23. How much would you trust the **top category/label** that were assigned to beacons **if they were assigned by an independent 3rd-party authority?** *

No trust at all	Very little trust	Somewhat trust	Moderate trust	Extreme trust
○	○	○	○	○

Beacon Sensitivity

24. How much would you trust the **average privacy concern levels** that were associated with beacons **if they were based on crowdsourced consensus?** *

No trust at all	Very little trust	Somewhat trust	Moderate trust	Extreme trust
○	○	○	○	○

25. How much would you trust the **average privacy concern levels** that were associated with beacons **if they were assigned by the retailer/beacon provider?** *

No trust at all	Very little trust	Somewhat trust	Moderate trust	Extreme trust
○	○	○	○	○

26. How much would you trust the **average privacy concern levels** that were associated with beacons **if they were assigned by an independent 3rd-party authority?** *

No trust at all	Very little trust	Somewhat trust	Moderate trust	Extreme trust
○	○	○	○	○

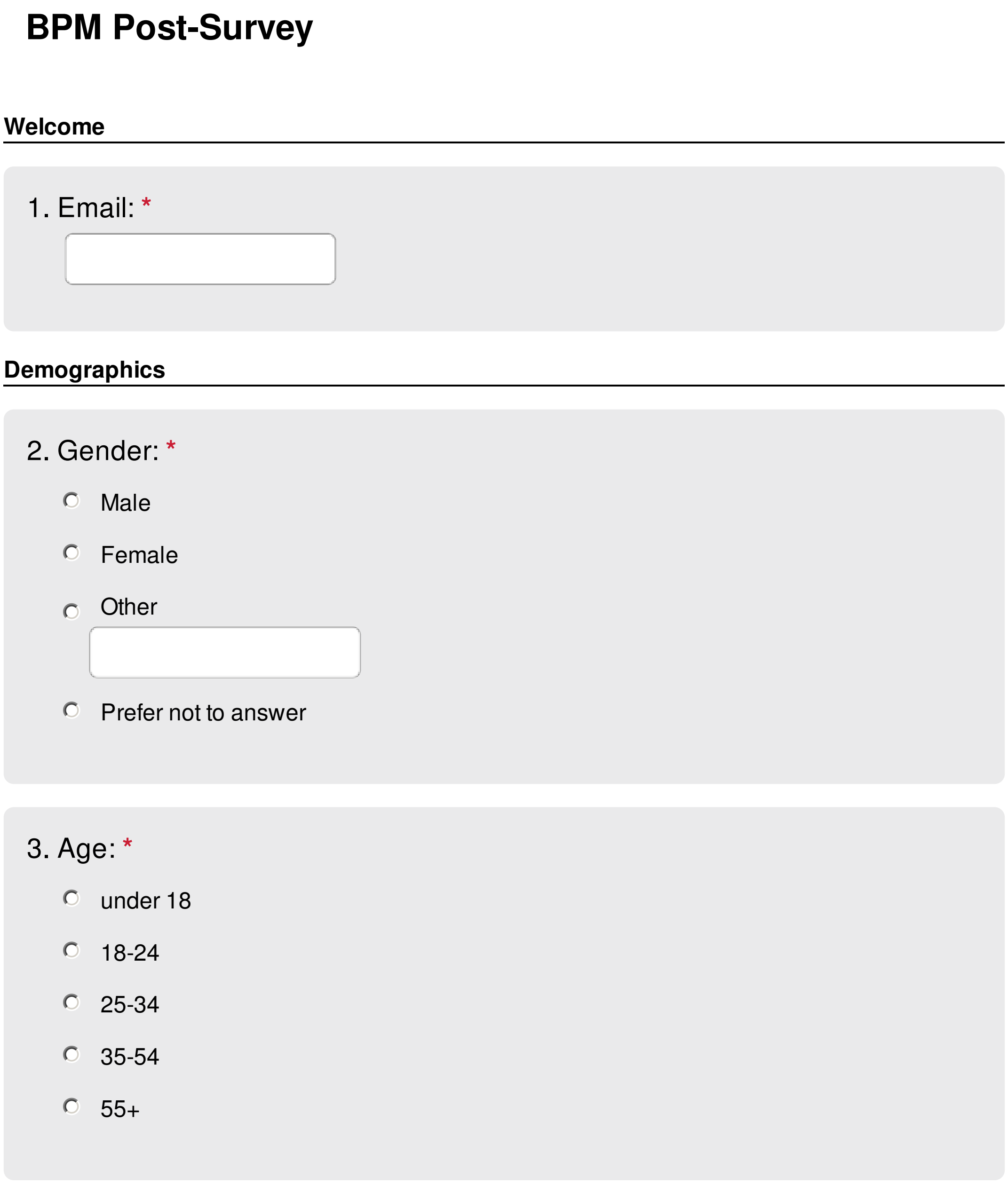
Information Sharing

27. How much do you agree that your willingness to share the following information from a beacon encounter **depends on the context** (i.e. the category and sensitivity level): *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Beacon encounter information (e.g. time/duration of visit, frequency of visit)	○	○	○	○	○
Mobile device information (e.g. operating system, device version, cell carrier)	○	○	○	○	○
Demographic information (e.g. age, gender, religion, sexual orientation, marital status)	○	○	○	○	○
Physical location (e.g. current city, state, country, zip code)	○	○	○	○	○
Personally identifiable information (e.g. social security number, phone number, email)	○	○	○	○	○

28. Any final comments?

APPENDIX E: BPM USER STUDY POST SURVEY



BPM Post-Survey

Welcome

1. Email: *

Demographics

2. Gender: *

○ Male

○ Female

○ Other

○ Prefer not to answer

3. Age: *

○ under 18

○ 18-24

○ 25-34

○ 35-54

○ 55+

4. Race/Ethnicity: *

○ Native Hawaiian or Other Pacific Islander

○ Black/African-American

○ White

○ Hispanic/Latino

○ Asian/Middle Eastern

○ American Indian/Alaska Native

○ Other

5. Which of the following best describes your highest achieved level of education? *

12th grade or less
Graduated high school or equivalent
Some college, no degree
Associate degree
Bachelor's degree
Post-graduate degree

6. Which of the following best describes your primary occupation? *

○ Student

○ Employed

○ Unemployed

○ Prefer not to answer

○ Other

Technical Expertise

7. Do you have a college degree or work experience in computer science, software development, mobile app development, web development or similar computer-related fields? *

○ Yes

○ No

8. How often do you spend time on the Internet? *

○ Never

○ A few times per month

○ Once per week

○ Several times per week

○ Once per day

○ Several times per day

9. Do you own a smartphone? *

○ Yes - Android

○ Yes - iPhone

○ Yes - Other

○ No

10. How often do you spend time on your mobile phone each day? *

○ Never

○ Rarely

○ Sometimes

○ Often

○ Always

11. Have you ever done the following? (Select all that apply) *

□ Purchased a product or service online using your mobile phone (e.g., music, books, clothing, etc.)

□ Used a social networking app (e.g., Facebook, Twitter, LinkedIn, Instagram, etc.)

□ Clicked on an ad that appeared in an app to get more information about the advertised product

□ Accidentally clicked on an ad that appeared in an app

□ Used health, wellness, or medical information apps (e.g., MayoClinic, MyFitnessPal, Men's Health, etc.)

□ Used retail apps (e.g. Starbucks, Macy’s, Best Buy, etc.)

□ None of the above

12. Have you ever done the following? (Select all that apply) *

□ Refused to give information to an app because you felt it was too personal or unnecessary

□ Decided not to download an app or not to purchase something using an app because you were not sure how your personal information would be used

□ Read an app's privacy policy

□ Cleared the cache of an app on your phone

□ None of the above

13. How much do you agree or disagree with the following statements: *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
When websites ask for personal information, I usually think twice about providing it	○	○	○	○	○
Consumers have lost all control over how personal information is collected and used by companies	○	○	○	○	○
I feel that as a result of my visiting websites, others know more about me than I am comfortable with	○	○	○	○	○

App Usability

14. Please rate the follow statements about the usability of the "Beacon Privacy Manager" app. *

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I think that I would like to use this app frequently.	○	○	○	○	○
I found the app unnecessarily complex.	○	○	○	○	○
I thought the app was easy to use.	○	○	○	○	○
I think that I would need the support of a technical person to be able to use this app.	○	○	○	○	○
I found the various functions in this app were well integrated.	○	○	○	○	○
I thought there was too much inconsistency in this app.	○	○	○	○	○
I would imagine that most people would learn to use this app very quickly.	○	○	○	○	○
I found the app very difficult to use.	○	○	○	○	○
I felt very confident using the app.	○	○	○	○	○
I needed to learn a lot of things before I could get going with this app.	○	○	○	○	○

Awareness of BLE Beacons

15. This user study you participated in employed the use of Bluetooth Low Energy (BLE) beacons. How familiar are you with Bluetooth Low Energy (BLE), or "Bluetooth Smart"? *

Not familiar	Slightly familiar	Somewhat familiar	Moderately familiar	Extremely familiar
○	○	○	○	○

16. How familiar are you with BLE beacons? *

Not familiar	Slightly familiar	Somewhat familiar	Moderately familiar	Extremely familiar
○	○	○	○	○

17. How much do you agree with the following? *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
BLE beacons are necessary to enjoy free mobile apps.	○	○	○	○	○
I find beacons useful.	○	○	○	○	○
I find beacons to be relevant to my interests/activities.	○	○	○	○	○
I find beacons to be safe and secure.	○	○	○	○	○
I find beacon technology pointless.	○	○	○	○	○
I find beacons to be intrusive on my interests/activities.	○	○	○	○	○
I find beacons to be a threat to my privacy and security.	○	○	○	○	○

18. In a few sentences, tell us what you know about standard Bluetooth, as well as Bluetooth Low Energy. What do you know about each? How do you think they compare or contrast?

19. Briefly tell us what you know about **BLE beacons**. What is your experience with them, if any, other than this study?

Beacon Privacy Policies

20. In this study, were you asked to first set the policies upfront, then discover, or only to set each policy as you discovered the beacon?

- ○ Set all policies upfront first, then discover
- ○ Set policies as I discover

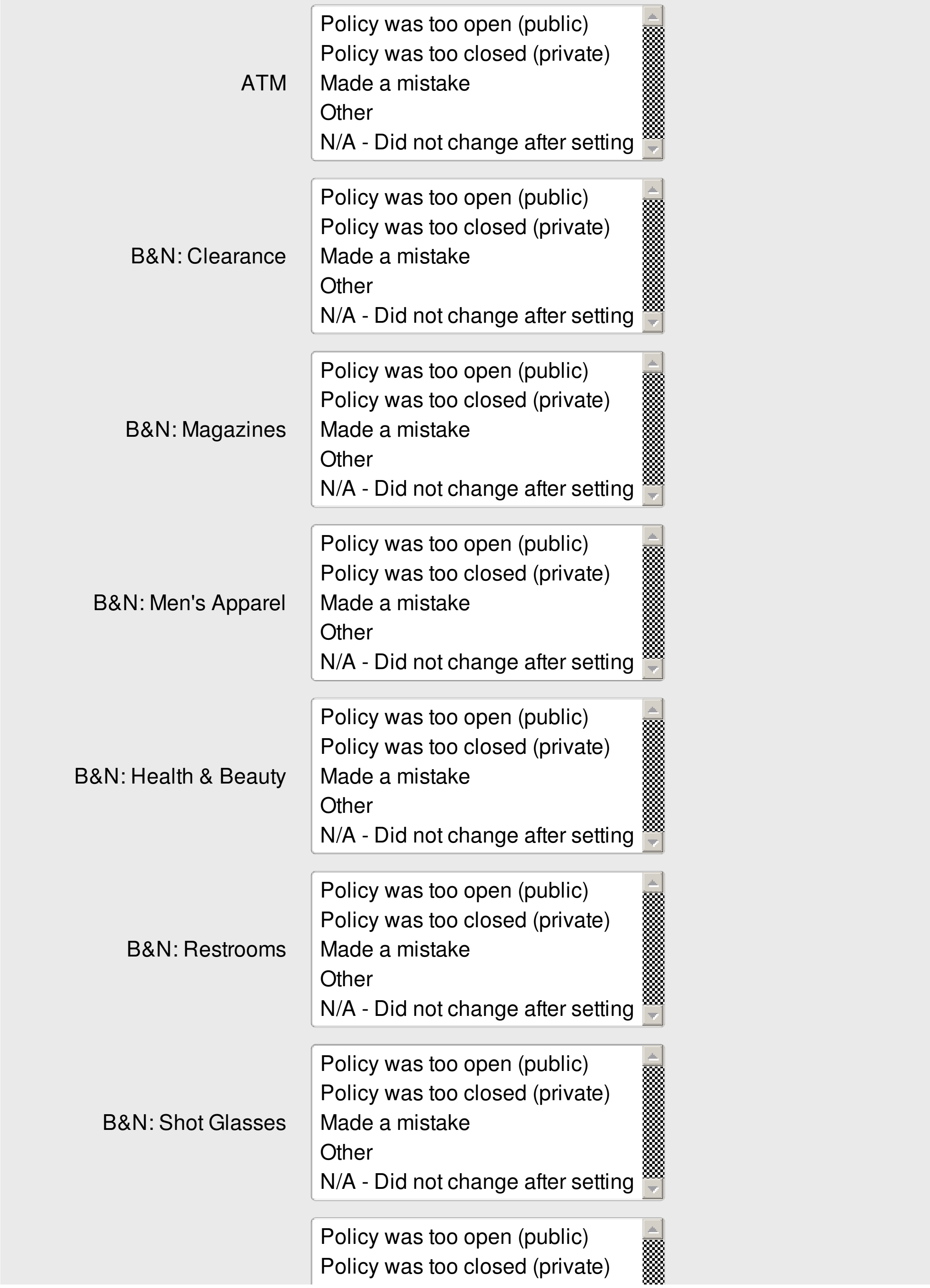
21. How much control did you feel you had over the privacy policies you set? *

No control at all	Very little control	Moderal control	Significant control	Extreme control
○	○	○	○	○

22. How much trust did you have that the policies you set were being enforced? *

No trust at all	Very little trust	Somewhat trust	Moderate trust	Extreme trust
○	○	○	○	○

23. In any situation where you went back and changed a previously set policy, what was your reason for doing so? *



ATM
Policy was too open (public)
Policy was too closed (private)
Made a mistake
Other
N/A - Did not change after setting

B&N: Clearance
Policy was too open (public)
Policy was too closed (private)
Made a mistake
Other
N/A - Did not change after setting

B&N: Magazines
Policy was too open (public)
Policy was too closed (private)
Made a mistake
Other
N/A - Did not change after setting

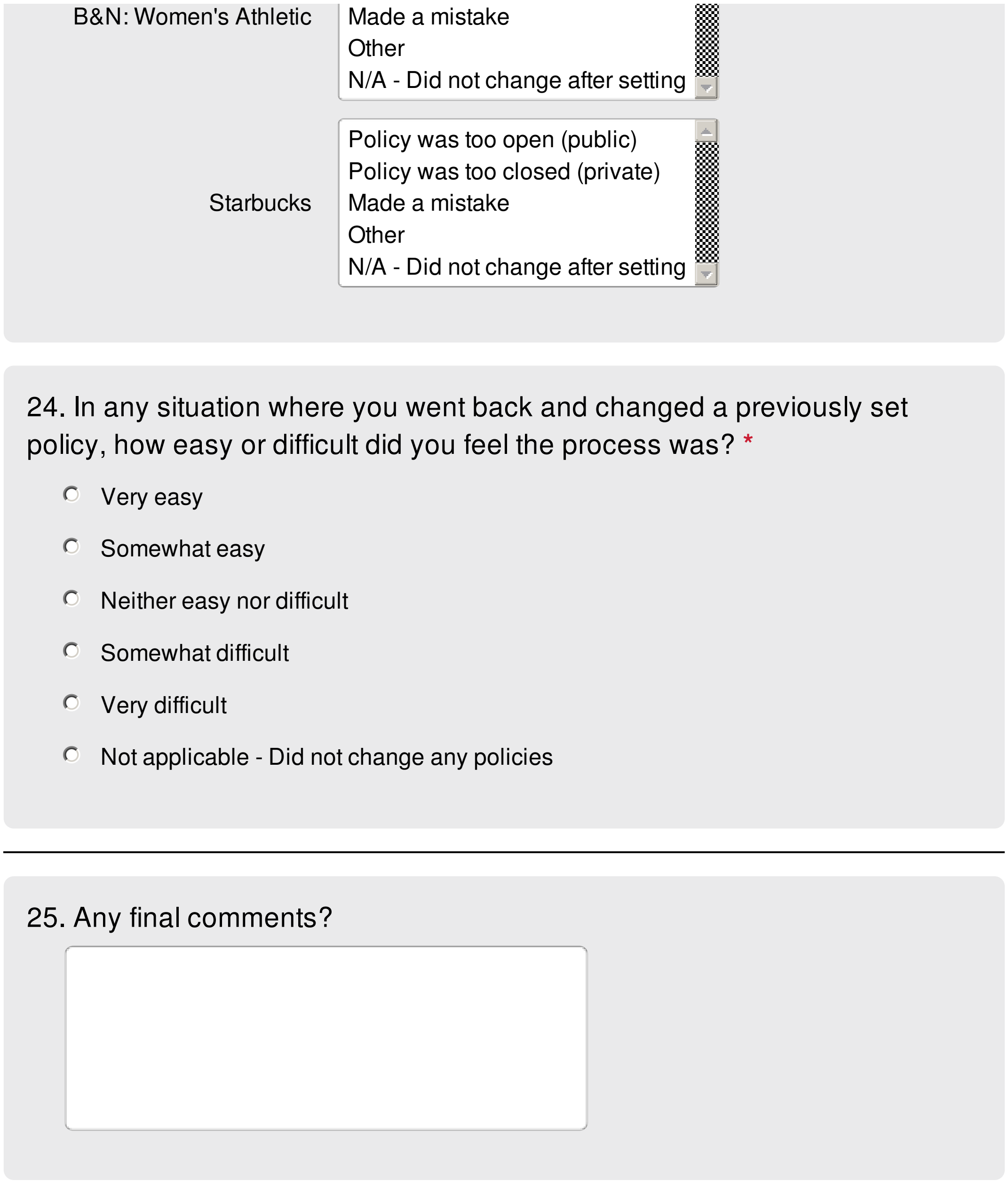
B&N: Men's Apparel
Policy was too open (public)
Policy was too closed (private)
Made a mistake
Other
N/A - Did not change after setting

B&N: Health & Beauty
Policy was too open (public)
Policy was too closed (private)
Made a mistake
Other
N/A - Did not change after setting

B&N: Restrooms
Policy was too open (public)
Policy was too closed (private)
Made a mistake
Other
N/A - Did not change after setting

B&N: Shot Glasses
Policy was too open (public)
Policy was too closed (private)
Made a mistake
Other
N/A - Did not change after setting

Policy was too open (public)
Policy was too closed (private)



B&N: Women's Athletic

Made a mistake
Other
N/A - Did not change after setting

Starbucks

Policy was too open (public)
Policy was too closed (private)
Made a mistake
Other
N/A - Did not change after setting

24. In any situation where you went back and changed a previously set policy, how easy or difficult did you feel the process was? *

○ Very easy

○ Somewhat easy

○ Neither easy nor difficult

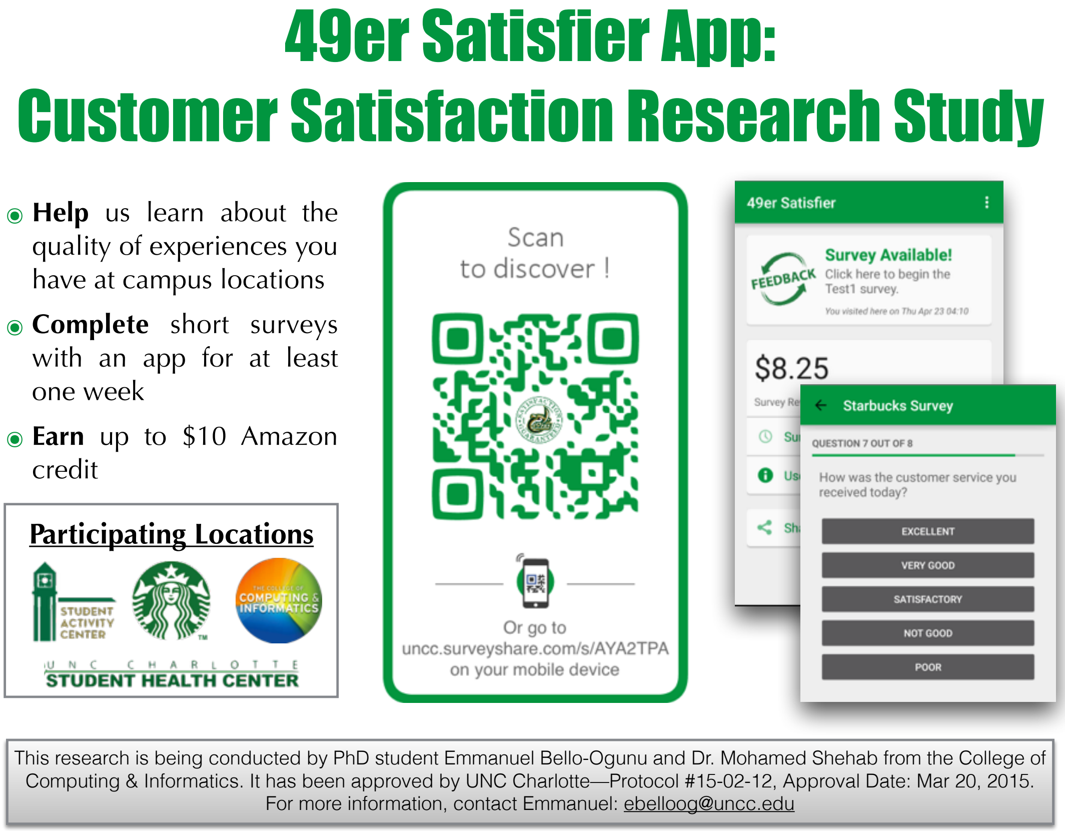
○ Somewhat difficult

○ Very difficult

○ Not applicable - Did not change any policies

25. Any final comments?

APPENDIX F: 49ER SATISFIER USER STUDY RECRUITMENT FLYER



49er Satisfier App: Customer Satisfaction Research Study

- **Help** us learn about the quality of experiences you have at campus locations
- **Complete** short surveys with an app for at least one week
- **Earn** up to $10 Amazon credit

Participating Locations

STUDENT ACTIVITY CENTER
COMPUTING & INFORMATICS
UNC CHARLOTTE
STUDENT HEALTH CENTER

Scan to discover !

Or go to uncc.surveyshare.com/s/AYA2TPA on your mobile device

49er Satisfier
FEEDBACK

Survey Available! Click here to begin the Test1 survey.

You visited here on Thu Apr 23 04:10

$8.25

How was the customer service you received today?

This research is being conducted by PhD student Emmanuel Bello-Ogunu and Dr. Mohamed Shehab from the College of Computing & Informatics. It has been approved by UNC Charlotte—Protocol #15-02-12, Approval Date: Mar 20, 2015. For more information, contact Emmanuel: ebelloog@uncc.edu

APPENDIX G: BKNBKTS USER STUDY RECRUITMENT FLYER

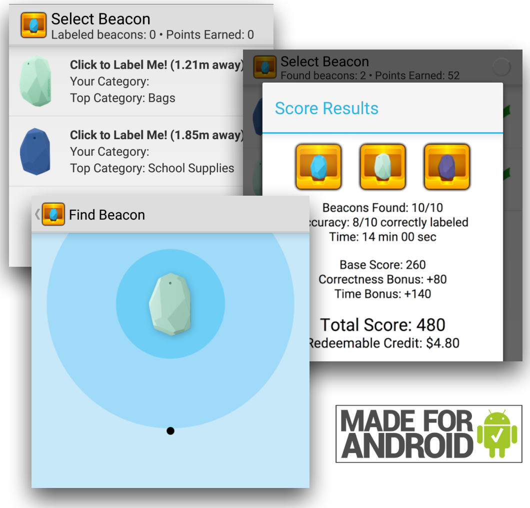
BknBkts™:
Beacon Scavenger Hunt Game

1. **Download** the app and email ebelloog@uncc.edu to schedule a session between 8am-5pm M-F
2. **Visit** the Student Union
3. **Hunt** for beacons placed around the Bookstore, Starbucks, and the Union Rotunda using the app
4. **Find and label** all beacons correctly
5. **Compete** for top points and earn $$$
6. **Complete** short post-survey
7. **Redeem** your gift card reward!

Scan
to discover !

Or visit
tiny.cc/BknBktsApp
on your mobile device

(No Android device? Email ebelloog@uncc.edu to sign up, and ask to use a loaner phone)



Select Beacon
Labeled beacons: 0 • Points Earned: 0

Click to Label Me! (1.21m away)
Your Category:
Top Category: Bags

Click to Label Me! (1.85m away)
Your Category:
Top Category: School Supplies

Select Beacon
Found beacons: 2 • Points Earned: 52

Score Results

Beacons Found: 10/10
ccuracy: 8/10 correctly labeled
Time: 14 min 00 sec

Base Score: 260
Correctness Bonus: +80
Time Bonus: +140

Total Score: 480
Redeemable Credit: $4.80

MADE FOR ANDROID

This research study is being conducted by PhD student Emmanuel Bello-Ogunu, Master's student Sanika Joshi, and Dr. Mohamed Shehab, from the College of Computing & Informatics. It has been approved by UNC Charlotte —Protocol #08-12-2015-01, Approval Date: Mar 20, 2015.

For more information, contact Emmanuel: ebelloog@uncc.edu