EXPLORING THE PERCEPTIONS OF USERS-AS-BEACONS SYSTEMS: DEVELOPING AND DEPLOYING REAL-LIFE PROTOTYPES

by

Md Nazmus Sakib Miazi

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

2020

Approved by:

_____

Dr. Mohamed Shehab

_____

Dr. Heather Lipford

_____

Dr. Weichao Wang

_____

Dr. Lina Zhou

ABSTRACT

MD NAZMUS SAKIB MIAZI. Exploring the Perceptions of Users-as-Beacons Systems: Developing and Deploying Real-Life Prototypes. (Under the direction of DR. MOHAMED SHEHAB and DR. HEATHER LIPFORD)

Bluetooth Low Energy (BLE) beacons are widely adopted in a vast range of industries involving the Internet of things (IoT). BLE is primarily used for indoor location estimation. It is often utilized to provide contextual information with low energy consumption and low-cost mobile beacons. BLE beacons are currently deployed in superstores, stadiums, and hospitals to leverage proximity marketing, inventory management, utility management, as well as enhancing usability. In this dissertation, I propose and explore a novel system, named 'Users-as-Beacons' (U-a-B) built upon BLE technology, where BLE-enabled smartphones become live beacons.

In my research, I explore the possibility of developing U-a-B systems through multiple user studies. In these studies, I investigate the following research questions. (i) What are the potential application areas and appropriate contexts of U-a-B? (ii) What are the users' preferences for the disclosure of personal information in U-a-B? and (iii) What are the general perceptions and preferences, particularly around privacy, of users in U-a-B?

From the exploratory studies, I classified the potential application areas including localized advertising platform for shopping areas, instant review platform for shopping areas, a crowdsourced localized platform for reviewing places, and community-based social networks. I also identified several design challenges to develop such a system, such as the trustworthiness of the system, relevance of the contents, timeliness of the

content delivery, and the desired form of interactions among users. Subsequently, I developed a fully working real-life prototype and deployed it in a festival. Based on all these results, I describe a set of privacy-preserving design guidelines to implement a scalable, usable, and privacy-preserving Users-as-Beacons platform.

ACKNOWLEDGMENTS

One thing that someone needs over the course of a doctoral program would be the patience to build better habits throughout the journey. If I look five years back, I was not the person I am now. This excursion to explore the unknown shaped me to a different, hopefully, a better person. I would not have been able to complete this arduous journey without the grace of almighty. Hence, first and foremost, I give thanks to the almighty, my parents, my younger brother, and my beautiful wife, Madiha, and acknowledge the grace bestowed on me.

I thank my family for all they did for me, from breakfast to the words of wisdom, and everything in between. I am privileged to have parents who encouraged me in every way to pursue success and instilled me in the value of education. I cannot express enough thanks to my wife Madiha, who held me up steady from the ups to the tipping points. I thank my younger brother Sabbir, who has always provided me with support and encouragement. I also want to express my gratitude to my in-laws, especially Sadia, my sister-in-law, for their consistent support and confidence.

I would like to state my gratitude to Dr. Mohamed Shehab, my advisor. I believe one of the most crucial and righteous decisions in my Ph.D. was to find him as my advisor. I was fortunate in having such a knowledgeable, forthright, hands-on, and above all, inquisitive person as my advisor. He was kind enough when I needed support, yet challenged me in every step, that built me as an independent researcher. I also want to express my special gratitude to Dr. Heather Lipford, my co-advisor, more than a mentor, a real guide toward the end of my dissertation. There are

no words that can manifest my appreciation to her adequately. I also thank and appreciate Dr. Weichao Wang and Dr. Lina Zhou for being in my committee and providing their insightful comments and suggestions all the way. I would also express my heartiest gratitude to Dr. Mary Lou Maher, a super lady, for guiding me through many of my tough situations. And, I would like to acknowledge Sandra Krause, our *mother* abroad, who listened to all my problems and solved them like magic.

Living 8,500 miles away from home is never easy. However, I am privileged to have such a kind Charlotte-family here. My heartiest gratitude toward Ashutosh Dutta, and Moumita Das, without whom it would be unthinkable for me to finish this journey. I am honored to be one of the founding members of Ekush - Bangladesh Student Organization and acknowledge all their support throughout this arduous journey. I reminisce about the memory of Imtiaz Ikram and Pracheta Dutta, whom we lost tragically along the way. I thank Mehedi, Mehrab, Moinul, Mahbubur, Rakeb, Mohi, Nasheen, Abdullah, Mahfuz, Faria, Shishir, Shamir, Rabby, Syeda, Saquib, Sajid, Jeba, and many others for always being there with me. I also thank Mr. and Mrs. Biswajit, Mr. and Mrs. Raqibul, and Mr. and Mrs. Mallik, for their support.

I was fortunate enough to have such steller colleagues during my graduate career. Over a cup of coffee to even collaboration in some instances, I have learned a lot from the people around me at UNC Charlotte. In no particular order, these colleagues included Abeer AlJarrah, Fadi Yilmaz, Usman Rauf, Yousra Javed, Stephen McNeil, Amirreza, Fadi Mohsen, Emmanuel Bello-Ogunu, Abhinav Mohanty, Mohammed Al-saleh, Lipsa Sahoo, Elham, Obaidat, and Abdul Majeed. I will always cherish the time we spent together as peers, where we shared each other's burdens and celebrated

successes.

I would want to acknowledge some of the all-time mentors of mine. I am blessed to have Dr. Abdur Razzaque as my undergraduate advisor and mentor, from whom I learned how to conduct academic research. I am especially grateful to Dr. Mahmudul Hasan Nayeem, who encouraged me all the way from undergrad to Ph.D. He is one of the persons I never hesitate to contact when I need any advice. I would be forever thankful to some of my favorite professors, Dr. Lafifa Jamal, Dr. Syed Monowar Hossain, and Mr. Shahed Anwar.

I would be remiss not to mention my closest friends and biggest fans, who provided support that was unmatched to others. No amount of words is enough to express how grateful I am to Farhan, Muntasir, Rahat, Tonmoy, Muttaki, Prantar, and Tajdid. Not to mention Nusrat, Asma, Amit, Tamal, Ashraf, Humayra, and Sakin. You were always with me when I needed you, and I cherish every moment we spent together.

Finally, I would like to recognize the countless participants, reviewers, and other scholars, whom I have relied on throughout the journey. And lastly, I would like to thank UNC Charlotte for the fantastic five years of my life. I am proud to be a 49er.

TABLE OF CONTENTS

LIST OF FIGURES xiii

LIST OF TABLES xiv

CHAPTER 1: Introduction 1

1.1. Bluetooth and BLE 1

1.2. BLE Beacons: a Brief Introduction 3

1.3. Users as Beacons 5

1.4. Potential applications of a 'users-as-beacons' system 7

1.5. Thesis Statement and Contributions 11

1.6. Contributions and Outline of the Dissertation 13

CHAPTER 2: Background 15

2.0.1. BLE applications 15

2.1. Platforms related to Users-as-Beacons' application areas 16

2.1.1. User generated content 16

2.1.2. Review systems 20

2.1.3. SARS-COV-2 contact tracing 21

2.1.4. Privacy-preserving localized systems 22

2.2. Privacy in similar contexts 28

2.2.1. Location-based systems 28

2.2.2. Behavioral tracking in social and advertising systems 31

2.2.3. Targeted and tailored contents in social systems 33

2.3. Summary 35

CHAPTER 3: Exploring Mobile Users' Opinions and Experience while being deployed as advertising beacons 37

3.1. Introduction 37

3.2. User Study Design 40

3.2.1. Hypotheses 45

3.2.2. User Study Flow 46

3.2.3. Analysis Procedure 49

3.3. Results 50

3.3.1. Effect of Product's Sensitivity Level 52

3.3.2. Effect of Exposure to Public 53

3.3.3. Effect of Public Influence 54

3.3.4. Post-study Survey 55

3.4. Discussion and Limitation 58

3.4.1. Analysis on our results 59

3.4.2. Takeaways 60

3.5. Summary 61

CHAPTER 4: Users' Perceptions of being Users as Beacons 62

4.1. Introduction 62

4.2. User studies 63

4.2.1. User study 1: users as beacons for reviewing products 64

4.2.2. User study 2: users-as-beacons for reviewing places, services, and events 67

4.3. Participants and Analysis procedure 70

4.3.1. Participant Recruitment and Demographics 70

4.3.2. Analysis 71

4.3.3. Limitations 72

4.4. Results 72

4.4.1. General perceptions about reading reviews 73

4.4.2. Writing reviews to the people around 75

4.4.3. Sharing personal information 77

4.4.4. Interacting with others 77

4.4.5. Interacting with establishment 80

4.4.6. Privacy in users-as-beacons 81

4.5. Discussion and Implications 86

4.5.1. Feasibility and applicability of the system: 86

4.5.2. Design Challenges 87

4.5.3. Future research needs 89

4.6. Summary 90

CHAPTER 5: Developing the Prototype 92

5.1. Introduction 92

5.1.1. Prototype test-bed 92

5.1.2. Challenges and Limitations to Develop and Deploy the Prototype 92

5.2. The Design and Functionalities of the Prototype 93

5.2.1. The Back-end 94

5.2.2. The Front-end 97

5.3. Development Environment and the Public Project 101

5.4. Summary 101

CHAPTER 6: Deploying a Real Life Prototype to Investigate the effectiveness of Users-as-Beacons in a Crowded and Localized Context 103

6.1. Study Design 105

6.2. Recruitment 106

6.3. Results 106

6.3.1. System Utilization 107

6.3.2. Survey Results 111

6.3.3. Post-study interview 114

6.4. Discussion 124

6.4.1. Managing Trustworthiness 124

6.4.2. Managing Boundaries 124

6.4.3. Relevance and Localized Setting 125

6.5. Summary 125

CHAPTER 7: Discussion and Implications 127

7.1. Introduction 127

7.2. Revisiting the potential application Scenarios 127

7.3. Finding the appropriate context 128

7.4. Privacy implications 130

7.4.1. Information disclosure and privacy trade-off 130

7.4.2. Location privacy 132

7.4.3. Managing boundaries in peer-interaction 133

7.4.4. Managing trust 134

7.4.5. Motivations and Incentives 135

7.5. Privacy preserving design guidelines 135

7.6. Conclusion 138

REFERENCES 139

APPENDIX A: Supplementary data for chapter 4 146

Demographics of the participants 146

Interview Questions 146

Study 1 146

Study 2 150

Survey questionnaire 153

APPENDIX B: Supplementary data for chapter 6 156

Demographics of the participants 156

Survey questionnaire 156

LIST OF FIGURES

FIGURE 1: How BLE beacons work [12]. 2

FIGURE 2: BLE Beacon advertising mechanism. 4

FIGURE 3: Users as Beacons. 6

FIGURE 4: Example of a 'users-as-beacons' app for creating crowd-sourced and localized posts in a festival. 10

FIGURE 5: Experiment Testbed, the Bookstore. 41

FIGURE 6: Sorted sensitivity levels of store products 44

FIGURE 7: Screen-shots of the application and in-store big screens. 47

FIGURE 8: Examples of artificially tailored ads. 52

FIGURE 9: "I would be willing to allow to collect the following information for benefits." 58

FIGURE 10: Screen-shots of the design probe built for conducting study 1. 65

FIGURE 11: U-a-B user interaction backend. 94

FIGURE 12: Screenshot of the prototype deployed at iFest (part 1). 98

FIGURE 13: Screenshot of the prototype deployed at iFest (part 2). 99

FIGURE 14: The map of iFest (Halton Arena at UNC Charlotte). 104

FIGURE 15: Histograms for system utilization. 108

FIGURE 16: Survey Summary. 112

LIST OF TABLES

TABLE 1: Demographic Summary of the participants 45

TABLE 2: Descriptive statistics of information shared for various conditions 50

TABLE 3: Test of Normality 51

TABLE 4: Correlations between Agree Levels and Percentage of Information Shared 57

TABLE 5: Demographic Summary of the participants 70

TABLE 6: Demographic Summary of the participants 106

TABLE 7: Descriptive results for system utilization. 107

TABLE 8: Categorized list of interview participants 114

TABLE 9: Demographics of the participants in study 1 146

TABLE 10: Demographics of the participants in study 2 147

TABLE 11: Demographics of the participants in deployment study 156

CHAPTER 1: INTRODUCTION

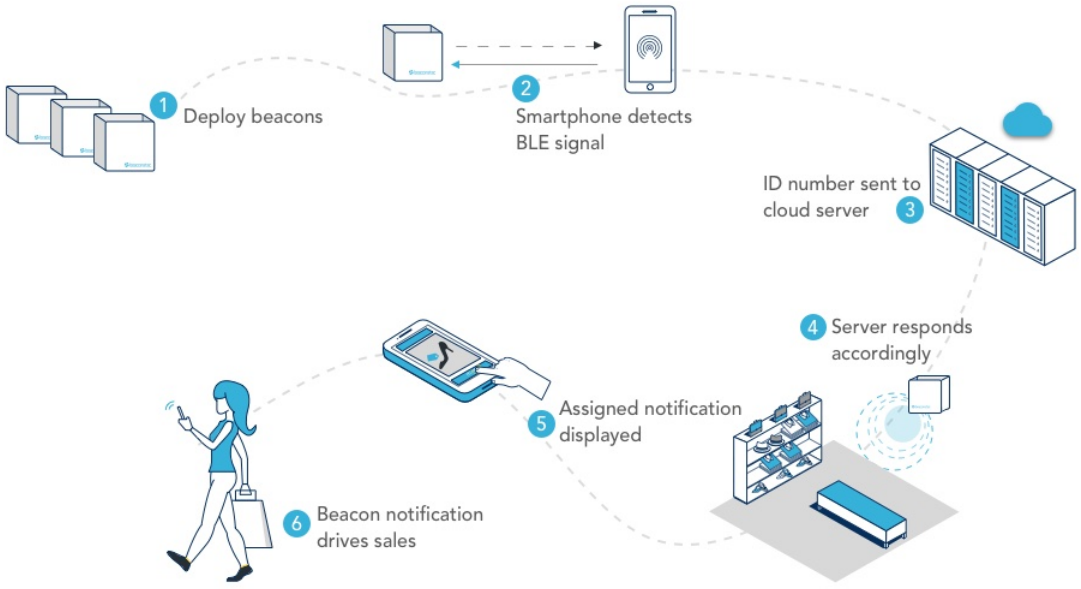
In this era of modern technologies, smart devices play a pivotal role to make our lives more comfortable and convenient. From phones to thermostats, we use smart devices in every part of our day. The widespread trend of smartphone usage is pushing businesses and services to focus on mobile user experience to keep competitive and bring in more customers. The usage of the Internet of Things (IoT) is playing a pivotal role in transforming the industries for developing a mobile-friendly distributed ecosystem. Bluetooth Low Energy (BLE) beacons are an example of an IoT technology, and are widely being adopted by modern businesses. BLE is a modern extension of traditional Bluetooth technology, primarily intended to provide a low cost and low energy solution for continuous advertising for Bluetooth enabled devices. Our primary contribution in this dissertation is extending the BLE technology to build up a new platform we refer to as 'Users-as-Beacons' where we can turn the BLE enabled user devices into customized live user-beacons.

1.1 Bluetooth and BLE

Bluetooth is one of the most known technologies for device communication, and has been used in numerous places and things like phones, keyboards, mouses, pointer devices, cameras, computers, cars, and many other devices and peripherals since the late 90s. The Bluetooth Special Interest Group (SIG) comprises of more than 30,000

member companies in the areas of telecommunication, computing, networking, and consumer electronics monitors and guides the development of specification, qualifications, and deployment of the technology [8]. Bluetooth SIG is involved in designing and marketing the technologies evolved from Bluetooth, and one of the examples of these developed technologies is Bluetooth Low Energy (BLE). The SIG started marketing BLE since 2010, aiming at novel applications in the fitness, beacons, healthcare, security, and home entertainment industries [6]. The main advantage of BLE compared to classic Bluetooth is that BLE is intended to resolve the energy consumption problem of Bluetooth and use considerably reduced power and cost while maintaining a similar communication range. BLE is not backward compatible, thus the devices with Bluetooth 4.0 standard capability or later can implement services for both classic Bluetooth and BLE.

Figure 1: How BLE beacons work [12].



Organizations are focusing on the widespread use of mobile technologies to reach more customers due to the increasing number of smartphone users. In doing so, the Internet of Things (IoT) becomes a dominant tool for the business entities to transform the infrastructure to accommodate mobile-friendly ecosystems. Gartner predicted that 25 billion connected things would be in use by 2020 [4]. BLE Beacons is an example of IoT, which has been widely adopted by a vast range of industries recently.

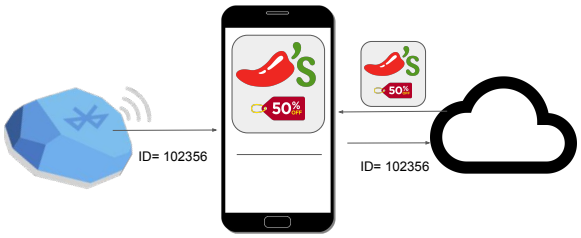
1.2 BLE Beacons: a Brief Introduction

The Bluetooth Low Energy (BLE) specification is defined in Bluetooth 4.0 specifications [2]. Unlike standard Bluetooth, which has been widely used in cars, smartphones, and many IoT devices to transmit a large amount of data, BLE focuses on delivering a minimal amount of data ensuring low energy consumption and longer battery life. BLE generally functions as a one-way advertising mechanism where it uses the advertising channel to transmit a data packet having at most 47 bytes, in intervals from 20 milliseconds to 10 seconds. Any BLE enabled device in the proximity of that beacon can receive the packet, extract the information, and fetch the content from the Internet based on the information. Figure 4 shows the procedure. The format of the BLE packet for a beacon deployed in a chain superstore is shown in Figure 2a. Every BLE data packet contains a 20 bytes long beacon ID which is divided into three sections. In this particular example, the UUID (16 bytes) represents a specific location, where the beacon has been deployed, the Major numbers (2 bytes) represent serial numbers identifying the particular sets of beacons, and Minor

numbers (2 bytes) identify the particular beacons.

Figure 2: BLE Beacon advertising mechanism.

(a) BLE Beacon detection by a smartphone.



(b) BLE sample packet format.

Store Location		City 1	City 2	City 3
UUID		88e50b28-6045-4d60-b657-d1c613436106		
Major		1	2	3
Minor	Aisle A	101	110	111
	Aisle B	201	203	189
	Aisle C	405	445	412

A traditional BLE beacon is a a tiny device which is placed physically in the place of interest. It periodically transmits BLE packets to its surroundings which notifies Bluetooth enabled devices of its presence. Each beacon transmits a universally unique identifier periodically, which can be picked up by a compatible app, or a device and sent over the Internet to the cloud server to fetch the information the beacon is broadcasting. Figure 4 shows an example of a smartphone receiving the unique identifier of content, and fetching it from the cloud. Also, it is easy for that utility server to know the exact position of the Beacon, hence, knowing the probable location of the receiving user device. This ability of precisely locating the users enables the service providers to utilize such location information, for example, if the store manager knows where the shoppers spent most of their time or the places in the mall where they can reach most of the shoppers, the management can post real-time offers or discounts through those beacons, or place advertising posts in those locations. In 2016, 93 percent of the baseball stadiums have been equipped with beacons to facilitate visitors to find seating locations, restrooms and other facilities[65]. Reports say that approximately 400 million beacons will be deployed by stores like Macy's, McDonald's, Walmart,

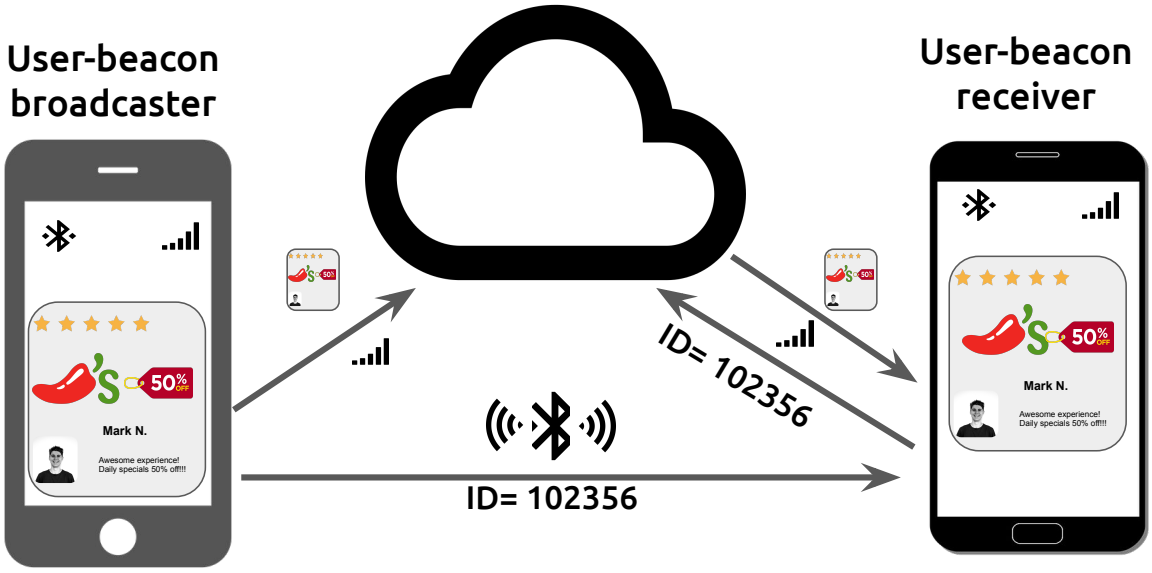
Amazon Go, Woolworths and so on by 2020 to leverage proximity marketing, and it will give the early adopters a huge boost by helping to optimize the space and inventory management[53].

BLE technology has become a very feasible and low-cost way of broadcasting information. Currently, almost 90% of mobile devices are BLE enabled [2], which creates a massive audience for companies to use this technology. However, with the vast scope, it also brings a new paradigm of privacy concerns. We can relate the privacy concerns of BLE Beacons to the privacy concerns of the usage of cookies in online marketing [14]. BLE Beacons pose similar privacy concerns as cookies in online marketing. For example, in the online world, many companies track user activities with cookies. Similarly, information gathered from beacons can be used to track user activities. Then the companies can make profiles of the users, and also can tailor targeted ads to them. Therefore, it opens a new area of research in the field of privacy. Recent research has examined the level of awareness and perceptions of users on cookies. This research shows that there has been a shortfall of awareness among the users [52, 32, 47]. Similarly, it is essential to understand the perceptions of the users about advertising using BLE Beacons regarding privacy.

1.3 Users as Beacons

The term *users-as-beacons* was first mentioned by Bello-Ogunu [14]. He introduced this term envisioning a future for BLE beacons in marketplaces, in contrast to the traditional use of BLE beacons which is only used to broadcast ads to the surroundings. In the 'users-as-beacons' system the user devices (e.g. smartphones) are turned

Figure 3: Users as Beacons.



into beacons, utilizing their BLE capabilities. We refer to each user device as a 'user-beacon,' which performs both a BLE broadcast and a BLE receive. The broadcaster user-beacon broadcasts a BLE packet having 20 bytes of a uniquely identifiable BLE ID, and information up to 27 bytes. This packet can reach up to 100 meters, the standard BLE range. When a user-beacon receives the packet, they extract the information from the 27 bytes of payload and fetch the content from the cloud identified by that information. This mechanism enables a set of nearby devices to create a wireless mesh network among them. In that network, each node (user-beacon) can forward any received BLE packets to its surroundings, and thus scales the network to a greater extent. A user-beacon can also create new content, upload it to the cloud, and share the content ID to the nearby user-beacons. Thus it enables the users to be the content creators. For example, if a user uses its user-beacon to create a new review of a store product, using this network, it can reach another user-beacon on

the other side of the shopping area. Figure 3 presents a simple procedure of how a receiver receives a BLE packet from a broadcaster, and fetches the corresponding content from the Internet.

'Users-as-beacons' is envisioned as a scalable and privacy-preserving BLE enabled platform. This platform enables an entirely localized method of user-to-user communication, within the Bluetooth range. It will be particularly useful where a user would benefit from trusting the physical presence of another user. For example, it can potentially be used as a localized user-generated review system in shopping areas. The physical presence of a reviewer who is in proximity to a user adds reliability that the review is from a real person. Moreover, a users-as-beacons system may increase location privacy, as content can spread without the user-beacons sharing their GPS locations with the system or other people [42]. Thus the users-as-beacons system is resilient against GPS spoofing and faking. We believe a users-as-beacons system can be deployed in several contexts for a variety of applications for consumer generated information and advertising.

1.4 Potential applications of a 'users-as-beacons' system

We envision various potential applications of a users-as-beacons system that can be developed on top of current BLE technology and infrastructure, including:

- *Community based social networks:* Users-as-beacons can be implemented as a community based social network, for example, a localized social network on a college campus for sharing thoughts and ideas. It can also be a way of circulating news and events throughout the community. It could also be a method

of social posting within festivals and events. It could also function as an extension of neighborhood review systems, such as Nextdoor, where people in a neighborhood can share reviews or thoughts on small businesses and services.

- *Localized advertising platform for shopping areas:* If user-beacons are deployed throughout a shopping area, current offers, coupons, or other information from a shop can spread from one point to an entire area surrounding the store.
- *Instant review platform for shopping areas:* User-beacons can review and instantly broadcast a product or an experience that can then be shared both within and surrounding the shopping area.
- *Crowdsourced localized platform for reviewing places:* Users-as-beacons can potentially be a localized instant review system for places such as restaurants, businesses, recreational facilities, and so on, similar to Google and Yelp but by crowdsourcing from, and spreading to, users in a locality.

While a users-as-beacons system can offer functionality similar to other existing social platforms or review sites, we believe this platform may provide several benefits, including

- *Trust:* We believe the platform will be particularly useful where a user would benefit from trusting the physical presence of another user. As the system would require a device to be physically present somewhere to be a user-beacon, faking a user-beacon would be a difficult task on a large scale.

- *Location privacy:* This platform enables an entirely localized method of user-to-user communication within Bluetooth range. Users need to be physically nearby another person, so the system does not require the location of the user to be tracked or shared. Thus, the system may increase location privacy, as content can spread without the user-beacons sharing their GPS locations with the system or other people [42]. The system would also be resilient against GPS spoofing.

- *Localization and potential of peer-interaction:* This system provides a unique way of information dissemination, and thus allows potential peer-interaction among nearby users. Users may be able to directly meet and talk about a comment that they might think is helpful, which would make it more reliable and further increase trust.

Yet, similar to other social platforms this system will not be fully immune to adversaries, fake posts and location tracking. While requiring a beacon will make large-scale spoofing more difficult, there is not guarantee the beacon is connected to a real person. And while GPS is not used, a user's location could still be inferred based on proximity to various beacons. Therefore, this kind of system will only be worth deploying if the benefits are valued by users, and can be understood through use of the application. Thus, to investigate the potential of users-as-beacons applications and inform the design of such a platform, we conducted several formative studies of user perceptions and interactions with such a system.

An example of the potential applications of a 'users-as-beacons' system is a crowd-

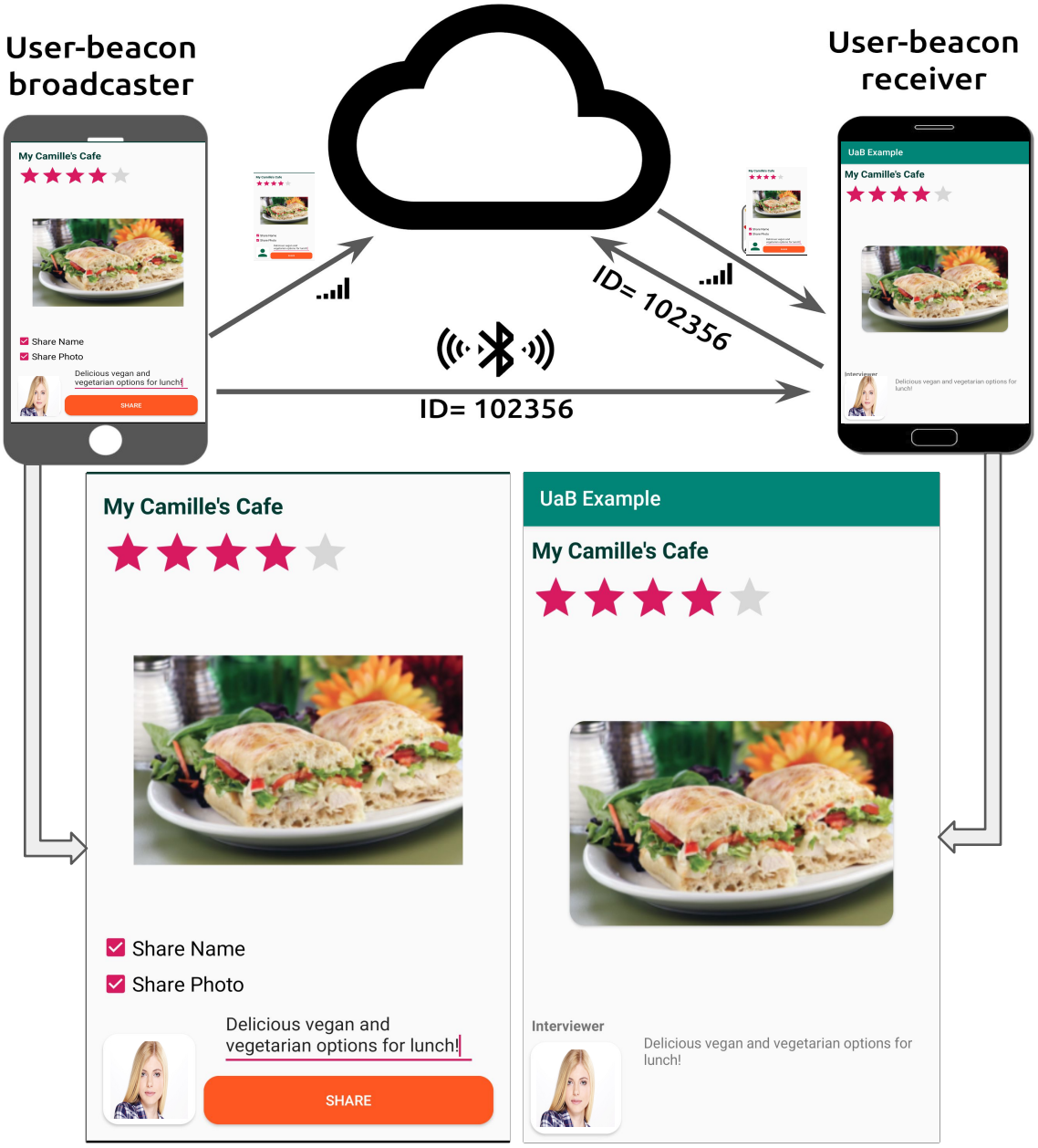


Figure 4: Example of a 'users-as-beacons' app for creating crowd-sourced and localized posts in a festival.

sourced, localized social platform, such as for sharing information at a festival. Figure 4 shows an example screenshot. In this scenario, 'Kim' visits a food festival and decides to share a picture of the food she likes. She takes a photo of her food and creates a post to share with others around her at the festival. The post's content is uploaded to the cloud. As Kim moves around the festival, her application advertises the ID of her user beacon using BLE to any other users she is near. Whenever she comes within BLE range of anyone else using the same app, their phones sense and store each other's BLE ID. The receiver would then retrieve any content related to the stored ID from the cloud. Thus, the receiver can then see Kim's post. Receivers would have their own unique repositories of posts, depending on who has been encountered. There are a variety of features one could imagine in such a system, such as bookmarking and sorting posts, endorsing and forwarding posts, and customizing when the posts are shared and received.

1.5 Thesis Statement and Contributions

My Thesis statement is, *"With BLE technology being widely available, I propose that a BLE-interaction based system called Users-as-Beacons can be built that consists of numerous user-beacons within close proximity. Users-as-Beacons can be developed to be a privacy-preserving platform for user-generated content that is communicated based on user proximity, including for localized social interactions, mobile advertising, and location-based reviewing."*

The goal for this dissertation is to propose a set of design guidelines for a privacy-preserving localized 'users-as-beacons' system and design and develop a privacy-

preserving framework for a 'users-as beacons' model. To accomplish that we explore how people think about being deployed as the user-beacons in the wild, what the privacy concerns are, how the overall user experience would be, and what desired controls and preferences the users have. I also design and develop a usable prototype, deploy the prototype, and explore the privacy policies the users would prefer. Finally, I propose design guidelines for further development of such systems for with privacy in mind.

I divided my dissertation into several parts.

1. Exploring the possibility of deploying the users as beacons system as a method of Consumer Generated Advertising.

2. Exploring the user-beacons' preferences on the disclosure of their personal information under the different levels of exposure they face in real life.

3. Exploring the general perceptions of the users, their preferred controls over the system, and desired user experiences, and the privacy concerns while being deployed as user-beacons.

4. Developing a working prototype to deploy the system in real life and investigate the research questions.

5. Deploying the user-beacons in the campus for exploring the users' reaction to peer interaction, privacy, and comfort.

6. Designing a privacy and developing a privacy-preserving design guidelines for the future deployments of Users-as-Beacons.

In order to accomplish the tasks, I performed the following activities.

1. Designed and developed a 'users-as-beacons' prototype around the idea of Consumer Generated Advertising.

2. Deployed the user-beacons with the prototype in a shopping area and conducted a research study to understand the users' preferences of the disclosure of private information, exposure to public, and the effect of product types in decision making.

3. Designed and conducted an exploratory user study to understand the potential of a 'users-as-beacons' system, the users' perceptions and preferences on such a system, and the potential benefits and challenges to develop it. The main target was to find out the initial research questions related to privacy in a 'users-as-beacons' system, and the potential design challenges.

4. Developed a working prototype to deploy a 'users-as-beacons' system in the wild as an advertising/ review system.

5. Deployed the prototype in a festival to investigate the research questions related to privacy and design of U-a-B.

6. Accumulated the results from the studies and developing a design guidelines for the future implementation of a 'users-as-beacons' system.

1.6 Contributions and Outline of the Dissertation

In this dissertation, I will describe my contributions in developing a real-life prototype for a Users-as-Beacons system. Firstly, I describe the research space in the

context of current Bluetooth Low Energy Beacons technology and social interaction technologies in chapter 2. Then I discuss my contribution on exploring the mobile users' opinions and experience as user-beacons in chapter 3. Subsequently in chapter 4, I describe my contribution on exploring the users' perceptions of being user-beacons in several potential application areas. In chapter 5, I describe the procedure of designing and developing a real-life prototype for a Users-as-Beacons system. Then in chapter 6, I describe my contribution on deploying the prototype in a festival environment and assessing its applicability. Finally, in chapter 7, I conclude with discussing the overall implications of a Users-as-Beacons system in real life, the appropriate application scenarios, the users' opinions on managing privacy, and a privacy preserving future design guidelines. Overall, this dissertation will demonstrate the viability of Users-as-Beacons as a novel infrastructure that can be used to develop social and privacy-preserving applications.

CHAPTER 2: BACKGROUND

In this chapter I will describe the state of the art related to my dissertation topic. I will primarily focus on previous research related to the application areas of Users-as-Beacons, and users' opinions of the comparable systems. Since Users-as-Beacons is a localized and potentially location privacy-preserving infrastructure, I will also describe the privacy scenarios of the various similar applications.

2.0.1 BLE applications

I am proposing Users-as-Beacons as a system built on top of BLE technology. Therefore, it is important to look at how people have already embraced this technology, as well as the privacy and other challenges that have been raised. BLE beacon technology is especially useful for indoor settings, by enabling a plethora of location-based services [22, 75]. While the technical implications of BLE beacons have been well researched, only a few researchers have examined users' perceptions and privacy needs around this technology. Thamm et al. investigated the adoption of BLE technology in retail stores in Germany [68]. They have found that although 58% of the users have experience with Bluetooth, only 4% knew about BLE beacons. Also, even after explaining what BLE beacons are, 44% of the users did not agree to the use of beacons, mainly because of the fear of misuse of the collected data, and the unwillingness of installing too many apps. Yao et al. investigated people's understandings of

BLE beacon systems by conducting a semi-structured interview. They have identified several factors, such as information flow and user knowledge about beacons system, that leads to people's understandings and misunderstandings that can bring in potential privacy risks [75]. They suggested that user education is essential as beacons usage is growing fast, and that would help to reduce the chance of overlooking real privacy problems, and mitigating unnecessary concerns. Bello-Ogunu et al. proposed a crowdsourced beacon system to improve privacy decision-making, proposing that users create a rating system to mark the sensitivity levels of particular places in a shopping area [13]. Then using that rating, users can define fine-grained policies for using particular beacons in specific places. Bello-Ogunu also briefly mentioned the idea of end users broadcasting beacons, but did not explore this idea further [14]. Thus, we are the first to provide a detailed proposal and exploration of users-as-beacons.

2.1 Platforms related to Users-as-Beacons' application areas

I am discussing Users-as-Beacons as a localized, proximity-based interaction system that has potential application for social interaction, localized user-generated advertising, localized reviewing, and crowd-sourced location reviewing. Therefore, I will discuss current literature on similar applications developed for existing platforms.

2.1.1 User generated content

As we discussed earlier, localized advertising through user generated content in shopping areas is one key potential application that can be developed on top the idea of Users-as-Beacons. This is often referred to as consumer-generated advertising. So,

it important for us to discuss the mindset of users on CGA on different platforms. Several studies show that users generally trust other user reviews of products more than the ads created by the producers, or companies. Hansen et al. examine the effects of source credibility, product involvement, and cognitive needs of consumers on the behaviors of the consumers in the context of advertising and brand attitudes [34]. They employed 175 participants to conduct an online study using YouTube. Their study reveals that participants feel that the source credibility is higher for consumer-generated ads than traditional ads. Moreover, the higher source credibility positively affects the attitude toward the ad, and interactivity. The research also suggests that the knowledge base, practical involvement, and motives contribute to the increase of user interactions. Besides, Lawrence et al. identified that user generated contents impact other users' minds via source effects and it enhances ad and brand attitudes [46]. They conducted an extensive analysis on user generated contents' effectiveness on gaining the users' attention, and the impact of multiple factors on consumers' minds. Their results also show that there is statistically significant evidence that user generated contents are more trustworthy, and thus, the people display positive attitudes toward it. Moreover, their result shows that indeed user generated contents make the users more engaged with their peers, and thus, they take user generated contents more positively, and think that they are more effective.

It is well researched that the user generated contents are more effective, hence it certainly can be leveraged to build a localized Users-as-Beacons system in shopping areas.

2.1.1.1 Privacy in user generated content sharing

To implement a proper base for Users-as-beacons, we need to discuss the privacy and user perceptions in the context of the contents generated by the user beacons. It is essential to establish the trustworthiness among the users to properly work as a user-beacon. An example of building up trustworthiness among the user-beacons can be given by describing a similar scenario in Social Networking Sites (SNS). In SNSs, like Facebook and YouTube, people utilize self-disclosure[1] to create and spread mass information about a product, service, or experience [77]. Now, in an SNS, self-disclosure can be defined as the disclosure of users' personal information, or preferences to others through that network for any monetary, or social benefits [63]. The CEO of *Intuit* Scott Cook in an interview mentioned that, it is prevalent for the traditional enterprises, such as Honda, Procter and Gamble Best Buy, and Hyatt to apply *consumer contribution* to ameliorate their customer services, improve their product line-up, and to expand their venture [60]. So, user-generated contents or self-disclosed advertising is better than firm-generated advertising. Moreover, Forman et al. found that self-disclosure increases contact opportunities, and credibility to improve future market expectations [27]. Therefore, it is imperative that when the user-beacons create contents and advertise them to the peers, self-disclosure is vital.

To understand how the users would react to a self-disclosing platform like Users-as-Beacons we need to understand what are factors that influence the users to disclose their personal information. In this part we will discuss the catalysts and factors that

[1]Posey et al. defined self-disclosure as, "Self-disclosure refers to individuals who voluntarily and intentionally reveal their thoughts, feelings, and experiences to others ."

influence the users to disclose their personal information in different platforms.

Shih et al. investigated the effects of switching cost, dependency, and cognitive trust on consumers mind to disclose their private information and preferences through Social Networks [63]. The authors defined switching costs as, the monetary and non-monetary costs involved in switching to another service provider entity. In their opinion, dependency is a lock-in mechanism that obtains a psychological cost when the customers think that they need to change the service providers, and cognitive trust is an inter-personal trust based on rational thinking To investigate the effects they ran an empirical study on 395 participants. Their results show that switching cost positively and significantly influences the participants to disclose their personal information. Their results also indicate that dependency also influences the opinion to disclose information positively and significantly. Moreover, cognitive trust indeed has a significant positive effect on participants' mind to disclose personal information. It is important to build up the trust among the users as well as the trust to the systems, because mutual trust encourages user to disclose more to the trusted society.

Alashoor et al. investigated the role of cognitive absorption[2] in the context of the privacy paradox with the effects of perceived benefits and perceived risks [67]. Their study reveals that cognitive absorption possibly leads to some negative consequences like improper disclosure of information, and reduces privacy concerns. Their analysis displays more surprising results, for example, cognitive absorption with social networks can lead to magnified perceived benefits and underestimated perceived

[2]Cognitive absorption refers to the habitual relation between the user and technology, or a system that grows over time, after hours of interaction and usage.

risks. Most interestingly, the disclosure of sensitive information increases perceived risks and makes users more prudent; thus the users deviate from the cognitive absorption and get more reserved about the disclosure of their behaviors. The authors also show that users in experiments settings and survey environment express more sensible opinions on information disclosure, however, in real life settings, the users display more relaxed behavior on self-disclosure. In summary, they have found that cognitive absorption makes users more aware of their perceived benefits and risks. Perceived benefits positively affect the opinions on self-disclosure, and on the other hand, perceived risks, privacy concerns, and information sensitivity negatively affects the opinions on self-disclosure.

2.1.2 Review systems

A localized review platform is another potential application for the Users-as-Beacons system. In traditional review systems, such as Google review or Yelp, there are numerous concerns related to fake reviews. Also, many of them introduce incentives as a part of rewarding the review creators to write more constructive reviews, thus helping the community. The current literature examined the effectiveness of these systems and the users' opinions of these systems.

Many platforms and organizations invest in incentives for reviewers, and sometimes even fake user reviews to appear competitive [10, 49]. Much research has been done on how to identify and mitigate fake reviews in various review platforms, such as Yelp and Amazon, and how the reputation of the reviewers and the quality of reviews impacts users' decisions [25, 50, 76]. In other words, for any kind of review system

the reputation of the users, and the reliability of their reviews are very important.

As mentioned earlier, one of the most viable applications of users-as-beacons is a localized review system similar to online review systems such as Yelp or Google reviews, but with reviews delivered based on physical presence that could potentially increase trust. Thus, we aim to understand the difference in user experiences between online review systems and users-as-beacons, as the latter facilitates a very different kind of user interaction. In existing research, the user experience between the reviewers is often ignored, because there is little direct interaction possible. On the other hand, in a users-as-beacons system, physical interaction among the reviewers is much more likely to occur and could be seen as both beneficial and a cause for concern.

2.1.3 SARS-COV-2 contact tracing

As the fight against the global pandemic of Covid-19 continues, the primary objective becomes to limit the spread of the SARS-COV-2 virus from human to human contacts. Some countries are using contact tracing using modern technologies to trace the actual spread of the disease and make decisions based on the spread by tracing proximal contacts people are making away from their homes. Contact tracing relies on knowing the proximity one has with other people. THus, one of the most promising technologies for doing contact tracing is BLE. And most interestingly, the approach of users broadcasting beacon ids is the method proposed for decentralized privacy-preserving proximity tracing for Covid-19 in Europe [3] and Singapore[11].

In the project named "Decentralized Privacy-Preserving Proximity Tracing"[3], the researchers are utilizing BLE signals to detect the close encounter of personal devices

to detect the probability of user-to-user contacts where a Covid-19 infection can be initiated. Privacy is maintained by only storing anonymized beacon id's within user devices, which can be matched against id's that are diagnosed with Covid-19. This system provides data to epidemiologists to estimate the spread of the disease and helps stop the further spread. TraceTogether [7] is the first national deployment of a contact tracing smartphone application deployed in Singapore utilizing the privacy-preserving BLE protocol designed by BlueTrace[11]. This protocol is functionally similar to Users-as-Beacons with extensive privacy preserving measures. These apps demonstrate the potential usefulness of a Users-as-Beacons approach. However, the applications explored here are more social in nature, expanding the need to focus on how to both preserve the trustworthiness of user-generated content along with the privacy of users sharing and consuming that content.

2.1.4 Privacy-preserving localized systems

The only privacy preserving framework for BLE so far was introduced by Bello-Ogunu et al. [13]. In that work they defined 5 types of policies for managing beacons encounters, such as a simple beacon encounter policy that enables the user to specify if he would like to opt-in or opt-out of sharing the beacon ID of a specific encounter, a beacon encounter time policy which enables the user to opt-in or opt-out of sharing the time stamp associated with a beacon encounter; the beacon encounter duration policy, which enables the user to control the length of time for an encounter being reported; the beacon encounter number policy which enables the user to opt-in or opt-out of sharing the number of times they have encountered a specific beacon;

and the beacon encounter frequency policy which enables the user to control the reporting of the rate of repeated visits for beacons. They developed a beacon privacy manager prototype to implement the framework based on these policies. They have conducted qualitative and quantitative analysis on the data collected from 90 users, and evaluated a policy manager as an extension to the Android Bluetooth protocol.

Traditional fixed beacons enable organizations to easily track location, while users-as-beacons allows for tracking proximity of users. There are different approaches to make BLE-sensing platforms more privacy-preserving by not allowing them to track the trajectory of users. For example, Higuchi et al. developed a novel privacy-aware mechanism called *Anonycast* [35] to deliver precise location information to pedestrian's smartphones leveraging the crowd-tracking systems while keeping the users anonymous. By deploying fixed BLE beacons sparsely, AnonyCast advertises location-dependent and time-variant keys. AnonyCast then estimates a subset of keys that each pedestrian's phone might receive in its path. AnonyCast uses a cryptography mechanism called CP-ABE to encrypt the keys before it gets delivered. Only the user can decrypt the information. In that way, nobody else gets the trajectory of the user, but the user gets location-precise context.

Schulz et al. developed a security concept to prevent the possibility of request tracking and forgery in indoor location tracking beacons [62]. Their mechanism consisted of cryptography algorithms and over-the-air signature transmission techniques to salt the beacon data in order to provide the users with secure and privacy-preserving contexts in transportation systems. Gao et al. developed a privacy-preserving framework for ubiquitous devices called TrPF [28]. TrPF intends to preserve user privacy when

the devices are deployed in a participatory sensing environment. They implemented a mix-zone model with considering the time factor from the perpective of graph theory. A Users-as-beacons could learn from such examples to prevent users from inferring location and trajectories of other users they encounter within the system.

Many research works have been conducted to develop privacy-preserving frameworks in other platforms like Desktop and Mobile. Projects like Adnostic and Privad [70, 31] keep the personal profiles locally, and keeps a local ad rendering engine, that renders the ads from a cloud ad network to target the local personalities. A similar idea has been implemented using a local pool of ads in the mobile platform in MobiAd[33]. Several other research works such as ProfileGuard [72] focus on Android permission systems and flow-tracking mechanisms to prevent third-party apps from inferring user interests. We will now discuss some of these frameworks, to understand how users' perceptions on privacy played a role in designing the frameworks.

The primary concern of the users on targeted advertising is the loss of privacy to the third parties. As soon as personal data goes into their hands, they start using the data and selling it to other parties. So, to prevent that Toubiana et al. proposed a privacy-preserving targeted advertisement framework [70]. This framework allows the users to share only a well-filtered version of their profile. The detailed personal profiles are kept locally and based on the profile, the local agent downloads the appropriate ads for them. The prototype developed by them include a Firefox extension having two modules: profiling module, and ad-rendering module. The profiling module tracks the user activity to create a detailed profile of them. It builds a detailed list of interests inside the browser. Using this list of interests, the ad-rendering module searches the

ads appropriate for the user and downloads them. If the user clicks on an ad, their billing module takes care of it to make sure that the profile information does not get shared with the ad networks, but the information related to the number of clicks gets shared.

However, to deploy it in a real-life scenario, the ad networks need to change their way of serving ads. Guha et al. developed Privad [31] which also follows a similar pattern to protect user privacy. This framework works with four modules: client, dealer, monitor, and broker. The client downloads the appropriate ads from the broker server based on the user profile. The dealer protects the user privacy by acting as an anonymous proxy staying in between the client and broker. Also, the communications between the broker and the client are encrypted with a public key mechanism. On top of everything, the monitor restricts the client to connect with the broker using any covert channel. Another framework named MobiAd[33] takes the same approach to implement it into mobile platforms. It creates a pool of ads locally that match with user's interests, and makes sure that the ad network only gets the aggregated information of all the users as a filtered out form. Advertising types of systems built on users-as-beacons would need similar mechanisms for organizations to track ad interest, yet also reduce user profiling and tracking.

The majority of the customers who use mobile platforms to browse the Internet and social networking apps, have a common concern of being tracked by several apps [72]. Ullah et al. proposed a mechanism called ProfileGuard [72] to obfuscate third-party mobile apps which track the user activities and infer user interests. ProfileGuard is a mobile app that analyzes the data from the installed apps to properly obfuscate the

apps to protect user information. They developed an Android app to let the users have the authority to customize their interest categories. The ability to customize personal interest categories inherently protects users' interests getting exposed. ProfileGuard can analyze the information of all the installed apps on the mobile device and suggest the potential vulnerabilities regarding profile information sharing. Then it suggests the candidate apps that obfuscate personal information. The user then can download and install the apps, so that the ad networks cannot identify the users' real interests. The list of obfuscating apps is generated following two strategies; first, finding several apps that match the user privacy preferences, and second, selecting apps that match user profile interests. Lantz et al. developed an Android application sandbox named Droidbox [9] which monitors the installed apps' behaviors and provides a timeline view of their behavioral patterns for identifying malicious behaviors. It can actively protect the user from unwanted personal information. Liu et al. developed a complete framework to solve several problems and concerns such as reporting view/click information to the ad networks evading them to collect personal interests information, deceiving click-fraud mechanisms of the ad networks, providing a proper platform for the advertisers where they can gather enough information to provide tailored ads without tracking the users directly, and most importantly, building a trusted platform for the users [48]. They also focused on solving authentication issues, and permissions dilemma in their platform. Again, similar solutions may need to be developed to address user profiling and tracking with a Users-as-beacons system.

Along with the use of the platforms mentioned above, the usage of ad blocker programs are increasing day by day. Ad blockers are applications, mainly in the form

of browser extensions to block ads from appearing on the web pages. A PageFair report suggests that ad blocker usage increased 30% in 2016, where there were 615 million devices which were using ad blockers by the end of the year[45]. In that report, their poll results show that 30% of the 4,626 surveyed users install ad blocker software due to malware concerns, and 29% of them use ad blockers to avoid interruptions. The most important finding of the study was that ad blocker users use the blocker only for the problems with the digital advertising delivery methods, not the digital advertising itself [51]. There are several popular ad blockers currently available in the market, such as AdBlock, JBlocker, Ghostery, uBlock, and so on. In general the technique utilized by these ad blockers is to create a database of ad servers and providers, and blacklisting them. Some of them give the users the opportunity to create their own filters according to their preferences. One of them, Ghostery is specifically designed to block the behavior trackers using a blacklisting database. It informs the users about the tracking, and gives them independence to set their preferences.

Now we turn our focus to BLE enabled devices. The common types of maintenance issues we face in current BLE equipped devices are the lack of ability to upgrade the firmware Over The Air (OTA), poor update distribution network from the vendors, and the lack of financial resources to maintain the devices after deployment [36]. That poses a serious security threat of the privacy being compromised. Due to poor design or implementation, BLE advertisements leak a substantial amount of information. Adversaries can now profile, track, or fingerprint the users' activities. To prevent these issues, Fawaz et.al. proposed a privacy protecting system called BLE-guardian. This system equips the user devices with the control over the devices from those

who discover, scan, and connect to their devices. With Users-as-beacons, many of these concerns are mitigated as the beacons are on users' mobile phones, and can be regularly updated and controlled by users.

2.2 Privacy in similar contexts

Users-as-Beacons is aimed to be potentially a location privacy-preserving platform for localized user interactions. Hence I will now discuss the literature that investigate the privacy management of similar contexts, such as location tracking, behavioral tracking, targeted content delivery, and so on.

2.2.1 Location-based systems

For the past few decades, researchers have been putting a lot of effort to analyze and resolve the privacy issues related to location-based technologies [20, 44]. With the broad use of GPS-enabled mobile smart devices, the popularity of location-aware applications has been increasing. Now, almost every location-aware app can track the location of the user, and tailor appropriate services to the users. For example, a car buying mobile application needs to use the location of the car buyer to find the best deals nearby. However, there is a trade-off of compromising privacy. The same application can easily track the location of the user, and sell it to the third parties, like ad networks. Consequently, right after searching for a car in a car-buying app, if the user logs in to Facebook, there is a high probability of seeing an ad there related to the best car deals nearby. As a result, people naturally feel the privacy threats from location tracking systems.

Fawaz et al. surveyed 180 smartphone users, recruited through Amazon Mechanical

Turk, and social media platforms, to understand their perceptions. 78% of the users believe that apps accessing their location can pose privacy threats, and 85% of them care about who accesses their location information [24]. Also, 52% of the users feel that it is OK to provide an imprecise location to protect their privacy. Another survey conducted by a team at Microsoft on consumer awareness of location-based services and privacy implications depicts some interesting results [17]. They surveyed 1500 people in the U.S., United Kingdom, Canada, Japan, and Germany to evaluate their perceptions. 51% of the users use the location-based services regularly. 94% users who use the location-based services think that it is valuable. Coming to the point of privacy concerns, 84% of the users are concerned about identity theft while sharing location, and 83% of them think that they lose privacy. Interestingly, 49% of them agree to share their location, if they can manage and control the entities who can see their location information. Users-as-beacons could enable location-based services without sharing precise location through GPS, and thus could potentially alleviate some of these concerns.

Movement tracking in superstores is gaining popularity among the companies. OpinionLab wanted to know the shoppers' perceptions on in-store monitoring by companies [57]. They conducted a study among 1042 consumers. Their research shows that 80% of shoppers refuse the idea of their movements being tracked via smartphones. The top privacy concerns raised by the users are data privacy (68.5%), and spying (67%). Interestingly, even if the retailers promise to the consumers that the acquired data will only be used to improve the customer-experience, 88% of the users do not change their mind toward movement tracking. Moreover, they expect

the retailers to provide price discounts (61%), or free products (53%) if they agree to be tracked. In a different survey conducted on 200 people, Fawaz et al. found that people are generally concerned about potential leakage of personal information due to location tracking in stores [23]. 61% of the participants wanted to prevent location tracking entirely, 24% of them wanted to allow some part of tracking, and 15% wanted to enable full location tracking. The most prominent privacy-oriented reasons behind rejecting location tracking were lack of trust in the store (49%), lack of comfort with their mobility information being gathered (43%), and lack of incentives in exchange for the personal data (41%).

Users-as-beacons leverages users' capability of socializing with other users in a mobile environment; hence, it is essential to explore the users' perceived comfort around others, concerns on data dissemination, behavioral tracking, and privacy perceptions they have. In current social platforms, users are getting more concerned over time about their data privacy, even while they are sharing significant amounts of information with other users [16, 43, 73]. As a result, we have seen the increased utilization of privacy settings and users have become more cautious about social interaction on popular platforms [40, 64]. BLE technology is currently used to provide location-based services. While a users-as-beacons system is not dependent on estimating location and would not require the collection of location data, the system could still potentially infer location and users may still perceive the system as a location-based service. Early studies found that location-based mobile services are privacy intrusive in many users' opinions, and users want granular control over location settings [37, 18, 61]. However, over time these concerns may fade, and people have become comfortable sharing

their location with their friends and other users provided that they have control over location sharing settings [15, 69, 54]. In contrast to sharing location to friends, users remain concerned about sharing their locations with advertisers, and third parties [41, 26]. Yet, despite these concerns, many users regularly share their location with applications, perhaps due to their lack of awareness of the extent of location tracking [15]. Thus, we can expect similar location concerns in users-as-beacons, with users expressing concern over advertisers and third-parties potentially knowing their location, yet still being willing to share their location with other people and organizations to gain benefits.

2.2.2 Behavioral tracking in social and advertising systems

Marketers and vendors have been using users' purchase data to analyze and track their behaviors and characteristics for almost three decades. Three decades ago, these data were gathered and used only by the direct marketers. That scenario began to change in the 90s when the retailers, manufacturers, service providers, and non-profit organizations started collecting individual-specific information of users regularly [19]. Analyzing several surveys, we can say that users are generally concerned about what the companies know about them, how the companies gather their personal information, and how accurately they exploit the information [55, 66, 59]. According to the previous surveys, users are fond of privacy protection measures, such as restrictions on information exchanges [55]. A Consumer Union poll shows that 72 percent consumers are concerned that their behaviors were being profiled by companies [39]. Another study shows that among the 50 most visited websites, most of them use personal

information for customized advertising. Moreover, numerous tech giants like Google, Microsoft, and Facebook share their collected customer data with hundreds of companies [29]. Besides, another survey conducted with 786 American users finds that 84 percent of the participants expressed increased concerns of their personal data being lost or stolen [56]. Therefore, we can see that it is a matter of great concern to share personal information to the companies.

However, in the minds of most American people, the privacy issues in commercial settings are contextual and depends on several factors. A recent study done by Pew research center [58] shows that among 461 adult participants and nine focus groups of 80 people, most of them would share personal information or permit surveillance under a variety of circumstances, such as in return for getting incentives. For example, in that study, they found that 54% of the participants think that it would be acceptable for employers to install monitoring cameras following a series of thefts. Moreover, 47% of them said that it is acceptable to share information in return for incentives received from retail loyalty cards, compared to 32% who said that it is unacceptable. In contrast, in a different context, most Americans do not wish to share personal information. For example, if they are offered a smart electric meter that reduces their energy bill, but monitors their movements in the house, 55% of them do not like this trade-off. From this study, 4% of the participants would accept all of the deals where they need to share information and, 17% of them would not take any deal. Most importantly, the vast majority would accept at least one of the deals. It drives us to dig deeper into consumers' minds to perceive their opinions on privacy, their trade-offs in return for incentives, and their reactions to different levels of exposure.If

Users-as-beacons is used for reviews and advertising, we will need to understand how users perceive the tracking through such a system.

2.2.3 Targeted and tailored contents in social systems

The idea of Users-as-Beacons comes up with two-fold communication. Firstly, consumers generate content for sharing their opinions to the public. Secondly, consumers receive content from their peers. That is how the trusted community of user-beacons grows. Now, to build up a trusted community among the users it is needed to think carefully about privacy. In this case, it is important to look at privacy issues from both providers' (user-beacons) and the receivers' perspectives. Again, the concept of Users-as-beacons is thought of a powerful utility to the vendors and service providers. Now, to maximize the utilization of this method, the service providers, vendors, and retailers will focus on personalized advertisements more and target the users at the receiving end with tailoring the ads towards them based on their personalities. To tailor ads towards the targeted user, the companies generally collect and compile the record of purchase or other activities, interests, communications, and preferences and analyze them to find out the characteristics of the user and create the persona. Based on their analysis, they create personalized ads and send them to the users. In the advertising scenarios of users-as-beacons, we can clearly see an implementation of targeted advertisements can maximize the utility of the companies. However, from the birth of the idea of targeted advertisements, there has been a strong criticism against it regarding the concerns about invasion of individual privacy [74, 38]. Recent research works show that most of the people would not accept targeted ad-

vertisements by trading off their privacy, and only a third of the participants agree to accept targeted advertisements by trading off their privacy[21].

A research study [71] done by Turow et al. indicates that American marketers' claim of Americans giving out personal information themselves as a trade-off for benefits they receive, is misrepresenting a large portion of Americans. Their survey interestingly points out that most of the Americans do not agree with the phrase 'data for discounts' is a square deal. 77% of the participants strongly disagree that if companies give them a discount, it is a fair exchange for them to collect information about the customers without their consent. Moreover, 53% of them strongly disagree that it is fair for an online or physical store to monitor what the customers are doing in exchange for letting the customers use their facilities like WiFi for free. Furthermore, 55% of them disagree that it is okay if a store creates profiles of the customers to improve the service they provide to them. Most interestingly, only 4% of the participants agree with all three of the propositions. Only, 21% participants said that they would accept discounts in exchange for their personal data. Now, their study took an interesting turn when they presented a real-life scenario with the detailed view of how a supermarket collects customers data to improve the service, and in exchange, they provide discounts to the customers. 43% of the participants support discounts by trading-off their data. Further down the study, they found some more interesting facts. 49% of adults who use the Internet incorrectly believe that by law a supermarket is bound to take permissions from the customers before it gathers information about them. 69% people do not know that the pharmacy does not need permission to sell customers' information about the drugs they buy to

third parties. 65% think that a website that has a privacy policy will not share their information with other websites and companies without permission. 62% of them are not aware that it is not legally required for the price-comparison sites like Orbitz, or Expedia to include the lowest travel price. These data provide vital information about how little awareness most of Americans have regarding the ways marketers use their information. A large portion of the American consumers believes that the government protects them from discriminatory pricing. Most importantly, most of the Americans do the costs and benefits choices for trading-off their personal information based on incorrect information. These perceptions will also be important in adoption of a users-as-beacons system, particularly since the system will only work with sufficient users being nearby each other. If users feel they are being unfairly tracked or their information is being misused, they may choose to not use the system and reduce its utility.

2.3 Summary

In this chapter, I have discussed state of the art research related to my research area. We discussed BLE technology and its contemporary usage and the users' general perceptions on the BLE based systems. We also discussed the present privacy preserving frameworks related to BLE and other social and location-based platforms. Finally, we compiled the research about the privacy scenario throughout the location-oriented technologies, user-generated contents, targeted and tailored contents delivery, and behavioral tracking. These results demonstrate that while users express many concerns over their data being used to deliver content from organizations, users also value and

trust interacting with other people. In this dissertation we build upon this related work to examine the perceptions of users in a novel system, and the potential benefits the system could provide.

CHAPTER 3: EXPLORING MOBILE USERS' OPINIONS AND EXPERIENCE WHILE BEING DEPLOYED AS ADVERTISING BEACONS

3.1 Introduction

In this chapter, I describe how we designed and developed a design-probe to deploy users as mobile advertisers to explore the CGA capabilities of the users-as-beacons system. We also investigated the user experience of the mobile users based on the products they would advertise in a shopping mall being employed as advertisers. We defined these mobile advertisers as user-beacons. We conducted a role playing user study in the campus bookstore to explore the impact of sensitivity of the products on the user-beacons, the reaction to the exposure the users will face, and the possibility of getting influenced by the other user-beacons around. Before we get into the actual experiment, we need to rephrase the related aspects of our model. In this model, the retail shop broadcasts ads using the web of mobile users equipped with BLE enabled devices. Every mobile device can work either in relay mode or independent advertiser mode. In relay mode, a mobile device only works as an ad-post for the company; the user there does not know about anything that is being broadcast through their device. In contrast, in the independent advertiser mode, the user gets to know what ads are being broadcast through their device. It can be enhanced to a certain level where the user will have control over which ads to be advertised, and how much information will accompany them. An important step of employing user-devices is to identify what

the mobile user will get in return for being an advertiser. In our experiment scenario, we implemented a point based rewarding system for the users.

To design our experiment model, we can think of a scenario where a store gives its customers a mobile application to use. The customers then can surf products, post reviews of them, and can even advertise them along with their honest reviews. In this scenario, each of the users becomes an advertiser for the store. In return, the store provides some incentives in forms of points, or store credits to the users. It creates a win-win situation for both the vendors and consumers. The first goal here is to create a distributed platform for the stores to advertise their products. Secondly, the users have a reliable way of receiving honest reviews of the products from other users. Most importantly, the stores can manage their inventory very well if they get reliable reviews from the consumers. They can decide on selling different kinds of products based on the consumers' choice and comfort. However, the primary challenge here is to ensure the trustworthiness of the consumer reviews. To make a review trustworthy, the reviewing consumer should share a handful of personal information, such as the name, photos, experience with the products and so on. Sharing personal information is a concern for the users because of several factors, such as the sensitivity of the product, the exposure to the public, the level of knowledge on ad networks, the chance of incentives, and so on. Also, the store can track the users to target appropriate ads to them. That brings privacy concerns related to tracking and targeted advertising. Goodwin et al. did a survey where participants were asked to describe a product or service that they would not want most friends/relatives know they purchased. Most of them replied with sensitive items such as alcohol, tobacco, cosmetics, etc. Therefore,

a person is worried about the sensitivity of the products as well as being tracked[30].

We developed an Android application to employ the user-advertisers in store. The application was designed to give the users control over the store ads; for example, before advertising, the users could decide what ads they wanted to advertise and what specific personal information they wanted to share. We wanted to look into consumers' minds to find out what are the things they are comfortable to share based on various surrounding conditions. In this case, we primarily tried to find the consumers' perceptions based on two key factors: the sensitivity levels of the products, and the degree of public exposure of private information. We also wanted to see if they got influenced by the opinions of other users. We conducted the user study in our school's bookstore. The users completed several tasks using our mobile application. Our first analysis shows that statistically, it is evident that the sensitivity level of a product affects the consumer's opinion to share their private information. However, we cannot find enough statistical significance to state that the public exposure level of the private information through advertisements affects the users' opinion to share his/her personal information. Finally, we tested if the opinions of other users possess any impact on changing consumers' mind, and we found that, although the other users' opinions do not significantly influence consumers' minds to share personal information, there are confounding effects that should be addressed to understand the issue correctly.

3.2 User Study Design

The university's Internal Review Board approved our study. We submitted the whole plan with the full transcript of the procedure to the IRB before we ran the study. There were 102 participants in the study. In this study, we want to answer several questions. Firstly, do the users feel more reserved to share their personal information along with a sensitive product than with a not-sensitive product? Secondly, does the level of exposure to the public have any effect on sharing personal information? And thirdly, do the users get influenced by the other users who are also sharing their personal information? To find out the answers, we designed a real-life experiment having a 2x3 between subjects test in mind. We conducted our user study in our on-campus book-store; figure 5 shows a map of the bookstore and the placement of different types of products. Although the store is primarily a book-store, they sell a variety of products including souvenirs, athletic apparels, essential apparels, health and beauty products, and so on. The bookstore is a popular destination for the current and former students, faculty, staff, and visitors. So, it is one of the most convenient places on campus to get the opinions of consumers having a diverse background.

To build up our real-life scenario, we developed an Android application which can broadcast information to the users nearby. It can also receive information from the other users as well as the company server. We have integrated the user-control over the information, i.e., deciding what personal information to be shared, that the user devices broadcast. Our testbed was the on-campus bookstore, so we built

Figure 5: Experiment Testbed, the Bookstore.

our application as if the store created it. The products to create ads were selected from the actual products the store sells. We advertised for our user study for two weeks circulating fliers on campus, using e-mailing lists, and announcing to several classrooms. We also recruited on-the-fly, requesting the visitors at the time of the experiment. We created the utility to the users by introducing incentives here. The more personal information and ads a user shared, the more points they earned, and finally, the user redeemed a Starbucks gift card based on the points he earned.

We divided the participants into three groups:

Control Group (Group 1): this group of participants did not receive any ads from

the other user devices. They only received the ads which are provided by the store. They could customize the ads by adding their personal information, product reviews, and advertise the ads.

Low-exposure Group (Group 2): the participants from this group did the same thing as the members of the group 1 did. The main difference was that these users received notifications of the ads advertised from the other users, and could see and review the ads. The hypothesis is that receiving ads from the surroundings makes the user aware that the ads they advertise would be received and seen by the other users. Still, this awareness does not create the feeling of public exposure much, so we call it the low-exposure group.

High-exposure Group (Group 3): the participants in this group not only received ads from the surrounding users as in Group 2, but also, their ads and other ads were displayed on a large TV screen that was visible to the participants and shoppers at the bookstore. We used the big advertising screens of the bookstore to display the ads the participants created. In this case, the users felt high public exposure, because, even those who were not participating in the study but were present in the store, could watch the ads on the screens. To examine the influence of other users on how much personal information a user wants to share, we divided both low and high exposure groups into two sub-groups each:

Group A: we injected broad-minded artificially tailored ads to manipulate the thoughts of the users. Broad-minded ads are the ads of potentially sensitive products shared with some personal information; like women undergarments, shared with all personal information like name, profile photo, and so on. These ads were received by the par-

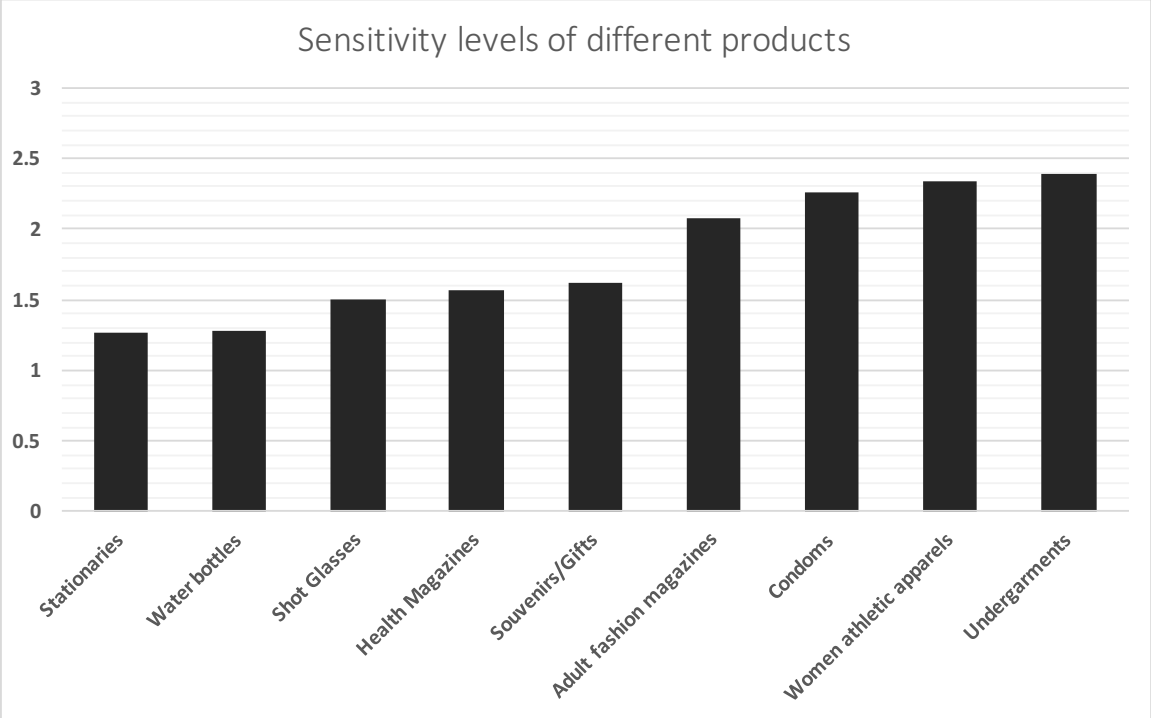
ticipants in this sub-group as if the other users broadcasted them.

Group B: in this case, we injected narrow-minded artificially tailored ads to influence the users. Narrow-minded ads are precisely the opposite of what broad-minded ads are. An example of a narrow-minded ad is an ad of a pen without any personal information shared with it. Both the broad and narrow-minded artificial ads were created manually and injected into the ad-pool of users' ads. To make sure they received the injected ads, these ads were put at the beginning of the ad-pool.

Each of the participants was given five not-sensitive and five sensitive products of the store to advertise. They were also given five more products, which were in between sensitive and not-sensitive, but for the sake of avoiding subjectivity, we did not consider them in our analysis. As they were customizing and advertising the ads on behalf of the store, they were generating consumer-generated ads. In each of the products, they had the options to share their name, profile photo, product review, and rating. They could even decide to advertise the product or not. Based on how much information they shared, they earned points. We divided the products into two types: not sensitive and sensitive. To determine the appropriate products for each category, we ran a small survey of 61 participants. The survey transcript was, *"Imagine you are in a superstore, roaming around to shop. There are products of numerous types. The superstore tracks your activity to improve your shopping experience. There might be several sensitive products for which you may not want to share the purchase information. Please rate the following products based on how sensitive they are in your opinion."* There were several types of products, such as stationaries, water bottles, souvenirs/gifts, women athletic apparels, shot glasses, health magazines, undergar-

ments, adult fashion/entertainment magazines, and condoms. For each product, there was a photo and three options to select from: not sensitive, neutral, and sensitive. We enumerated not sensitive, neutral, and sensitive as 1, 2, and 3 respectively took the average and then sorted them into three sensitivity levels. Figure 6 presents the summary of the results. Based on this survey we classified stationaries and water bottles

Figure 6: Sorted sensitivity levels of store products



as not sensitive, shot glasses, health magazines, and souvenir/gifts as neutral, and adult fashion/entertainment magazines, condoms, women athletics apparels, and undergarments as sensitive products. To avoid data mix-up for the sake of the analysis, we avoided analyzing neutral products in the main user study.

The study was conducted in several phases. First, the users signed up to the system using the application. Next, they were instructed to roam around the store, and

Table 1: Demographic Summary of the participants

Gender	%	Age	%	Education	%
Male	65.6	18-24	56.86	Bachelor	40.4
Female	34.4	25-34	41.18	Some College	34.6
		35-54	1.96	Graduate	11.5
				High School	10.6
				Associate	2.9

use the application. While walking through the isles, they received ads from others. They had five ads for each type of products, which they could customize and advertise. After they finish advertising, they logged out and returned the mobile phone. Finally, they filled up a complementary survey and redeem their points as a Starbucks gift card. The complementary survey included three sections: background and demographic questions, technical expertise related questions, and generic questions related to sharing personal information. There were 102 participants in total. Table 5 shows the demographic summary of the participants.

3.2.1 Hypotheses

We wanted to examine the following hypotheses:

- *The sensitivity level of a product affects the participant's opinion to share their personal information.*
- *The level of public exposure of personal information through advertisement affects the participant's opinion to share their personal information.*
- *The ads received from the other users influence the user's opinion to share their personal information.*

We also tried to find out the general perception of the exchange of information among

the participants. Finally, we tried to understand, if they did what they believe, or, we could change their mind by giving them incentives.

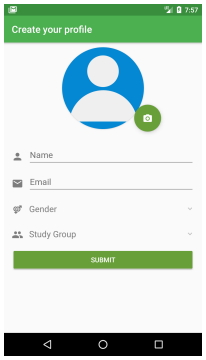
3.2.2 User Study Flow

Every participant began the task by registering their profile in the Android application putting their name, profile picture, email, gender, age, and the group randomly assigned to them. We conducted the study for the control and low-exposure group together, while the study for the high-exposure group was done on different days. We provided the participants with the devices. A short demonstration of the application was given before they start the task. After the demonstration, we gave the device with the actual application installed to them and instructed them to explore the store, advertise the products they have in their application, and watch the ads they receive from the other users. The task needed 30 minutes to complete on average. Figure 10 displays screen shots of the mobile application that was developed to conduct this study.

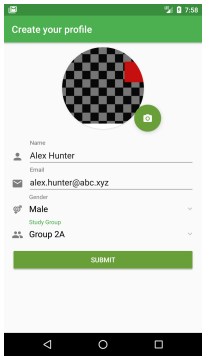
In the beginning, The user is first asked to signup into the application as shown in Figure 3(a-b). The signup process asks the user to provide their name, password, and a face shot of themselves. After the sign-up, the user is then asked to browse the main menu, where they find two options: *Ads to advertise*, and *Released ads*. Clicking on *Ads to advertise* takes the user to the sliding screens of 15 products they can choose to advertise from. At first, every product only contains an image of it along with a description. Now, for each of the products, the user can customize the contents of the ad; for example, they can release four information along with each

Figure 7: Screen-shots of the application and in-store big screens.

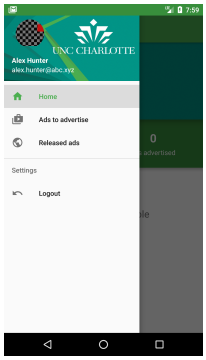
(a) Sign Up Screen



(b) Take photo, and fill up to register



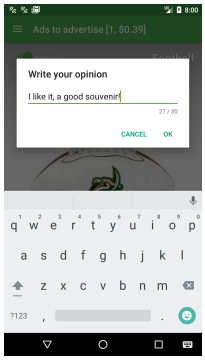
(c) Menu options



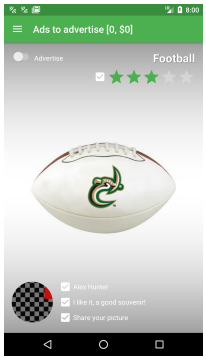
(d) Notification received at the top

(e) Clicked on a notification to see the Ad received

(f) Writing an opinion for the product



(g) Customizing ads before advertising



(h) Advertised, and earned points

(i) Released ads screen to see advertised ads

(j) Another example of a customized ad.

(k) Advertisements in store big screens for group 3.

ad, such as the name of the participant, profile picture of the participant, personal comment on the product, and rating of the product. The most personal information here is name, and profile photo. We also included personal comment and rating to make the user feel that they are contributing to the community and also helping the store management. All the four information are optional, and the user can choose the option(s) from them and share along with the ad. The more information they share, the more points they earn. Finally, once they switch the *Advertise* button on, the ad becomes public. They do not earn any extra point to turn *Advertise* button on. If they do not turn the *Advertise* button on, they earn no points for the ad. For groups 2 and 3, the participants also received notifications of received ads from the other users. Figure 7d displays an example of notification, a user receives. Clicking on the notification takes the participant to the *Ads received* screen. To get back to the *Ads to advertise* screen, the user needs to use the menu again.

Our application can handle three groups of users. We generated 20 artificially tailored ads for each of the two kinds of ads, i.e., broad-minded and narrow-minded, and queued them for groups 2A, 2B, 3A, and 3B. For groups 2A, and 3A, the participants received broad-minded ads, and for groups 2B, and 3B, the participants received narrow-minded ads. Figure 7h shows that once the participant advertises a product, based on the information they shared with the product, there is a certain amount of money added as points earned. The user can make from USD $0 to $10. To avoid the possible user bias to the store in return for the incentives, the rating and good comment do not carry any extra points. Even if the participant rates the product very low, they receive the same points as the participant who rated it five

stars. Thus we made sure that even if the user criticizes the product, the store pays them for their honest reviews. The honest opinion of the customers eventually helps the store too, for better understanding the needs of the customers, and for managing their inventory. For group 3, we dedicated the entire three days of the user study. We used in-store advertising screens, to display the ads advertised by the users. Figure 7k shows the advertisements displayed on the big TV screens in the bookstore, note that three advertisements were displayed at any given time to fill the big screen TV display.

After a participant completed advertising the selected ads, they were asked to fill out a survey form generated using Google Docs. Then, we checked their application to see how much they earned by advertising. We paid them the amount in the form of Starbucks gift cards. To summarize, our study focused on three key factors: sensitivity levels of the products (not sensitive and sensitive), the exposure level felt by the participants (low exposure and high exposure), and. Participants actively explored the store and used the app to advertise products and earn points. After finishing the advertising task, they answered a survey. We paid the amount they made in the form of Starbucks gift cards.

3.2.3 Analysis Procedure

In this study, our primary focus for this analysis is to measure the effect of products' sensitivity over consumers' minds to share their personal information in the context of CGA with incentives; controlled for public exposure. We designed a 2x3 between subject test to understand the effects. The change of opinion is represented by the

Table 2: Descriptive statistics of information shared for various conditions

Condition	**Control group**	**Low exposure**	**High exposure**
	N		
Not Sensitive	30	31	41
Sensitive	30	31	41
	Mean points earned (μ)		
Not Sensitive	3.19	3.18	3.49
Sensitive	2.58	2.92	2.94
	Standard Deviation		
Not Sensitive	0.94	1.02	0.76
Sensitive	1.19	1.29	1.28

percentage of information shared by the participants. Also, we ran the analysis to test the effect of public influence over the change of mind of the participants. Furthermore, we conclude with analyzing the general perceptions of the participants about privacy, their knowledge of line and retail marketing and usage of private information there. We analyzed their opinions of sharing personal information with increased levels of information sensitivity.

3.3 Results

We analyzed the application usage of 102 participants. The demographic breakdown is shown in 5. 34.4% of participants were female, and 65.6% were male. Regarding age, 56.86% of them were between the ages 18 and 24, 41.18% were between 25 and 34, and the rest of them were of ages between 35-54 years. Also, the main level of education completed by the participants mostly includes Bachelor's degree (40.4%), and Some College degree (34.6%). The rest of the participants completed their Graduate studies (11.5%), High School (10.6%), and Associate degree (2.9%). Table 2 shows the descriptive statistics breakdown for our 2x3 between subject test.

Table 3: Test of Normality

Sensitivity	**Exposure**	**Shapiro-Wilk**	***df***	***p***
Not sensitive	None	0.828	30	0.000
	Low	0.798	31	0.000
	High	0.702	41	0.000
Sensitive	None	0.903	30	0.010
	Low	0.804	31	0.000
	High	0.801	41	0.000

Paraphrasing our goal, this user study was designed to evaluate the effect of the sensitivity of the products on user's opinion to share information, controlling for the public exposure they feel. We measure the information a user shared by the points they earned. Before we proceed to the analysis, we should make sure that our data meet the requirements and assumptions for running the tests. From Levene's test of homogeneity of variance we see *F(5, 198) = 4.132, p = 0.001*. That means that there is a statistically significant difference among the variances. So, our data cannot satisfy the assumption of homogeneity of variance. Next, we look at the Shapiro-Wilk test of Normality. From table 3 we can see that the assumption of Normality is also not met. Linear regression was conducted with Mean Points Earned as the dependent variable, Sensitivity, and Exposure as independent variables to save the Mahalanobis distances. The smallest p-value of Mahalanobis distance is 0.04, which is greater than 0.01, so there is no bi-variate outlier. We can see that although there is no bi-variate outlier, the assumptions of normality and homogeneity of variances do not meet. Since our population does not ideally represent the society, the assumption of homogeneity of variances is expected to be not met. So, we have to keep this limitation in mind when we interpret the results.

Figure 8: Examples of artificially tailored ads.

(a) Broad-minded ad

(b) Narrow-minded ad

3.3.1 Effect of Product's Sensitivity Level

The first hypothesis we want to evaluate is that the sensitivity level of a product affects the participant's opinion to share their personal information. To test the hypothesis we need to look at the results of 2x3 between subject test. Before we run the analysis, we need to explain how we quantified shared personal information. Each of the participants was given five not-sensitive and five sensitive ads to advertise. At most 4 points could be earned from each ad. Sharing each of the information (name, photo, rating, and comment) carried 1 point. For each of the participants, we took the means of points they earned for both not-sensitive and sensitive products. The means represent the information they shared for both kinds of products. Table 2 shows the mean points earned for both types of ads.

Our test results shows that, the pattern of differences on mean points earned between the sensitivity levels are not significantly different with different exposure levels, *F(2, 198) = 0.463, p = 0.630, partial* η^2 *= 0.005*. However, our result shows that there is a significant difference on mean points earned between the sensitivity levels of the products, averaged across several exposure levels, *F(1, 198) = 9.236, p = 0.003, partial* η^2 *= 0.045*. Thus, we can primarily decide that there is statistically significant evidence to prove that, the sensitivity level of a product affects the participant's opinion to share their personal information, which means that users are willing to share more of their information when advertising less sensitive ads and less of their information when advertising sensitive ads.

3.3.2 Effect of Exposure to Public

Now, we look at the next portion of our analysis. In table 2 we can see that the mean points earned are almost identical in control and low-exposure group for not-sensitive products, although there is a slight difference in the high-exposure group. For sensitive products, there is a slight difference between the mean points earned in control and low-exposure group; however, the means are almost the same between the low-exposure and high-exposure groups. In all cases, the high-exposure group has the highest points earnings. Our primary findings on mean differences got reflected in the between-subjects test result. There is no significant difference on the mean points earned among the exposure levels, averaged across the sensitivity levels, *F(2, 198) = 1.591, p = 0.206, partial* η^2 *= 0.016*. So, we primarily decide that the level of public exposure through advertisement does not affect the participant's opinion to

share their personal information.

3.3.3 Effect of Public Influence

We mentioned earlier that we tailored some ads that the participants received from other users to replicate public influence. The idea of broad-minded artificial ads is to share more information with a sensitive product. In contrast, a narrow-minded artificial ad contains very few personal information along with an ad. Figure 8 shows examples of broad and narrow-minded ads. Here, we wanted to measure if there is any statistically significant effect of different types of injected ads over the amount of information shared. Only low-exposure (2) and high-exposure (3) groups received the artificial ads. We divided each group into two subgroups (groups 2A, 2B, 3A, and 3B). Groups 2A, 2B, 3A, and 3B consisted of 16, 15, 20, and 20 participants respectively. We did the study for group 2 and 3 separately on different dates, so we can divide the groups and eradicate exposure effect for this analysis for the sake of simplicity.

We ran two separate one-way between subjects tests for both low-exposure and high-exposure groups. Our results shows that there is no significant difference between mean points earned for low-exposure group on different public influences, $F(1, 60) = 3.822$, $p = 0.055$, *partial* $\eta^2 = 0.060$. Also for the high-exposure group, there is no significant difference between mean points earned on different public influences, $F(1, 80) = 1.063$, $p = 0.306$, *partial* $\eta^2 = 0.013$. That means that in our scenario, people, in general, did not get influenced by their peers.

3.3.4 Post-study Survey

We asked the participants to take a post-study survey. The survey consisted of 5 demographic background based questions, six questions about their technical expertise, and six more questions about their general concerns and consciousness of privacy and information sharing. In this sub-section, we look into several notable results we found by analyzing the survey data. We have already discussed the demographics, and Table 5 describes the summary of the demographic backgrounds of the participants. Now, coming to the questions based on technical experiences and general concerns, let us look at statistics to understand the participants' opinions.

The first three questions were about the technical backgrounds of the participants, and their habitual facts related to Internet usage and social media familiarity. Interestingly, 71.6% participants replied that they have at least some levels of experience of working in computer-related fields. 76.5% of them told that they use the Internet pretty often. 55% of the participants replied that they use Social media applications like Facebook, Instagram, etc. several times a day. The results imply that the participants were well experienced with the Internet and social networks.

Now, emphasizing on their familiarity to online businesses, targeted ads, personal information tracking, and retailing applications we asked them questions about the usage of those kinds of applications. About 94% of them answered that they often use Internet services and mobile applications to purchase products. 93.1% of them replied that they feel interested in the ads they receive through their social network websites and mobile applications. 57% of them answered that they willfully clicked

on ads to see the details of the products. 86% replied that they accidentally clicked on ads. 54% answered that they often used personal information tracking applications, related to health, wellness, and personal benefits. They are also very familiar with retailing applications, such as Macy's, Sam's Club, Starbucks, and so on. About 77% of them told us that they use retailing applications to purchase goods and take benefits of offers.

The next question was about their activities that could be threatening their privacy. We asked if they did any of the following things related to privacy and information safety. 83% of them told that they refused to give information to at least one application or service because they felt that the information was too personal or unnecessary. About 68% of them answered that they decided not to use at least one application or service where they were not sure how their personal information would be utilized. These statistics reflect that they are mostly concerned about their privacy and conscious of the private information misuse.

The next interesting result we get from another question in the survey. We asked that how much did the participants agree or disagree with the statement, "when websites ask for personal information, I usually think twice about providing it." There were five options: Strongly disagree (1), Disagree (2), Neutral (3), Agree (4), Strongly agree (5). The results are: 2%, 4%, 14%, 32%, and 48% respectively. We wanted to correlate Agree levels with the corresponding amount of information shared in the user study. Table 4 shows the results. As expected, there is a negative correlation between the two. However, the correlation is almost negligible. This analysis proves that although most of the participants are concerned and think twice before they share

their personal information, they indeed shared much personal information. The main reason we can think of is that they were given incentives based on the quantity of information they shared.

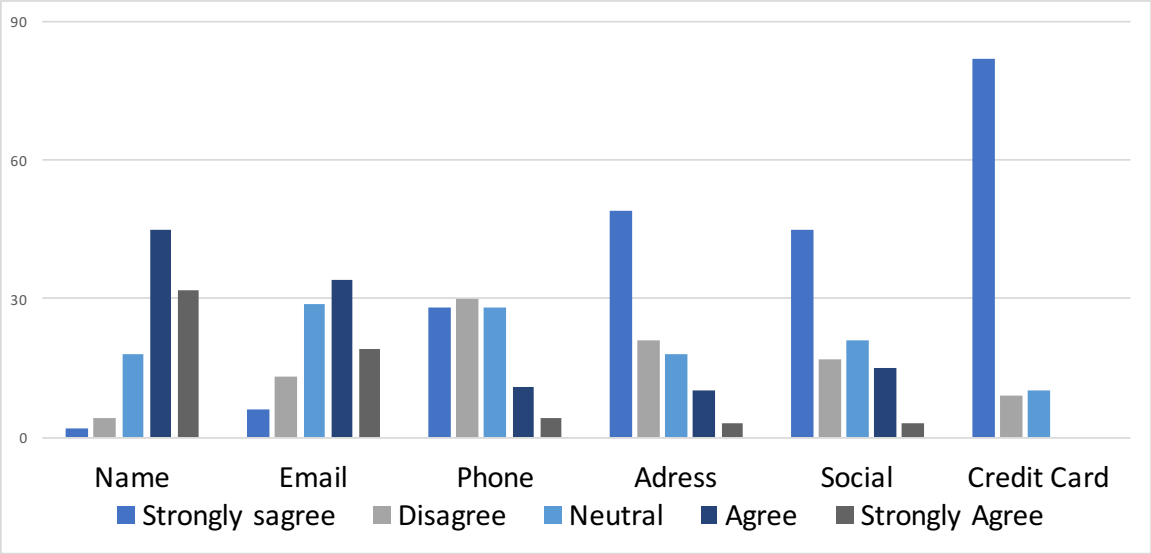
Table 4: Correlations between Agree Levels and Percentage of Information Shared

Correlation	**Coefficient**	**Decision**
Pearson	-0.284*	Negligible negative
Kendall's τ_b	-0.293*	Negligible negative
Spearman's ρ	-0.359*	Low negative
*Correlation is significant at the 0.01 level (2-tailed.).		

Besides, other statistics corroborate the previous statement we have made. We asked the participants that what they thought about the data points we would collect from the study. Table **??** shows the responses of the participants. Most of them were conscious about being tracked by us. The next question we asked was, "would you advertise for any store for benefits in real life?" 54% replied, "Yes," 34% replied,"Maybe," and only 12% replied, "No." We see that the users were highly conscious of the usage of their data. However, the majority of them would share their personal information in exchange for incentives.

Finally, we asked them about their willingness to share some specific personal information in exchange for incentives. Figure 9 shows the results. Most importantly, the more the sensitivity of the information increased, the more they disagreed with the statement. Therefore, we can say that the sensitive nature of the information is also a defining factor of how much the participants share their personal information.

Figure 9: "I would be willing to allow to collect the following information for benefits."



3.4 Discussion and Limitation

In the previous sections, we have analyzed the effects of several catalysts that might change the user's opinions to share their information with the public, when a store employs them as mobile advertisers. We divided the users into three groups: the control group, the low-exposure group, and high-exposure group. Last two groups were further divided into two subgroups each based on different types of imposed public influence (broad and narrow). We divided the ads into two categories: not-sensitive and sensitive. We designed a 2x3 between subjects test to evaluate our hypotheses. In the results for all cases, the effect sizes were ranging from minuscule to small. Also, our data set could not meet the assumption of Normality, because the incentives were attracting the users to share more information to earn more points, so the data was largely skewed to the left. Also, the lack of choices, for personal information, i.e., four choices with only two meant to be personal, can be a crucial

factor for the data being not normal. Moreover, the assumption of the homogeneity of variances is also not met for the same reasons. Therefore, we should be careful and judicious while interpreting the result.

3.4.1 Analysis on our results

In our first analysis, we could not find any collective effect of sensitivity and exposure on mean points earned, where the effect size is very negligible. However, it is evident that, although there is a significant decrease in mean points earned with the increase of sensitivity, the difference is not significant when we consider sensitivity and exposure together. In the next step, we wanted to measure the effect of exposure alone, averaged across the different sensitivity levels. From table 2, we can see that actually over the increased exposure the mean points increase. That is the opposite of what we primarily expected. Our primary thought was that increased exposure to the public would affect the users' opinions to share personal information negatively. Now, if we look at the result from the analysis, we find that there is no significant effect of exposure on the users' opinion to share their personal information. The reason behind this is the lack of choices of the personal information. Also, the study duration was minimal. To measure the actual effect of CGA, the users should use the system at least for several days. Also, to be more realistic, we should not have asked for exploring the store and posting reviews simultaneously. This task was one of the biggest limitations of the study.

Moreover, in our study, we overlooked the competition effect of the users. They were earning incentives from the stores to advertise, that created a positive influence

on their mind to share more information. Besides, for the high-exposure group, the big screen worked as a strong catalyst for creating the competition effect on the users' minds, as they were seeing that many people were very open-minded while advertising. Then, we tried to examine if the public influence can affect the user's opinion to share their personal information. Although not significant, for the users facing low-exposure, the result converges with our assumption. We think that the competition effect plays an important role here. For the low-exposure group, no public element directly influences the users to compete with others to earn money, so it shows the signs of public influence over the users.

3.4.2 Takeaways

The first confounding result we have found is, with the increase of the exposure level, the amount of personal information shared, also raises, which does not get aligned with our assumptions. It indicates that we need to run a separate study to examine the competition effect. Next, we are not quite sure about the users' willingness to trading-off privacy in context to earn money. Combined with the competition effect, the study also indicates that we need to dig deeper to find out how much a user might wish trade-off to earn more incentives. Moreover, to explore what happens to the users' minds when they are employed as an advertiser, more control over the advertising process should be given to them, for example, delayed advertising to the surroundings for enabling users to protect themselves from being exposed, selective advertisement delivery where a user can control their audience, and so on. Also, it is crucial to look at the contexts of place and time for understanding

how effectively mobile users as advertisers system can be deployed. For example, a user can visit different places throughout the day and keep advertising. We need to figure out, how their preferences differ based on different contexts.

3.5 Summary

In this chapter, we have discussed the possibility of using Consumer Generated Advertisements in employing mobile user as advertisers as a utility to both the vendors and the users. We replicated a real-life scenario and examined our hypotheses regarding the sensitivity of products, the influence of public opinions, and people's way of thinking based on the context of exposure. We also tried to gather general concerns and consciousness of individuals about sharing personal information with others. In the future, we want to extend our research to learn more about consumers' perception changes based on different factors. We also are keen to fully utilize 'users as beacons' model to make it more scalable. To sum up, in the following part of our research, we want to analyze the ways the consumers think and explore their mental models for being deployed as user-beacons in different contexts.

CHAPTER 4: USERS' PERCEPTIONS OF BEING USERS AS BEACONS

4.1 Introduction

In this chapter we are describing the user study we conducted on 27 people, to understand the mental model of the users while being employed as users as beacons in real life. In this study we wanted to explore what people generally think about the idea of employing users as beacons, what are the factors they consider when they are asked to use the system, how do they react to different circumstances, how would they handle various situations, what are the features would make the most sense, where can this model of advertising be applied to, what would privacy mean to the people who use that, how do they relate privacy in this system, when they are already using several different pervasive technologies already, and how do they trade-off the privacy in response to earning incentives in this system. In order to do so, we designed a user study to interview people to ask specific questions around several scenarios in shopping malls. In the interview, we described how our system works, painted several scenarios of what people might encounter while being users as beacons, and asked questions related to the scenarios. This interview focused mainly on deploying users as beacons in shopping centers, all the scenarios were set up based on how people in a shopping mall would experience this kind of system. After we compiled the results from the study, we found out that, a significant portion of the participants found the

potential of using the system outside the shopping malls, for places like restaurants, or college campuses, even we have found opinions of potential integration of this kind of system with neighborhood-based social platforms like Nextdoor for reviewing local small businesses and social causes. So, we decided to extend our study to explore the possibility of deploying users as beacons system outside of the shopping malls. We designed our next user study with a different set of scenarios painted around different contexts and situations a user might face and asked related questions. In the next sections, we will be describing the design of the user studies, results and our takeaways from the studies.

4.2 User studies

We conducted a user study with 27 participants to explore people's thoughts about a user-beacons system and its applications, factors they would consider in utilizing such a system, and their reactions to various situations unique to this system. We focused, in particular, on privacy concerns as compared to similar pervasive technologies. We chose a consumer generated advertising and review system as our application domain, as we thought this had broad applicability and would be understandable to users. We conducted an interview study, using a design probe to enable participants to have a more concrete understanding of sharing and receiving ads or reviews (Figure 10). We also described several different stories that participants might face in using the system as a prompt for additional interview questions. These scenarios and the interview questions are described below, with the full set of interview questions in the appendix.

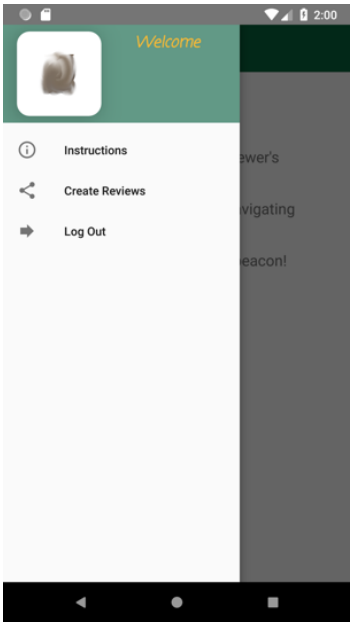
Initially, the design probe and scenarios centered around usage in shopping and advertising products. However, after conducting 13 interviews, we found that a significant portion of the participants saw greater potential in the use of a user-beacons system in other contexts such as restaurant review or event promotion. Thus, we redesigned the design prompt and study scenarios to explore the possibility of deploying the system in more social contexts. We then interviewed fourteen additional participants. Each interview was conducted in an indoor lab setting and took approximately 40-45 minutes. At the beginning of each interview we described the functionality of a user-beacons system and our design probe briefly to the participants. Both of the user study designs were approved by our university IRB.

4.2.1 User study 1: users as beacons for reviewing products

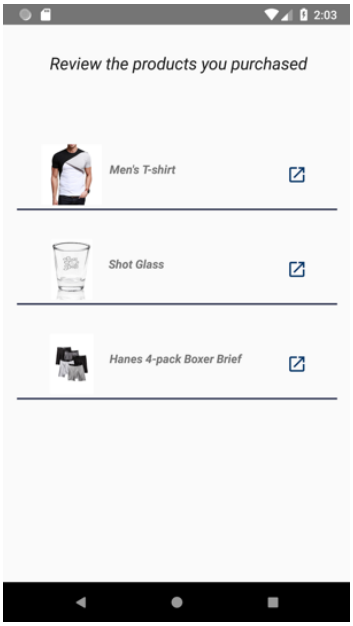
We have developed a design-probe for running the user study (see Figure 10). The design-probe has two versions, one is for the participants, and another one is for the interviewers. We explained several scenarios to let people understand how the system works, how in real life they might advertise ads, and how they receive ads from the surroundings. Using these scenarios, we conveyed the interview questions based on different conditions. We also used our design probe to understand how the participants interact with their peers, and how the people around might influence them. We have constructed two scenarios where the participants use the design-probe to learn how the system works. Then we painted the rest of the scenarios as real-life stories the participants might face and asked relevant interview questions to understand their mental model.

Figure 10: Screen-shots of the design probe built for conducting study 1.

(a) Navigation Pane to Create Reviews

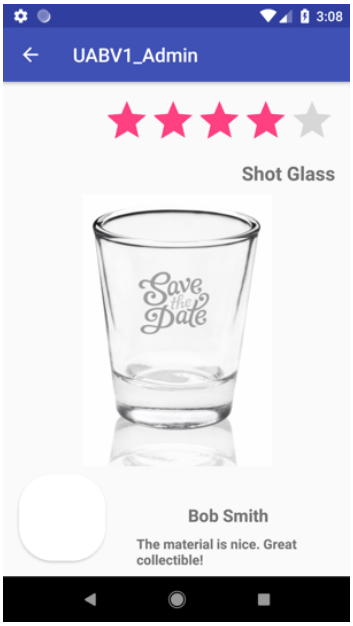


(b) Fake purchase history

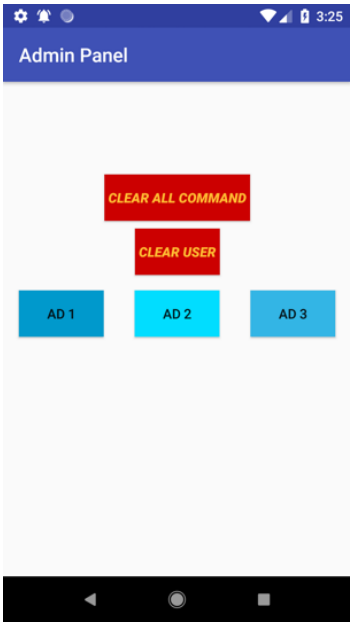


(c) The participant is creating an ad

(d) Interviewer received the ad



(e) Interviewer's Screen to send an ad



(f) The participant received an ad from the interviewer

Scenario one, signing up and creating ads: We started the study with the design probe, installed on a smartphone we provided to the participant. First, we asked them to sign up with the system, providing their name, and taking a photo. Then, we asked them to select a fake product and write and share a review as if they had used the product previously. They had options to share their name, photo, rating, and a product review. After they clicked on the Share button, it became a user-generated review visible to the surrounding user-beacons, (Figure 10c). As soon as the participant advertised the review, it was received by the interviewer's phone (Figure 10d). Then the interviewer showed it to the participant to demonstrated the receiver's view. The interview then commenced. Participants were asked general perceptions of using such a system, their opinion of sharing their personal information in the reviews, and how they would feel about other people recognizing them by seeing their shared reviews.

Scenario two, receiving ads: In this scenario, participants received a review in the design probe, sent from the interviewer (Figure 10f). By doing so, the participant understood how they would receive posts from nearby user-beacons. Participants then answered questions about receiving ads from people around them, their intentions about interacting with the reviewer, and the influence they think reviewers would have on their decisions.

Scenario three, different places: The interviewer described a daily life scenario where the user's device is beaconing throughout the day, in various contexts such as while shopping, traveling and at home. The interviewer then asked about the user's opinion of beaconing in different places, and incentives that may impact their

decisions.

Scenario four, control over the system: We wanted to learn the participant's reaction toward interaction with other users. So, we outlined a scenario where we gave the participant some controls to avoid the interaction by adding a short delay to a posted review. Participants then described their perceptions of that potential feature and its use, as well as other kinds of desired controls in the system.

Scenario five, product types: We then wanted to understand how participants would react to different types of products. The interviewer asked the participant to create a review of a sensitive product (underwear), and asked about the participant's opinion on the perceived comfort of sharing reviews of different kinds of products, along with the impact of potential incentives.

Scenario six, peer influence: In this scenario, the interviewer described receiving a review of a desired product from a person standing right beside them. Participants then further discussed their expected interactions with people around them, and the potential impact of incentives.

Final questions: We ended the interview with several questions about privacy concerns as well as potential applications of the system. Finally, participants filled out a survey with their demographics, education, and everyday Internet activities.

4.2.2 User study 2: users-as-beacons for reviewing places, services, and events

In the second study, we developed a slightly different design-probe to investigate users' thoughts on being user-beacons to make posts about places, small businesses, restaurants, social causes, and events. Similar to the previous study, we discussed

the functionalities of the system and demonstrated how the participant would receive and send reviews, as well as described several scenarios as part of the interview.

Scenario one, signing up and receiving ads: we changed the order of the scenarios in the second interview. In that interview, we first demonstrated to the participants how they would receive reviews from their surroundings, and then showed how they would create a review and send it to their surroundings. So, in the first scenario, we provided the users with a smartphone pre-installed with the design-probe. We asked them to sign up with the system putting their photo, name, email, and gender in it. After completing the registration, the user went to the home screen, where they were able to receive ads from the surroundings. The interviewer sent two posts, one about the review of a restaurant and the other about a service the interviewer took from a plumber. The user received it instantly. Thus they understood the idea of receiving ads from people around through BLE. Then the interviewer asked the users several questions related to receiving reviews from the people around throughout the day and in different contexts to understand their perceptions and preferences about receiving the kind of reviews they might receive.

Scenario two, creating ads: In the next scenario, we asked the participants to use our design-probe to create and share two reviews on their own. Firstly, they were asked to assume that they have taken a lock repair service from a locksmith who ran a small business. The interviewer asked the participants to create and post a review of the small business. Then the interviewer asked them to create a fake post about a social cause they might get interested. Right after they posted, the reviews reached the interviewer's phone through BLE. Then the interviewer showed them the

posts they received and asked a few questions related to the perceptions on reviewing different types of posts about places, services or social causes. The participants were asked about having people around, sharing personal information along with the posts, the controls or preferences the users wanted to have, and reviewing different kinds of things throughout the day in different contexts.

Scenario three, instant reviews: in the first interview, we did not design a scenario specifically around the people's perception of localized instant reviewing system like users-as-beacons. So, in the second study, the interviewer described a restaurant scenario where the participant was having dinner and wanting to leave a review. The interviewer asked the participant several questions related to sharing both positive and negative reviews and factors relating to whether the participant would want to leave reviews in the moment or later.

Scenario four, explaining a small business review story: As we discussed before, we added a scenario of reviewing small businesses, like what people do in Nextdoor platform. To do so, the interviewer described a story where the participant used a pest control service, and was then asked several questions related to their opinion on reviewing such a small businesses, their motivation, and the factors they would consider in writing reviews for them.

Scenario five, Describing stories about different controls and preferences applied in different situations: Similar to the fourth scenario in the first interview, we described two social situations - one being at a birthday party with friends and family, and another being at a club with many different people. The interviewer then asked questions related to the interaction with both familiar and unknown people, and

Gender	N	Age	N	Education	N
Male	11	18-24	5	Some College	4
Female	16	25-34	19	Associate degree	1
		34+	3	Bachelor	14
				Post-graduate	8

Table 5: Demographic Summary of the participants

participants' perceived needs for controls and preferences over potential interaction.

Final questions: As we did with the earlier study, we asked general questions on overall perceptions, privacy, and suggested features and then ended with a survey of their demographics, education, and everyday Internet activities.

4.3 Participants and Analysis procedure

4.3.1 Participant Recruitment and Demographics

We recruited participants around our university campus, through emails sent by our institutional research service and flyers posted on campus, and recruiting posts through social media in neighborhood groups surrounding campus. We also utilized Snowball sampling, where initial participants suggested additional participants. We recruited 27 participants in total for both of the studies. After the interview session, each participant was compensated with a 10$ gift card. Table 5 shows the demographics of the participants in the studies. The participants were from variety of occupations, including 13 undergraduate and graduate students, physicians, higher education administrators, health educators, and career advisers.

4.3.2 Analysis

All interviews were transcribed for analysis. We first analyzed the 13 participants in Study 1. As a primary coder, the first author conducted inductive coding for three sample participants and discussed it with the other authors. The authors agreed on a codebook containing 15 codes. The primary coder then coded the remaining transcripts with the codebook. Based on initial results, we decided to conduct the second interview study before further analysis. This time two researchers independently and iteratively coded three sample participants from the second study, comparing and merging their code books with discussion among all authors. An agreement was reached on the codebook and all codes for those 3 participants, resulting in a codebook of 19 separate codes. The two coders then coded all remaining participants independently with no further changes to the codebook. When coding was complete, the researchers compared each code and discussed and resolved any disagreements. Disagreements were tracked, and inter-rater reliability was calculated at 96.47%.

The contexts and the scenarios were slightly different between the two studies; thus, the codebooks are slightly different from each other based on instant reviews, irrelevant reviews, irritating notifications, and writing reviews in different places. Overall, X codes were the same between the two studies. Thus, as a final step, we grouped all the codes from both of the codebooks into higher-level categories to merge results for both of the studies altogether. While discussing the results, we enumerated the participants 1 to 13 for the first set of interviews and 21 to 34 for the second set of interviews.

4.3.3 Limitations

The limitations of our study are similar to other exploratory, qualitative studies. The sample size for each study was relatively small, with heavy student and university employee representation. Thus, participants were likely more educated than a general population, with views that may not match others from different populations or cultures outside of the United States. The system was also hypothetical, which means participants were discussing initial responses that may not accurately reflect later behavior with such a system. These responses may have also been more positive to be polite to the interviewer. Despite these biases, we believe our results provide valuable early feedback on the potential of this system, as well as inform the design of such a system.

4.4 Results

While the two interviews differed somewhat, many of the perceptions and reactions are similar across both studies. Thus, we describe our findings together, and only distinguish between the two studies as needed to further explain results or compare reactions if they differed. We regularly specify the number of participants while describing a specific perception in order to describe the prevalence of a sentiment in our sample. However, these numbers are not representative of a more general population. We also use generalized keywords such as ‘a few’, ‘some’, and ‘most’. We consider ‘a few’ as 2-6 participants, ‘some’ as 7-13 participants, ‘majority’ as 14-16 participants, and ‘most’ as more than 17 participants.

4.4.1 General perceptions about reading reviews

The most immediate reaction of participants to the notion of receiving reviews and ads from surrounding people was that it is not likely to be fake and instead comes from real people around them. For example, P30 said, *"Now when I need services now, I am Googling them. But, I would prefer to trust the people close to me, or want to hear from people who are nearby me. This Beacon idea is appealing in that sense because I know that people around me are referencing that."* And another example from P1: *"Actually, I think this ad will come from the nearby people. Let's think I am at home, and I live in an apartment complex. I may receive ads from my neighbors, right? I know them, so I would trust them..."* Thus, trust emerged as a key perception, and users reacted positively to the possibility of increased trust through this system. In order to trust reviews, they also expressed desire for reviewers to not be anonymous so they could know where an opinion came from.

Participants also talked about the types of reviews they would be most interested in. Most participants thought that the product reviews were useful to receive, but only in shopping areas, and that highly depends on time and contexts too. In their opinion the reviews of restaurants and local places would be the most useful things to receive. P22 said, *"I would wanna receive reviews of food, restaurants, home services, probably Craigslist kind of things- sold things around me."* Participants also mentioned the usefulness of receiving discounts, as well as updates about nearby events. *"Basically, I like to receive the offers related to food, to see if there is any discount, any offers available for food and restaurants, any updates for events nearby, and offers*

on shopping, and so on." - P24

On the other hand, many did not like the idea of promoting social causes. And, they wanted to receive service recommendations reviews only when they needed them. All but three participants said that the relevance and context of the received reviews are essential. P21 said, *"I think I need different kinds of reviews based on my need. Sometimes, for example, if my car is broken, I want to know about the mechanics near me and want to have the reviews, so it depends on time and context. It depends on the circumstances." "So if I am out and my phones keep telling me about good reviews about locksmiths, or plumbers or the ads those are most of the time probably I will not gonna need, it might get irritating."* - P28

Thus, most participants talked about customization features to filter the types of reviews they are most interested in. P30 said, *"I think I would maybe want to, I do not know if I want to subscribe to topics that I am interested in, or I would rather just everything. I think that it might be a good idea to create buckets of topics, and let people subscribe to the types of topics so that you would choose the topic."* P13 said, *"I would want to subscribe to specific categories of posts. I like foods, so I would not mind getting reviews about the restaurants in an area that I would be in. But I would not want the reviews of products that I have never considered purchasing."*

A majority of the participants thought that receiving a lot of instant notifications from others could be irritating. P2 said, *"Sometimes I see that people are saturated by posts. That is pretty irritating, and one of my concerns is that there is already a lot out there, I do not want any new system to add more."* And, P33 said, *"I think if I start to receive ads too much, like especially since I have the apple watch and I*

have the notifications turned on. It buzzes all the time, and if I am in a meeting, I think people think that I must be really rude when I am looking at my watch; where I am just looking at a notification that popped up." P33 continued the discussion by saying, *"I think that I would personally want to control maybe when I am getting them. If it were happening too much, like if I were at work, and I was getting from all of the people everywhere, then that might be overwhelming, and I would turn the notifications off."* P11 said, *"I think this could be useful, but you do not want to be overwhelmed by [receiving posts from] others, right?"*

4.4.2 Writing reviews to the people around

Participants were generally open to writing reviews if they liked the product or place and they trust the people around them. P21 said, *"Actually when I am sending my review, I would think that it might help people around me. When I am somewhere, and I feel that the thing I am using is really good and I want to let the others know, then I might review it."* Users compared this system to existing review platforms, such as Google or Yelp, and thought that this platform would be similarly useful.

Similar to preferences for receiving different kinds of reviews, participants stated that they would mostly write reviews for restaurants and interesting places, also if they have ample time, they would write reviews of products. They generally wanted to support small businesses as well, but only a few wanted to use it for social causes or service reviews.

In many of the participants' opinions, similar to receiving instant notifications, writing instant reviews was a matter of discomfort. In study 2, when asked about

writing a review in a restaurant, 12 participants stated that they would not write a review while still in the restaurant, but later, when they are out of the area. One reason was that writing reviews needs time, hence they would need to have ample time. Participants also acknowledged that they may need reminders and methods to make that as easy as possible. *"What would be rather cool is that if this app knew that I ate at whatever the restaurant was, they send me a reminder later, saying, hey I know that you ate here yesterday, what do you think? That would prompt me to write a review. Unless it is really easy and quick, I would do it later."* P28.

Participants also mentioned not writing a review immediately because of potential social interaction that might result. As P31 said, *"I would probably want to let people know in the long term, not instantly. But I do not want to be targeted as 'Oh you wrote that! I know that was you.' I think if I am sitting there at the restaurant, like, I do not want them to come and say, 'Oh I know who that was!' I am worried about probably restaurant management."*

The importance of social norms and network effects also emerged in how participants might react to such a system. As P6 said, *"It depends, like for now, I have my concerns. But, if after a few years it becomes a trend, then I might not feel that way."* Participants also acknowledged that while it feel strange at first to advertise certain products or places with this system, that perception could change if that became more visible and normal. P2 said, *"If this one guy can do that, then the others should not be that self-conscious about whatever the product is. So I think I would still review it."*

4.4.3 Sharing personal information

We wanted to know how the participants felt about sharing their personal information with other users nearby. All of the participants felt that it was acceptable to share their first name with the reviews. However, most of the participants were cautious about sharing their full name, as that would identify them, and instead would prefer an alias. All of them except two were hesitant to share their photo. As P2 said, *"I like the idea where you do not need to send the picture, and its when you can match a name and a face, I could see potential privacy problems. If you are on your phone and you just get like a random message from a random name, you don't know who it was around you. So, [sharing] photo is a concern."* Some were worried about trusting the peers to whom they are disclosing their information and thus desired anonymity. *"I might need the anonymity, because, you never know who is around, who is going to get it."* -P31. Five participants specifically mentioned concerns over being stalked and several others mentioned identify theft; as P12 said, *"I think it would also be a privacy issue if someone sees my photo and sees my name, I mean that is a lot of personal information, for predators or stalkers who can then easily get my photo and contact information for something."*

4.4.4 Interacting with others

In this subsection, we want to explore how the participants thought about the interaction with other user-beacons. We specifically designed scenarios to understand users' thoughts about interacting with other people around in users-as-beacons settings. Twenty-three participants anticipated that people around them would come

and talk to them about their reviews and ads. Seven of them felt at least some kind of discomfort in that, mainly because this was entirely a new situation that they have never experienced. P7 said, *"It is kind of uncomfortable. That is mainly because we never had this kind of experience before. Online reviews are different. Nobody knows the person who wrote the review there."* Some people felt discomfort because they thought that they were a bit shy, and not comfortable talking to strangers. P28 suggested the virtual communication feature would be preferred similar to existing review platforms, for example *"I would be fine if there is a way for someone to reply to my review, saying, hey, I have some questions about your review there, and then I can reply. But, I would not want strangers to come and talk to me."*.

In study 1, we described an option to delay sharing a review to prevent unwanted interactions with others. Nine of the 13 participants in that study thought such a delay would be a good idea for various reasons, such as the sensitivity of the content, public exposure, and interference from store management. P2 said, *"If I really want to review a sensitive product, then delay might be a useful feature to have."*

Yet, eight participants were positive about potential interaction. P5 said, *"It feels good actually. It does not make any difference to me, as I have created the posts. I already know that it will pop up onto your phone."* Two of them were even delighted to interact with people. The participants think that it is a new way of sharing thoughts and thus they can have a conversation with real users. P27 said, *"I would make friends out of it. There could be some negative experience, but that is probably less likely to happen."* A few participants, such as P10, took this model of real-time and localized communication as a new way of socialization. She said, *"Right now in America we*

are closing ourselves off from others. There's this culture of fear, and so I might only share information with a privileged group, people who I am inside with. Whereas, I might be in a different world, want to share information with anyone and everyone because that might come from the place of trust and community and society. So, an app like this could start to change that kind of way of thinking. For instance, with this deal on something on sale. Rather than for me to tell about this deal which is on sale to my friends, maybe I want to help everyone around me and tell everyone about the deal. I think that is wonderful."

In both versions of the study, we asked the participants about their opinions on beaconing throughout the day, in different contexts. In public places, 19 of the participants wanted to keep the devices' beacons open, particularly if they earned rewards for doing so. P33 said, *"It is like the Nextdoor app. I have the alerts turned on for that, and if there is something happens to my neighbors and they say something about it, I can help them... This could be a place where everybody can pay attention to their neighbors without having to physically do that. They could use the beaconing app, where they can feel the connection with their neighbors."*

Yet, participants were less sure about the need for beaconing with people in other contexts. For example, five participants did not want to keep beaconing in the workplace because they think that workplaces are professional places, and privacy is essential there. Also, they expressed concerns about sharing too much private information, such as shopping and other habits, with their colleagues. Only five participants were willing to keep beaconing at home; many of them said that they would not do that, mainly because home is for family, and they wanted little to no intrusion there. As

P31 said, *"I don't know if I would keep it on all the time in general, just because it feels like, whenever you are at the birthday party, you are spending time with the people around you. You don't want to be having them look at their phones just because you broadcasted something."* Several participants also argued that they can directly talk to the people they know instead of posting a digital review. P25 said, *"If I am at the birthday, I just want to have a good time with my friends and family. so instead of sharing, I can directly talk to them and tell them about the place."*

4.4.5 Interacting with establishment

There was a common feeling against interacting with the establishment related to the review, that those in authority could interfere when a user is writing reviews. For example, three participants wanted to use the posting delay because of fear that store management might want to confront them if they post a negative review. P3 said, *"I think a delay would be a good idea if the manager would want to... try to find you. I would want to add the delay if I fear that the manager might misbehave, they could be angry or something."* And P1 said, *"So I would be more interested in delaying because I am more concerned about the company or the employees to read the reviews if they are negative and get back to me."* Interestingly, in the second study, the participants were also thinking about confronting the restaurant management when they wrote an instant review. And P31 said, *"I think if I am sitting there at the restaurant, I do not want them to know who that was. I am worried about probably the restaurant management."* Moreover, 7 participants were worried that store management might want to intervene in the system to promote their products. P8 said, *"I would question*

the reviews of their own employees. I know that many employees might try to push their products."

4.4.6 Privacy in users-as-beacons

The participants expressed several privacy concerns perceived from our explanation of the system, many of which were the same threats found with the Internet and digital media in general. Participants were particularly concerned because, beyond just their reviews, they were not sure what kind of information the app would need to prompt them to write reviews. Thus, behavioral tracking was a big concern among the participants (n=11). P1 said, *"One of the questions that I have related to privacy is, how the app knows what I already purchased? So, is it through my email? And are they then pulling purchase orders?"* And P29 said, *"Using one app leads to using another app. so they send information to each other, and then the next thing you know there is another ad, another service sending you the information. You will have like people calling you because your information is shared. Phone number, email addresses, all these things are connected."* Yet, participants also discussed that existing applications and platforms already utilize such personal information, and thus they would also have similar levels of trust in reputable organizations. P31 said, *"We already know that Google is probably trading our identity, so, you know there are analytic and stuff on everything, on social media, Yelp, Instagram, Google reviews."* Thus, these privacy concerns were not related to the users-as-beacons concept itself, but merely using yet another review platform that may require access to personal information.

Not surprisingly, location tracking was a primary concern. P5 said, *"Also I can be*

tracked by the companies. They also know that I am around. That is a bit creepy." P11 said, *"I would wonder about how my information is being used, not just from the users of the system, but also from the businesses. What are they doing with the information and the decisions are they making?"* Interestingly, one of the potential benefits of users-as-beacons is that the app would not need to track location in order to work. Yet, users seemed to be expecting that their apps would know their location, even if not needed, and were thus not expecting any location privacy from this system. Surprisingly, some people wanted behavioral and location tracking to make the use of the system more convenient and receive tailored reviews. P3 said, *"I would prefer a system that uses a location-based model that can automatically sort this thing out for me. For me as a receiver, I would like to receive the ads related to where I am now. So, if I am a sender, I do not want to be a person who sends out-of-place things."*

As mentioned previously, a few of the participants were worried about their physical privacy. They did not want to share their information for fear of being tracked by predators and stalkers. P10 said, *"If I am somewhere, using a beacon, someone can find me; I was here, and there. I am worried about being tracked. People can track me easily if they follow my beacon."*. Others did not worry as much much mainly because they already use several apps where they can turn the user location sharing off.

Despite perceiving that one benefit of a users-as-beacons system was the increased trustworthiness of reviews, the majority of participants were still concerned about spamming from fake users and bots. This was also tied to their desire to not be overwhelmed by too many irrelevant notifications. P11 said, *"I think I mentioned*

that being spam will be a concern, it might be overwhelming to receive so many ads, especially if you do not have any control." Participants were also worried that, if they shared their full name along with their photos, it would become easy for spammers to create fake reviewer accounts using their identity, and use them to spam others who already trust those users. Thus, people were concerned about how their information would be managed and used, or misused, by organizations.

These concerns are similar to many existing applications already in use, and thus users were often expressing a desire to remain in control of their information and identity in this novel application. As P8 said, *"I always put reviews somewhere and I put my name behind that, positive or negative. So, I don't mind that aspect, it's just the control I am worried about."* Participants also expressed a desire to control the audience of their reviews, or block reviews reviews from other user-beacons. Thus, these issues overlap with needs and challenges of audience management in social media systems more generally.

4.4.6.1 Incentives, Motivations, and Trade-offs

Finally, we asked participants about what would motivate or incentivize them to use such a users-as-beacons reviewing system. Most of the participants thought that real monetary incentives, such as cash back or redeemable points would be a good motivation. Even those with high concerns over potential negative peer interaction would think twice if they get incentives. As P31 said, *"I mean, obviously I am doing this study because I am getting a gift card. So any incentives are certainly gonna peak interest to an extent."* And as P8 said, *"I would prefer cash back or discounts. But I*

do not know the threshold, where to put it. It is kind of cost-benefit analysis you do." Besides P12 said, *"I think for cash back or points that might accumulate into a good rebate, I would be willing to do that."* We also asked if they are interested in using this system voluntarily. Most of them were slightly reluctant to use that system when there is no incentive there. P2 said, *"I would still do that. But certainly money would keep more people, it would not fade away if you give incentives."*

We wanted to understand if there is incentive, would people trade-off some of their personal information or not. 4 of them said that incentivizing would undoubtedly motivate them to share the photo, but the incentives should have to be very reasonable; like P2 said, *"That is usually an incentive to add the photo I think. I am sure you will turn a couple of people over to share their photo who were skeptical. But that has to be a very good incentive, I mean very good."* 4 others were not much interested in sharing their name or photo even if they were incentivized.

In the second study, we also directly questioned what things besides money might motivate users. Many participants thought that community feedback such as an upvote, downvote, or comments from the people around who read their reviews would increase the appeal to review more. P31 commented, *"It is interesting to see how many people are seeing it, if they take any action as a result of it, if that is trackable if they get a positive reaction or not, like thumbs up or thumbs down, something like that. I think people, in general, like to see how many people are giving attention to them. So, just seeing how many people you have reached, I think it is motivational."* Others also thought that getting free items, such as a free cup of coffee or free donuts can be a good motivation too since it works in similar contexts: *"I definitely think*

that would be cool; like Google has their opinion reward thing. For example, you go to a restaurant and get a free drink or something. Or in a clothing shop get 10% off or something. I think that would be a really good incentive to use the app and spread it more widely." -P27

Some participants also acknowledged that they would make a trade-off between the benefits and incentives received, and what they were willing to share. As with any privacy calculus, the nuanced context matters. For example, some participants were quite positive about supporting small businesses, and would not need many external incentives to create reviews or share personal information. Thus, while the participants in the first study which focused on advertising products frequently mentioned the need for financial incentives, most of the participants in the second study were interested in using the system regardless of the incentives. And as mentioned previously, if such a system were to become widespread and normal behavior, then their privacy concerns would be lessened. P6 said, *"It depends, like for now, I feel that it is a concern. If after a few years it becomes a trend, then I will not feel in that way."* Some of the participants compared this system with Google reviews and Yelp and said that they are not worried about them much; like P4 said, *"Yes, I would use that. I use Yelp every other day, I am a review freak, and I think it would be a good platform."* Another participant (no. 1) said, *"I have the Target app installed in my phone, and never thought of reading the policies because people use that frequently. I figured that they are big enough. I am OK with it."* Some people also talked about the benefits they got from Google reviews, and Target application and related the utility of the reputed review systems with the users-as-beacons system. So, the reputation

of companies also motivates people to trade-off their concerns.

4.5 Discussion and Implications

We envision 'users-as-beacons' system as a privacy-preserving localized information dissemination system. The primary benefits include indoor localized services without having to share the location through devices, limiting the vulnerability of GPS-spoofing, and potentially restricting the scope of having fake users, thus improving trust and maintaining reliable communication among the users. We explore user reactions to multiple types of reviews and advertising, including product, places, and event reviews. While the overall response was relatively positive, users expressed a range of concerns that will need to be addressed for the successful development and deployment of such a system.

4.5.1 Feasibility and applicability of the system:

One of the most prominent user opinions of users-as-beacons was about the trustworthiness of the content in the system. In traditional systems, user-generated content is often considered more trustworthy than company-generated advertising [34, 46]. We have found a similar notion in our proposed platform, that enables users to create their own content. Users also seemed to understand the usefulness of a localized system such as this, perceiving that the platform would ensure the physical presence of user-beacons in their surroundings, ensuring the realism of reviews in the system. This provides motivation that our proposed system is worth further development.

Yet, while we tried to make sure that participants realized that their actual location was not needed by the system, users did not discuss location privacy benefits.

Interestingly, some of the participants even wanted their location to be tracked in order to gain the benefits of tailored and relevant posts. So, even though location privacy is a potential benefit of the proposed system over the currently deployed beacon technology, users did not perceive or value the privacy-preserving nature of users-as-beacons.

We believe the primary application domain for this kind of system would be a localized extension to current consumer-generated advertising methods, with increased reliability. Based on our study, this system has potential in reviewing places, event advertising, localized socialization, and reviewing products in shopping areas. Participants were most strongly in favor of supporting small businesses, while the utility of writing reviews of individual products was more mixed. And, despite some concerns over the potential social interaction with strangers, participants felt that this type of system would be useful mostly in public areas, such as restaurants and shopping areas, where reviews would also be most relevant. Some participants also saw potential benefits in the interaction between community members that such a system could provide.

4.5.2 Design Challenges

We believe our exploratory study encourages us to continue to explore users as beacons, and our initial results highlight several key challenges that we will need to address through the design of such a system and research in greater depth.

Trustworthiness: The biggest benefit the users perceived about the system is the trustworthiness of the contents. However, participants were still wary about sharing

their personal information with the system and other user beacons. Yet, the more users would share their personal information, the more trustworthy the contents become for receivers, and the more useful the entire system. Clearly, there is a tension between being able to know and trust those providing content in a users as beacons system, and a desire to restrict the sharing of personal information and remain private. As with other novel technologies, users' comfort in sharing personal information may lessen over time, as they become more comfortable with how the system works and as they see others trusting the system. Therefore, it will be a challenge to provide users with sufficient awareness of others' access of their personal information and controls to restrict information sharing and maintain privacy, while still providing sufficient utility through trustworthy content.

Relevance and Timeliness: In both our design probes, we demonstrated how a review was delivered instantly to another user (the interviewer). On the one hand, we expected this would provide users with content in a timely manner, while users are nearby others who want to broadcast this content. Yet, participants' biggest concern was the annoyance of too many notifications, particularly of things that were not of interest to them. However, eliminating notifications and moving to a less synchronous delivery of content may also reduce the potential benefit of receiving content that is localized and the potential of user-reviewer interaction enabled by the system. Many also discussed how they wanted the reviews they received to be contextually relevant to them, and mentioned different ideas for achieving that both through automatic tailoring and explicit user controls for filtering content. Therefore, a key challenge in this system will be to ensure the relevant and timely delivery of the content users

receive, and investigating which methods can achieve these goals.

Managing Boundaries: Some participants were not at all comfortable with interacting with others as a result of writing reviews, yet others embraced the benefits of peer communication and were intrigued with the possibility of greater social interaction. Thus, another challenge is enabling users to manage their openness to such peer interactions, while maintaining comfort and privacy. In study 1 we mentioned one potential mechanism to participants, that of delaying delivery of a review to users. There are likely other novel mechanisms that we can explore to provide users with methods for managing their boundaries, and protecting themselves from intrusion.

4.5.3 Future research needs

While this initial investigation provided a range of user opinions, these will likely differ and depend on the details of a specific design and context of use. In addition to the challenges raised above, there are a number of additional issues we believe can be explored within this type of system.

User habituation: In this study, users experienced a rather simple demonstration and a spoken description of the system, which might be insufficient to understand how the system works, without time for participants to get habituated to the system. Future research needs to investigate how users respond over the long term to such a system, where do they find the most benefits and how does their behavior change over time? What concerns will arise as users repeatedly encounter the same people, in the same or different places, providing multiple reviews? What positive and negative experiences will shape user behaviors, and lead to greater or reduced usage?

Incentives: We did question users about the potential incentives for using a users-as-beacons system. However, we did not examine this question deeply, and users for the most part answered based on experiences with other review platforms. Thus, we need to examine what incentives would be necessary and effective in motivating users to adopt and provide content to such a system. Examining this question can also provide insight into the key question of how users would trade off the benefits and incentives provided against their privacy concerns and needs.

Real life implementation: While we have outlined a users-as-beacons system abstractly in this paper, and implemented a basic system in our design probe, there are many additional questions about how to best design and implement such a system for real world deployment. Designs are likely to differ based on the context and domain of use, including different solutions to the various challenges we raised above. We plan to further prototype a system using our university campus as a test bed for understanding the feasibility and use of users-as-beacons as a localized social interaction platform.

4.6 Summary

In this chapter, we described the user study we conducted to explore the users' mental models when employed as the user-beacons in real life. We conducted 27 interviews with a design-probe we developed in Android. The study shows that users do perceive some benefits in a users-as-beacons review system, yet also demonstrates that there are still many issues surrounding privacy and peer-to-peer interaction that need careful design and additional understanding. I plan to use our results to design

and deploy prototypes to examine these issues more deeply, providing insights into the incentive and privacy trade-offs in future to accomplish my proposed dissertation.

CHAPTER 5: DEVELOPING THE PROTOTYPE

5.1 Introduction

In this chapter, we describe the development steps of a real-life prototype based on previous studies' findings. As I have discussed in the previous chapters, we have identified some of the crucial challenges that require more research. For example, user habituation in this new form of technology, the impact of incentives in habituation and usage of this technology, and the real-life reaction of the users while being employed as user-beacons. Taking these into account, we develop our prototype of a U-a-B system for a festival scenario. This chapter describes the features of this application, along with the implementation details. We describe the deployment study of this prototype in the next chapter.

5.1.1 Prototype test-bed

Considering the limitations and feasibility challenges, I planned to conduct the third study in a local festival, specifically the international festival (iFest) at UNC Charlotte, where it happens to be a sizable crowd within a reasonably large arena. Thus, I developed the prototype interface and features specific to the iFest.

5.1.2 Challenges and Limitations to Develop and Deploy the Prototype

There are a few challenges we need to consider before we design and develop the prototype.

- Familiarity: user understanding is a vital issue for this system, as it is a novel system, and there is no system deployed precisely like this. Therefore, making sure the users get familiar and comfortable with the system before conducting an initial study is a challenge. Hence, we need to keep the application simple, limited to straightforward functionalities. Additional features may be needed to support long term or repeated use.

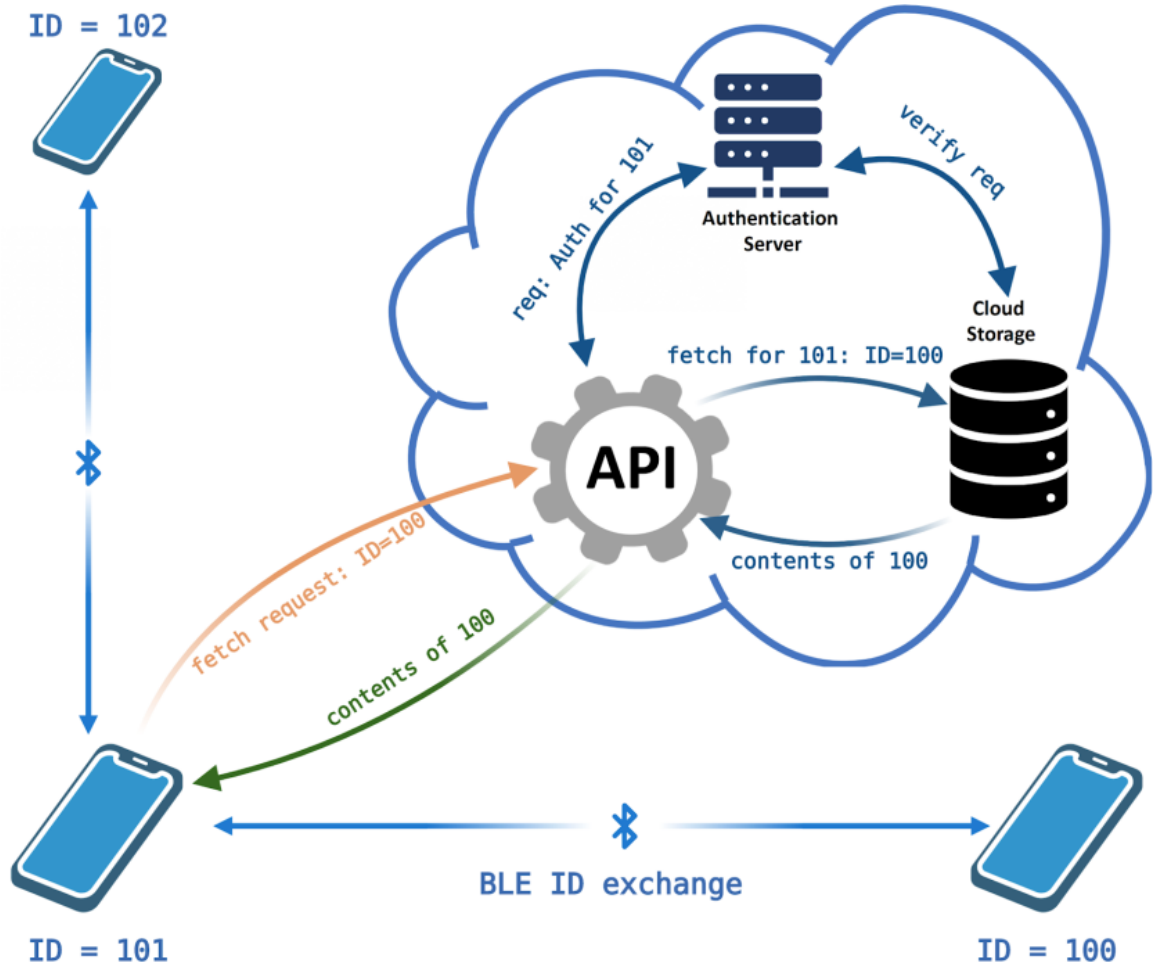
- Crowded place: managing a localized users-as-beacons system in a large crowded area is a challenge, especially indoors. Managing seamless connectivity is a big issue in both BLE and cloud communications. So, we need to decouple the underlying systems so that this problem has a minimal effect on the procedure.

- Managing the context: in U-a-B, it requires a localized context for the users to use the system. A crowded festival should be a suitable environment for keeping a shared context for the users, as the visitors are there for a common goal, which is exploring the activities and booths of the festival. However, iFest is a reasonably large festival, and facilitating the proper context to the application's users is crucial. Thus, the app interaction was customized to this festival and may need to be generalized or modified to work well in other contexts.

5.2 The Design and Functionalities of the Prototype

In this section, I describe the prototype we built to deploy in the iFest. First, I describe the back-end of the system, followed by the front end application we built for the festival. We describe the prototype using the storytelling of how a user uses the system.

Figure 11: U-a-B user interaction backend.



5.2.1 The Back-end

5.2.1.1 Registration, Login, and Authentication

To start using a U-a-B system, a user installs the application and registers their profile. In the case of registration, the application submits the registration form to the server API. The API server sends a request to the Authentication server, and if the request is successful, the Authentication server replies with a 265-bit session key, unique to that user. The API forwards that key to the application. The application

now uses the key as the session key for the rest of the use until the user logs out.

The login is similar to register. The user enters their username and password, and the application forwards it to the API. The API then authenticates it with the authentication server and forwards the session key to the application.

5.2.1.2 Managing interaction among the user devices

Figure 11 shows the working procedure of the U-a-B platform. The procedure has several steps:

- BLE handshake.
- Request to fetch content from the cloud API.
- Cloud API backend:
  - Authenticating the user.
  - Access control.
  - Fetching particular content from cloud storage and database.
- Delivering content to the user.

BLE Handshake: when a BLE-enabled smartphone with the U-a-B application installed comes across another smartphone having the same application installed, they exchange each other's IDs. Each BLE ID is unique and mapped with the user's ID upon registration. Each user then asks the cloud API to verify that it is a real user and then saves the exchanged IDs as users nearby. That is how a BLE handshake between two proximally close devices is done in the U-a-B system.

Request to fetch content from the cloud API: Once a U-a-B device D1 has done the handshaking with and received another device D2's ID and verified it with the authentication server, it sends a request to the API server to fetch D2's contents.

Cloud API backend: A cloud API for the U-a-B system does several background tasks to deliver content to the user devices. Such as,

- Authentication: after the API receives any request, it authenticates the requesting user with the 256-bit session key generated after login.
- Access Control: after verifying that the request is from a real user, the API then sends the request to the cloud storage. The cloud storage rechecks the authentication server to check the access permissions for the request. If the requester is eligible for retrieving the content, the authentication server allows the cloud server to provide the content to the API.
- Fetching particular content from cloud storage and database: the cloud server then provides the API with the appropriate data for the requested content.

Delivering content to the user: after the API server receives the content, it structures the data in the content in JSON (JavaScript Object Notation) format. After the application retrieves the JSON, then it parses the data and displays it to the user. Thus, a U-a-B user receives the content from the people around.

5.2.1.3 Managing own content

As each of the users is mapped with a unique ID from the cloud server, the contents are saved for each user in the cloud database mapped to their corresponding user IDs.

When a user creates a post, the application sends the content to the API server. The API authenticates it with the session key and saves the content in the cloud storage.

5.2.2 The Front-end

Figures 12 and 13 display the screenshots for the application I developed for the International Festival (iFest). The application has several features:

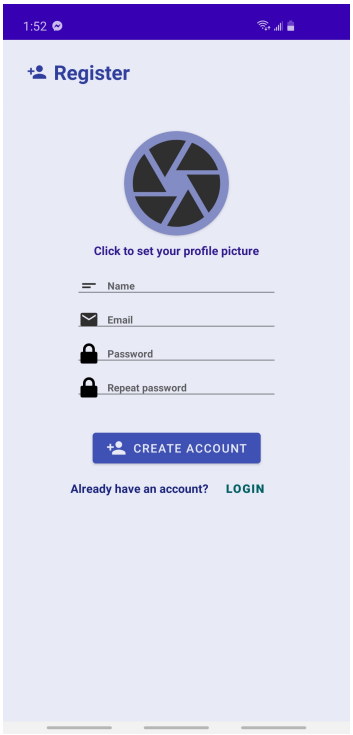
- Signing up and creating a profile.
- Logging into the system.
- Creating posts.
- Receiving posts.
- Marking posts as favorite.
- Controlling own posts.
- Managing favorite posts.

We have developed an Instagram-like Android application as the prototype for deploying the Users-as-Beacons technology in real life. As we mentioned earlier, we deployed the prototype at the International Festival. In the following, I am describing the usage of the application in detail by storytelling.

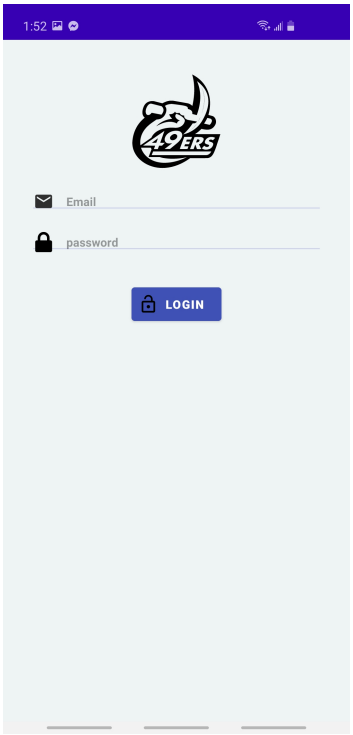
A user Ron comes to the iFest and visits our booth. They install our app and start roaming around the festival. We asked them to use the application as they do in social media applications; however, constrained only within the event.

Figure 12: Screenshot of the prototype deployed at iFest (part 1).

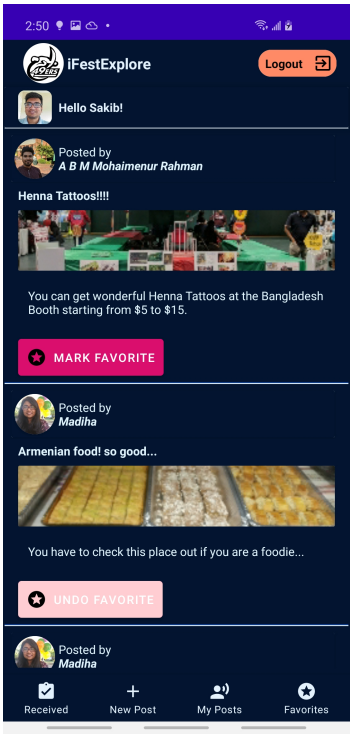
(a) Signing up



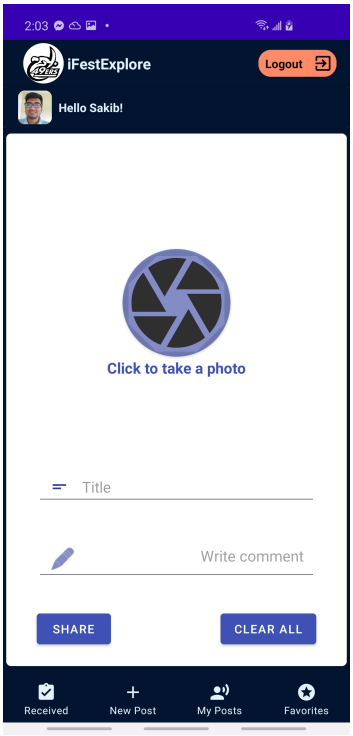
(b) Logging in



(c) Home screen



(d) Create a post screen

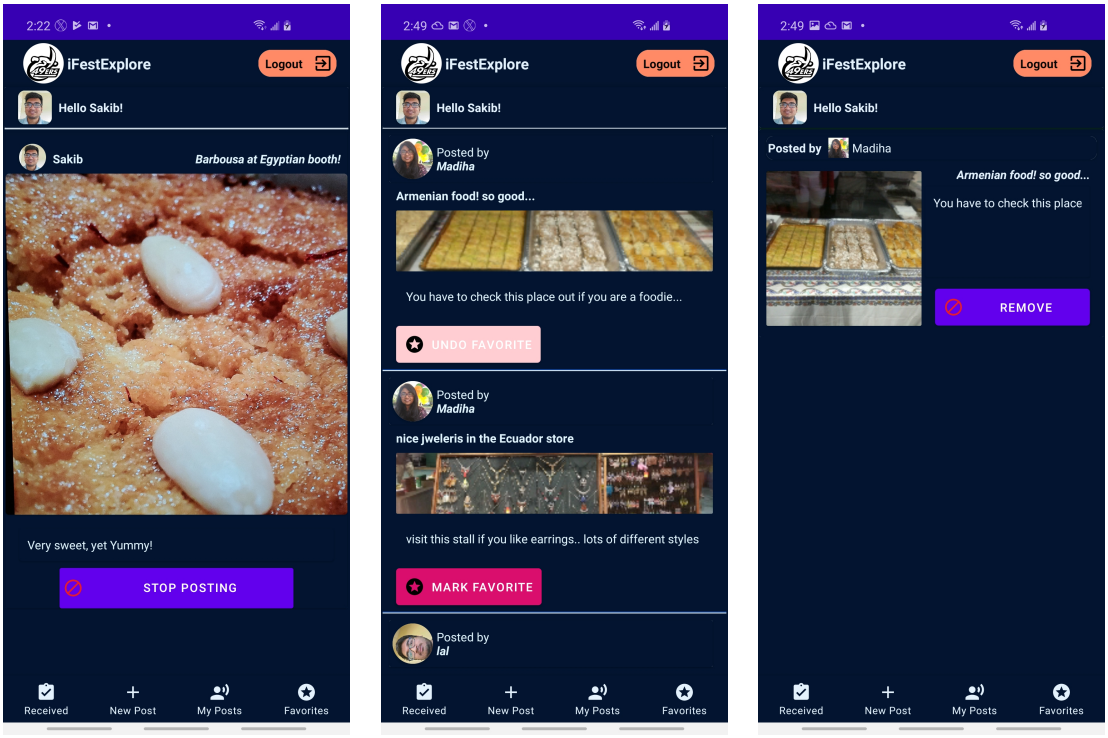


(e) Taking a photo of a subject

(f) Posting the subject

Figure 13: Screenshot of the prototype deployed at iFest (part 2).

(a) MyPosts screen (b) Marking a post as favorite (c) Favorites screen



Register / Login: Now, Ron starts using the application by signing up with our system. They take their photo, put their name, email, and password, and click on the 'Create Account' button to register them into the system (see Figure 12a). If the user is already registered they can log in using the 'Login' button (see Figure 12b). Once Ron logs in, the application takes them to the Home screen.

Home screen: The home screen consists of a few elements (see Figure 12c):

- A list of received posts: while Ron roams around the festival, his phone encounters BLE signals from other devices from the surroundings. Whenever his phone senses the BLE signal from another device, it does the handshake and exchanges the BLE IDs with that device. After the BLE exchange, Ron's device

fetches the contents related to the other user's BLE ID. Furthermore, the list of posts is displayed on the Home screen.

- Each post has a few attributes:
  - The name and the photo of the post creator.
  - Title of the post.
  - An image of the subject.
  - A comment or description of the subject.
  - 'Mark Favorite' button.

  Clicking on the 'Mark Favorite' button adds the post to Ron's favorite posts and switches to the 'Undo Favorite' button. Ron can now undo mark favorite by clicking on that button again.

- Bottom Navigation pane: this navigation pane consists of four navigation items, such as (i) received, (ii) new post, (iii) my posts, and (iv) favorites. This navigation pane is used for switching between the screens of the application.

- Logout button: This button allows the user to logout from the system.

Create a post screen: Ron visits the Egyptian booth in the festival and tasted a dessert named Basbousa. He thinks that it might be useful to the people around who are already in the festival if he creates a post about Basbousa in the booth, and posts it to the surrounding user-beacons. So, he needs to click on the navigation item named "New Post," and the Create a post screen appears; see Figure 12d. Then Ron

takes a photo of Basbousa from that booth, creates and posts it to the surroundings, (Figures 12e and 12f).

My posts screen: This screen contains all the posts made by the user (see Figure 13a). The user can control the posts from here, and delete them. Favorites Screen: This screen consists of the posts that are marked as favorites by the user. Using the screen, the user can save the posts they are interested in the most. Then they can use the posts to find the booths, talk to people, and so on. They can also remove the posts from favorites.

5.3 Development Environment and the Public Project

I developed the prototype in Android Studio [1], the official tool to develop Android applications. As most of the legacy BLE libraries are written and documented using Java, I have used Java as the development language. The Android development platform is cross-platform. It runs both in Windows, macOS, Linux, and all other UNIX based systems. Therefore the project I built for the development of the prototype can be compiled, built, and run using the Android Studio.

I have published my current project in a GitHub public repository [5]. Anyone can clone the project from here: https://github.com/sakibnm/iFestExploreV2.git.

5.4 Summary

In this chapter, I described the design and the functionalities of the prototype I developed for the iFest. The prototype supports the exchange of BLE IDS and retrieving content from the cloud, demonstrating the feasibility and implementation of a UaB system. The code is available to be used by any researcher to adapt to a

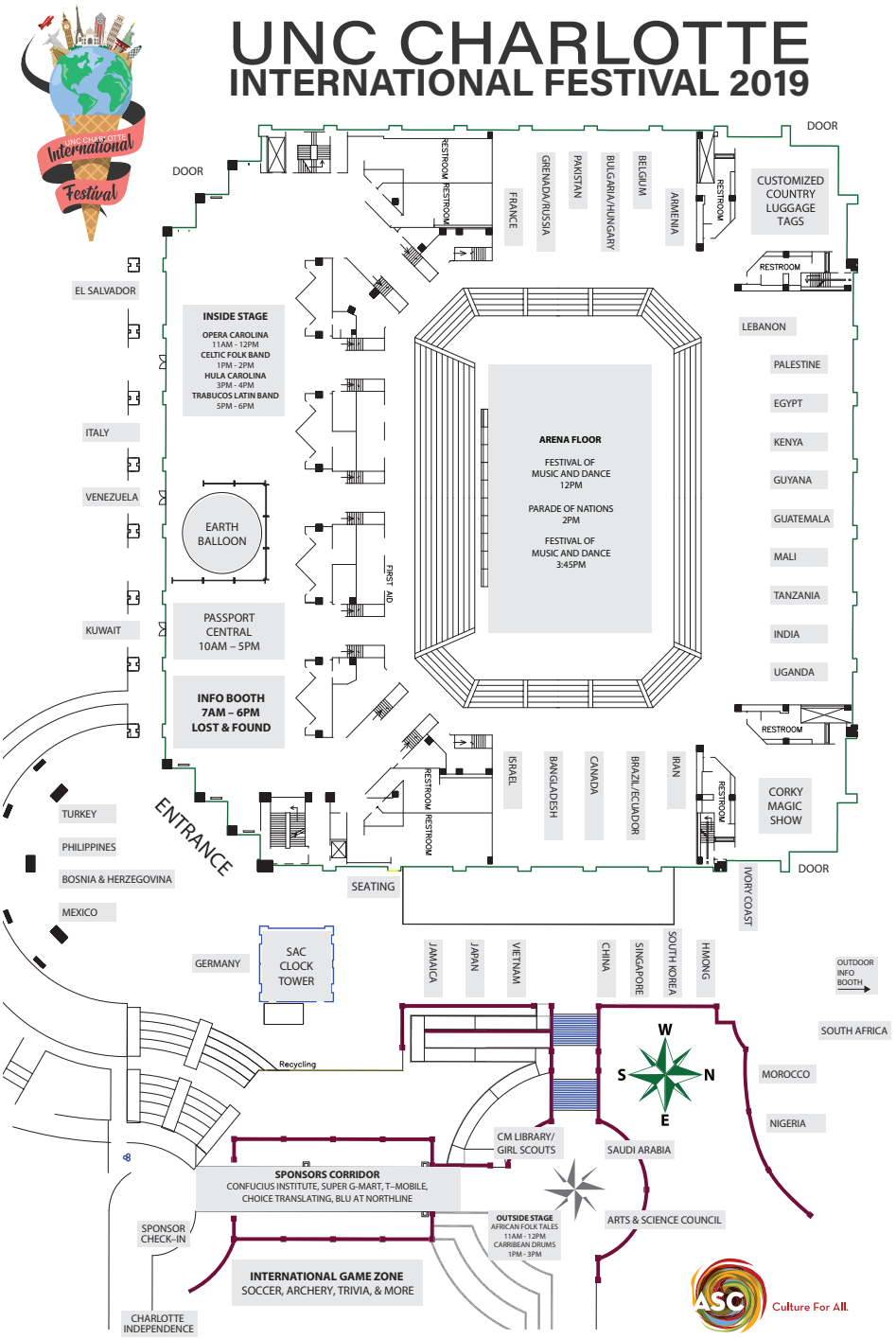
different event or scenario to further the research. In the next chapter, I describe the study I conducted with this prototype in the iFest.

CHAPTER 6: DEPLOYING A REAL LIFE PROTOTYPE TO INVESTIGATE THE EFFECTIVENESS OF USERS-AS-BEACONS IN A CROWDED AND LOCALIZED CONTEXT

We have described the prototype design in chapter 5. In this chapter, I describe how we deployed the prototype in a localized environment. We selected the International Festival at (iFest) UNC Charlotte. We named our prototype as "iFest Explore" and built it for Android smartphones. In the festival, booths are arranged in a colorful marketplace style representing over 50 nations' cultures. The booths are managed and organized by international students and the members of Charlotte's international community featuring art, crafts, and costumes from each participating country. Many booths offer international food for sale.

The previous studies indicated that a localized environment is a good fit for deploying the U-a-B system. Hence, we decided to deploy our app to such a festival where usage would be limited to a short amount of time and a fixed physical location. In this chapter, I describe the study and the results from 30 participants who used it while they visited the festival. From the study, we have found that the participants responded very well to our system. Furthermore, our data show encouraging system utilization and positive feedback from the users. We received a small number of privacy concerns and new feature suggestions from the users. The most important discovery from this study was that U-a-B is a perfect fit for a localized festival environment, where people find it very useful in a contextual environment.

Figure 14: The map of iFest (Halton Arena at UNC Charlotte).



6.1 Study Design

The study consists of three parts:

- **A user study at iFest:** As I described in the previous section, a user started the study having to install our application. Then the user registered with the system using the application, including entering their name and their photo. Then we gave them a demo on how to use the application and how it works. It involved demonstrating how to post an example content and control their posts and received posts. The user then went on exploring iFest. The only study requirement was to make at least two posts in the festival with their contents of choice. Otherwise, they were free to use the app as they wished. All user interaction with the app was logged on the server and analyzed to examine user behaviors.

- **Taking a post-study survey:**After the user completed visiting the iFest, they clicked on the survey button on the application and completed an online survey. A detailed survey can be found in the Appendix. Participants who made two posts and completed the survey received a $10 Amazon gift card.

- **A post-study interview:** After they completed the survey, we invited all the users to participate in an interview to discuss their perceptions of the U-a-B usage in more detail at iFest and their expectations in future development. The interview questions are also attached in the Appendix. Of the 30 users, 8 completed the interview and were provided an additional $5 Amazon gift card.

The interviews lasted for 20-30 minutes. Interviews were then transcribed for analysis.

6.2 Recruitment

We set up a booth at the iFest entry point and asked people at the event to participate in our study. We recruited 30 participants from the visitors having diverse demographics. Table 6 shows a summary of the demographics of the participants. Seventeen out of 30 participants were students, of which twelve of them were from

Table 6: Demographic Summary of the participants

Age		**Gender**	
18-24	**8**	**Male**	**19**
25-34	**10**		
35-44	**7**	**Female**	**11**
45+	**5**		

UNC Charlotte. Eighteen of the participants had at least some familiarity with computing education. The rest of them did not have any experience in computing.

6.3 Results

We asked the participants to make at least two posts, and all did so. Also, our application has several features, such as notifications and marking favorites. By and large, participants made more than two posts and used the other features too. Several people even reported talking to others about their posts, visited the places they saw in the posts, and favorited several posts. A few participants used the application for several hours, which means that they were not only using the app for the sake of the study incentive but also using the application as a localized social interaction method.

Table 7: Descriptive results for system utilization.

	Min	Max	Mean	Median	Standard Dv
Total Time Spent	129	12237	4605.666667	5580	3283.3539
Number of posts	1	7	3.333333333	3	1.26854066
Number of times opened the notifications	0	10	2.733333333	2	2.7283105
Number of times used Favorites	0	3	0.933333333	1	0.90718714

In this section, I am summarizing the results of the study. The results are organized as follows: system utilization, peer-interaction, privacy and exposure, and incentives.

6.3.1 System Utilization

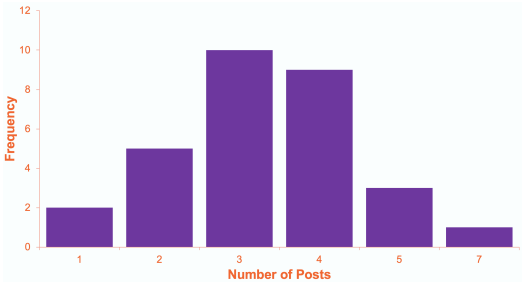
As I mentioned above, when a participant signed up with us at the festival, we asked them to install and use the app. We created log traces for all of the participants and created individual timelines for each of them. We then analyzed these traces to summarize overall behaviors as well as examine usage patterns. Table 7 shows the descriptive statistics for application use, and the Figure 15 shows the histograms of vital key usage of the application.

6.3.1.1 Posts Created

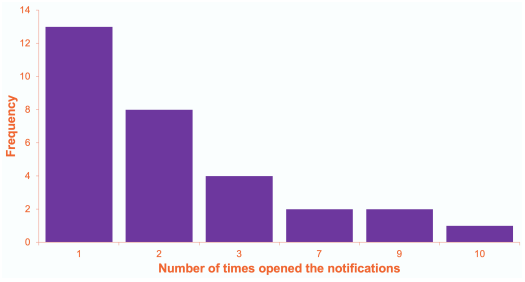
We asked the users to post at least two times in order to receive the study incentive. If we look into Table 6, we see that the mean number of posts created was 3.33, with a standard deviation of 1.268, and the maximum number of created posts of 10. That means that many participants used the application not only for the rewards, but they also used it as a social interaction method for their purposes and benefits like getting to know the festival from each other. After we looked into the contents that people were adding, we found that people posted various kinds of contents ranging from

Figure 15: Histograms for system utilization.

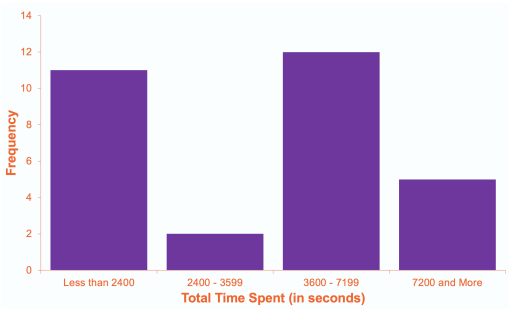
(a) Number of posts made



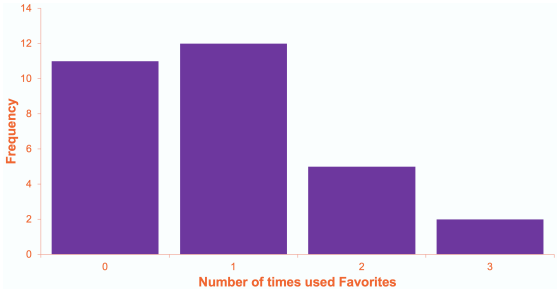
(b) Number of times opened the notifications



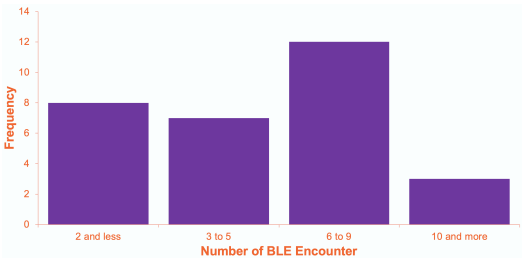
(c) Total time spent



(d) Number of times used Favorites



(e) Number of Beacon Encounters



activities to ornaments. All of the posts were in context and relevant to iFest, and potentially useful to other iFest visitors.

6.3.1.2 Notifications Opened

One of the features of the application was the notifications after a user receives a post. The notifications were adaptive not to irritate the users regularly, and thus participants may have received more posts than notifications. Our results show that people opened the posts they received by checking their notifications. The mean

number of times the participants opened notifications was 2.73, with a standard deviation of 2.73. From the histogram in Figure 15b, we see most of the participants opened 1 to 3 notifications. Five of them opened more than six notifications. That implies that while it was not required, the participants opened the posts received from other users around and paid attention to the received posts.

6.3.1.3 Total time spent

We calculated the total time each user spent using the application. We can see from Table 5.1 that the average time the users spent using the app is 4605.66 seconds, with a standard deviation of 3283.35 seconds. It translates into more than an hour for average cases. From 15c we see that 18 people used the application for about 2000 seconds and less. Nevertheless, most of them used it more than that. If we think about the purpose of the application, it was to visit the iFest and receive useful posts. They were not only posting and receiving using the application, but also visiting the iFest and using the app occasionally. It is a significant amount of time they kept their app open at iFest.

6.3.1.4 Favorites

We added a feature to mark posts as favorite. The idea behind this was to keep the post in the favorite list so that a user can visit that particular place and check that out. The mean number of times the users marked posts as favorites is 0.933, with nine people using it more than once. Although the number is relatively smaller in this case, users did use the feature, and several later reported that they used the feature to visit the places.

6.3.1.5 BLE interactions

Finally, the system relies on BLE encounters to run the web of user-beacons. Therefore, we calculated the number of times a user-beacon encountered other user beacons. Figure 15e shows the actual BLE encounters that happened among the user beacons. Eight users encountered two or fewer user-beacons, seven users encountered 3 to 5 other user-beacons, 13 users encountered 6 to 9 user-beacons, and two others encountered more than ten user-beacons. Therefore it is evident that there was somewhat a good number of BLE-encounters occurred during the study considering the limited number of participants in the event.

6.3.1.6 Characterizing the users based on their usage

With more in-depth analysis from the timelines of the app usages, we characterize the users based on the persistence of their usage.

- **Minimal users:** The participants who created only the required number of posts (2 posts) are characterized as minimal users. Seven users can be categorized as minimal users. By looking into their timelines, we have found that most of the minimal users also used the app for the least total time, ranging from 20 minutes to 40 minutes. Also, they were not checking others' posts and were interacting with the app very little.

- **Regular users:** The participants who created between 3-4 posts are qualified as regular users. There were 19 users we categorize as regular users. They also used the application ranging from 40 minutes to 2 hours. From the timelines,

we can determine that regular users opened 2 to 4 other users' posts and marked at least one post as favorites.

- **Power users:** These are the users who used the app heavily in the festival. They created more than four posts and often used the app for more than 2 hours. They have also marked posts as favorites more (more than two favorites). They also opened more than four posts created by others. Four users qualified as power users.

6.3.2 Survey Results

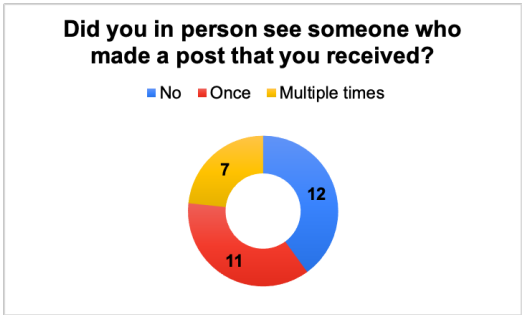
We asked the users to complete a short post-study survey before they redeem their gift cards. Figure 16 shows a summary of the opinions we gathered from the participants.

From 16, we can see that users answered several questions about their experiences using the iFestExplore app. One of the key areas we inquired about was potential identification and interaction with other users. Thus, we asked the users if they had seen someone else who made a post that the user received. 18 of 30 users said, 'yes', and seven said they had seen multiple people who posted around them. We also asked the participants if they had interacted with other users about a post they received. Six of the participants had interacted with others. When asked about their interactions related to the posts they made, ten said that they have interacted with others about the posts they made themselves.

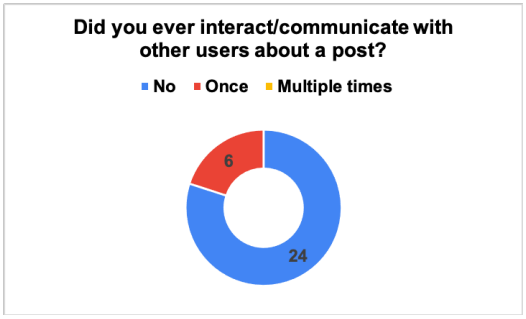
We also wanted to learn users' perceptions of the benefits of the app. We asked the participants how useful this app was in the iFest. On a scale of 1 to 4, 11 of them

Figure 16: Survey Summary.

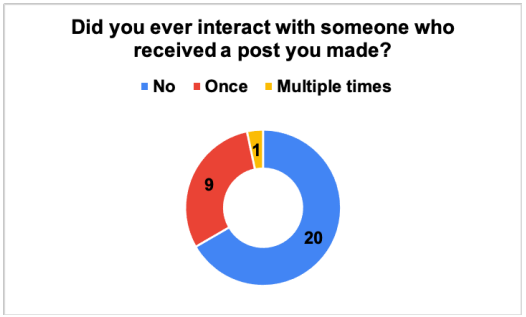
(a)



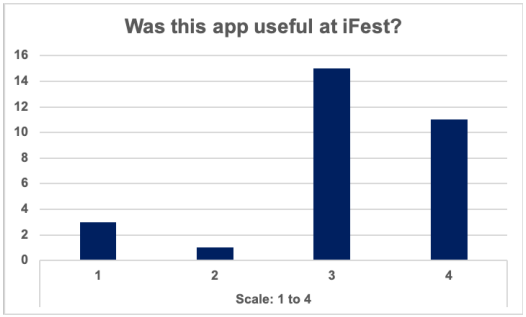
(b)



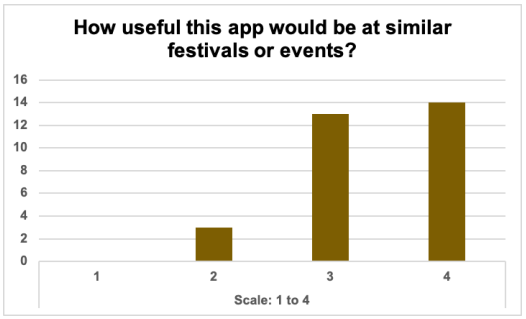
(c)



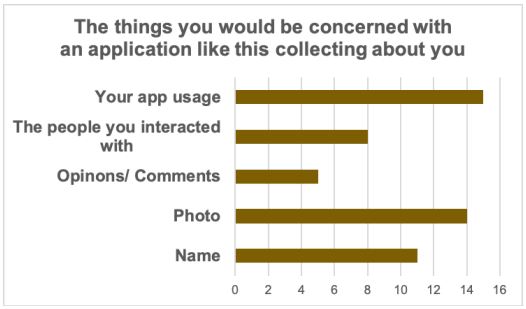
(d)



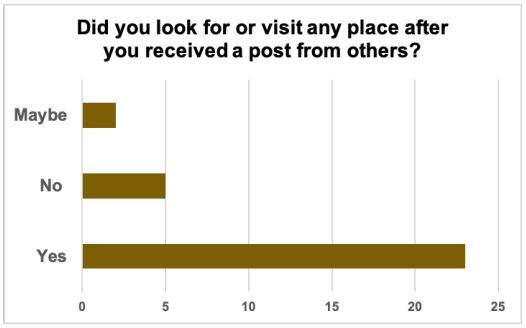
(e)



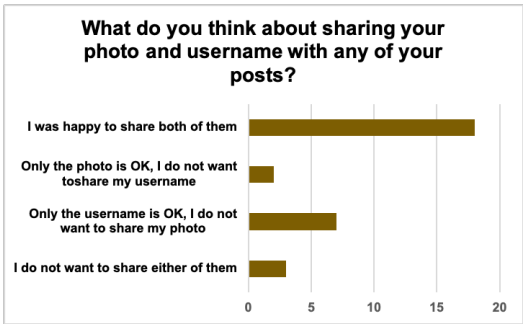
(f)



(g)



(h)



rated it 4, 15 of them rated it 3, two of them rated it 2, and three rated it 1. When we asked about a future deployment to another festival with an improved version of the app, they rated it higher. Fourteen of the participants rated it 4, 13 of them rated it 3, three of them rated it 2, and none rated it 1.

We asked the participants if they visited the places they had received the posts about. We found that 23 out of 30 participants visited the places after seeing the posts they received, which reflects the usefulness of this technology in a localized place like a festival.

Finally, we asked about users' privacy perceptions. We asked participants about the privacy concerns in the survey. Eleven of the participants were concerned about their names being collected by the app. 14 were concerned about their photo being collected, five were concerned about their comments, and 15 were concerned about their app usage. Eight of the participants were worried about the possible interactions this system might create. Besides, we put an open-ended question to know additional privacy concerns. We have found the following additional privacy concerns from the answers:

- The password is not being secured in the back-end, i.e., not-encrypted
- Keeping Bluetooth open may invoke unexpected privacy breaches
- Being spammed
- Physically getting tracked if used beyond a localized area

6.3.3 Post-study interview

We invited all 30 participants for a phone interview after they redeemed their rewards. Eight of them responded, and we interviewed them over the phone. We asked both specific and open-ended questions related to peer-interaction, privacy and exposure, incentives, and system utilization. The interview questions and user demographics can be found in the Appendix. Table 8 shows eight interviewees with their categorizations based on their app usage in the festival.

User ID	**Category**
P1	Power User
P2	Power User
P3	Minimal User
P4	Regular User
P5	Regular User
P6	Power User
P7	Regular User
P8	Regular User

Table 8: Categorized list of interview participants

6.3.3.1 General thoughts

We asked the participants about their overall perceptions of that experience. All of the eight participants but one liked using the application. The other one neither liked it nor disliked it.

One of the power users, P2, said, *"I read the posts. I have seen some people share photos of many things like food and other things. That helped to find food from booths. That gave me a good understanding of how the festival was and what are things I should try."*

Even a minimal user like P3 said that it gave them an excellent opportunity to

explore the festival. Mainly because they were receiving the posts only related to the festival, whereas, if they used any other social media, they would not get much of the needed posts. Moreover, frequent posting about festivals will not be ideal for generic social media postings. In the case of the festival, both the post makers and receivers found it useful.

A regular user, P4 said, *"I think it's good in a sense that in that festival there were many people around and they have so much information to share, but they cannot use regular social apps to share because they cannot reach so many people in a small place like that using them. Otherwise [without this app], it becomes complicated."*

Although the participants liked it, one of the early users, P7, said that there were not many users found to be using the app, so they did not receive many posts. So, as the app was intended for the localized setting, it is critical to accommodate sufficient users in a place to enable the potential of the application. Adding to the positives, one of the power users, P6, said that sometimes a very feature-rich app like Facebook, makes it very complicated to use, and people want easy interfaces. For events, U-a-B can bridge the gap between the contextual features and users' actual needs. Despite being a minimal user, P3 mentioned the app's utility as meeting with friends. One of the participants talked about the network effects over technology becoming a trend. In their opinion, they would feel more comfortable using other social networking platforms, because they already use them, and they are already popular, and people around them use them with confidence. The more people would use a system, the more they would trust the system. In their opinion, they would need more time and more people to use it to get used to the system.

From this subsection, we found that despite having a few concerns about being very new and unknown, people were, in general, very positive about the U-a-B system in the iFest. U-a-B seemed to be a better alternative for generic social media in terms of an event or festival.

6.3.3.2 Receiving posts

We asked the participants about the posts they received at the iFest while using the app, what kind of posts they received, and whether the participants visited the places they have seen in the received posts? All of the participants said that they had received several posts from the people around them. When we asked about the kind of posts they received, the participants talked mostly about foods and mentioned observing activities and ornaments.

The most compelling finding was that six participants said that after seeing posts they received, they visited the places. They utilized the system to find the places they liked. For example, P3, despite being a minimal user, said, *"That has been one of the pictures I saw. It was like one of the foods, so I tried looking for that food in that booth."*

Likewise, the participants paraphrased what they said in the previous subsection, most of the participants said that the app was useful because they received posts of their interests, about foods, different activities, decorative items, and all the other stuff they expected to explore in the festival. P6 said, *"I found some reviews that reflected my interest. I saw other people's reviews and tried to get an idea about different food carts and booths. Then, I visited a few food carts and booths from*

African countries, especially Ghana and Angola. Finally, I shared my reviews with other people."

Thus, from the follow-up interview, it was apparent that people found the system useful to receive the contents of their interest. Also, adding to the previous subsection findings, the users found the system particularly contextual and suitable for a big localized event or a festival.

6.3.3.3 Making Posts

We asked the participants about their general thoughts about being posters themselves. In doing so, we asked the participants about the posts they made, and the reasons and motivations for making those posts. People talked about various things about what they posted, like foods, decorations, and activities. P2 said, *"I love these booths. So I went to this booth. I liked their decorations. I also liked this booth with food. So I just took different pictures and posted with some nice comments."* P4 said, *"I posted a couple of photos of activities near a booth. I guess that was a cultural dance."* Some other participants such as P5 and P6 said that they posted contents about decorative items and desserts.

Helping each other find the things of their interests was the primary motivation for the users to keep posting in iFest. Most of the participants thought that they shared what they believed to be the points of interest of the people around. They found it suitable for the iFest as they were not worried about posting irrelevant content to other users. For example, P2 said, *"I thought I could help people by sharing my experience. They can also try those things. So I just post those things."* Likewise, P4

said, *"I thought of something. If that is interesting to me, I might share, and it may help others."* Also, P6 said, *"I reviewed a specific food from the Bosnia booth because I wanted other people to taste it. To talk about the gift review from the Angola stall, I would say, I liked their traditional gifts and wanted other people to experience them."*

6.3.3.4 Peer Interaction

To understand the perceptions of having face-to-face interactions with peers, we asked the interviewees about the overall perceptions about peer-interactions in the iFest. We specifically asked the participants if they looked for other users and talked to them, or did they expect any kind of peer interaction with other users around themselves. Five out of 8 participants said that they expected at least some kind of interactions. For example, P4 said, *"Yes, of course. They had pictures. It's a very dense place, so I could find a person from their pictures. So if someone is looking for a place, and can't find it. So they might ask."*

A regular user, P7 appreciated the chance of new social interaction by saying, *"So a good way to talk to people, which we don't nowadays like it's usually just virtually talking through social media now. When I'm in Bluetooth proximity, I can [say to someone], hey, you posted this review and I can talk to you about it. I think it's a good way to start."* Interestingly, one user who was one of the power users, P1, said that they had actual interactions with other users. They said, *"It was interesting, I even asked a guy about that Bosnian bread of which I received a post from him."* On the contrary, some of the users did not appreciate peer interactions. For example, P4 did not appreciate peer interactions even though they expected them. They said,

"If there's, there are too many people, then no, I don't appreciate it. Okay, the app could be improved to enable commenting and messaging. I would rather answer the questions in the app."

We also wanted to explore the users' comfort using the system. The participants mentioned that they were more comfortable using the application as it was localized and more focused on the school campus. So the localized context and a familiar and trustworthy population worked very well for the deployment of U-a-B. For example, a power user, P2 said, *"The people were all related to the campus, so I don't have any issue with sharing my personal information there."* They continued, *"So, if it is only my name and pictures, I don't have any problem, especially the familiar school people."* Some users, especially some of the power users, shared their privacy concerns about this communication method in close proximity. A power user, P2 said, *"The user should know, who are the people around, before they go and use this application."* Another power user, P6 said, *"Maybe they would be prone to be biased as they might trust people in the app. And they also have the chance to have sensitive information about myself."*

P6 continued, *"I don't like sharing information with other people when I am close to them. But I have no problem sharing something with other people if I can share anonymously without harming my privacy."* P8 said, *"The system concerns me of security, and privacy. If I am near another Bluetooth device, then I benefit [laughing]. Like if I saw a good girl, nice looking girl, I can know her name and everything."* P8 continued, *"The problem is that if someone, some intruder is around my area, in my Bluetooth proximity, then he will get my information. That is actually, I don't want*

to."

Similar to the last study, some participants talked about the network effects on U-a-B applications. They thought that if U-a-B becomes a trend, people would get used to this technology and use it more. P7 said, *"It's a new concept, so I really don't know at this point how I feel that when I'm around them. But if it becomes, for example, it becomes somewhat popular, I would be more comfortable."*

From the interview, we found that the users mostly accepted the phenomenon of peer interactions when being the user-beacons. However, the people who used the app more had privacy concerns related to proximal tracking, as they understood the system more. They also reflected on the network effects on new technology like U-a-B and identified user habituation as a factor for building up trust in U-a-B usage.

6.3.3.5 General privacy

To explore the privacy scenario, we asked specific questions about general privacy questions about sharing personal information with the people around, location privacy, electronic privacy, and the kind of controls and preferences the users need if they use the application.

About personal information being shared, three participants said that if that is only a name and profile picture, they do not have any problem with that. P3 said, *"As long as it was the name and photo, I think it was fine by me."* However, others were not as comfortable. P4 said, *"I have concerns with any information, I would not put it in the first place."* P4 continued, *"I'm concerned about someone using the picture that I have taken for some other purposes. I'm not comfortable with it. I*

don't want anyone to use the information that I'm posting in the app for some other reasons." P6 said, *"I have concerns sharing my name, photo, and the exact location."* In contrast, users like P7 showed more relaxed opinions, *"When I'm making a post, my picture and a user name and it being shared with people who are near to me, around me. They might not be someone I want to share my information. But then again, it's not a lot of information. It's just my name and picture."*

Moreover, some of the participants expressed concerns about the possibility of proximal tracking. P4 said, *"It's actually broadcasting Bluetooth beacon. So what if someone can physically trace me?."* Also a power user P6 said, *"What if anyone can trace me and find my exact location?"*

In addition, two of the participants talked about electronic privacy concerns, like social tracking and hacking. P2, who happened to be a power user, said, *"I am more concerned about the app tracking me. How would I know, the app will not extract my data?"* Also P3, a minimal user, talked about fake users using the app maliciously, *"People can use your pictures to create fake pictures, which is kind of they can use it to take on somebody."* P3 also talked about reverse-engineering the system and hacking into a user device, *"So people can reverse engineer these things. So on that, I have security concerns."* We also wanted to explore the kind of controls and preferences the users want when using the app to mitigate their privacy and security concerns. People came up with several opinions about usable privacy settings, settings about maintaining civic distance and boundaries, and the settings to keep anonymity.

P5 expressed their opinions about a generic deployment of U-a-B, *"Now, this app was distributed within a certain event, so I would not mind if something is tracking*

me, even my location. But if there was a community-based thing, like if I wouldn't have added a friend, then I have the preference of a civic distancing, the privacy setting that I wanted to share with my friends only I wanted to share."

Some users talked about having the preferences for sharing personal information. Like P6 said, *"I want to have the option to decide whether I am interested in sharing my photo. Having the option to post reviews anonymously."* Also P8 said, *"Control my privacy and [settings] so I can control that. Bluetooth eats up your battery. So I need to shut down the Bluetooth sometimes. So that's like, that's the kind of thing I needed to be included. Like if I have an option to shut down the Bluetooth for some time, then I should have. But if you turn off the Bluetooth. Sometimes I need some time and space for me."* Interestingly, two of the participants mentioned that they are not concerned about using this app if it is in a local environment like a festival.

In general, the perceptions about privacy were not much different than the previous studies. However, they mentioned that the very environment of iFest made the users more comfortable using the system, even though they had several concerns related to proximal tracking, electronic privacy, and personal information. Hence, a festival scenario is a viable environment to deploy U-a-B.

6.3.3.6 Incentives and motivations

We also wanted to investigate the effect of incentives as the motivation for using U-a-B. We asked participants about the incentives they would want and how the incentives would motivate them to use such a system. Seven of eight participants said they would use it without incentives to control their privacy and security settings.

P4 said, *"Yeah, of course, I would use it, but it depends on the security and privacy measures that have been taken. It was this one time [in iFest] I used it. If I find it secure, why not again?"* P5 mentioned that the motivation was more about helping each other than the monetary incentives, *"You hear from other people that are actually at the events and shedding any good information that will help others."* However, despite being a power user, one participant (P6) said they are happy to participate in the studies, but in real life, they are so concerned about the technology's invasive nature that they will not use it. Additionally, we asked the participants about their intentions of using similar applications in future festivals. Moreover, we asked about the other scenarios, such as in a shopping mall or in a restaurant. All but one said that they would use the app in other festivals if it is only within the festival. On the other hand, opinions on using the app in another context were mixed. Two participants thought that the restaurant scenario would be a better fit because they would like to get food reviews. Three of the users liked the shopping mall scenario. However, two people did not like any of the scenarios.

In this subsection, I wanted to understand the effects of incentives as the deciding factor for using the U-a-B system. Interestingly, nobody mentioned the rewards they were earning as the motivation of using the application. Most of them thought that helping each other through the system was the motivation for using the system. Furthermore, the locally constrained format of the festival made it easier to help each other within the festival context.

6.4 Discussion

In this section, we discuss the implications of our study and compare the previous chapters' findings.

6.4.1 Managing Trustworthiness

From the previous studies, we have understood that 'trustworthiness' was one of the most significant benefits of the Users-as-Beacons system. However, there was an apparent tension between being able to trust the contents and content posters and sharing personal information to make the contents more trustworthy. In this study, we have found that participants were seemingly less concerned about their personal information being shared with others due to the very nature of the festival and the constrained context. There was less tension between trustworthy content and sharing their information. Thus, trustworthiness was reflected even stronger than before in the context of iFest. The context of having the people being in a place where their goals coincide makes the system more trustworthy. Although it worked very well in the iFest context, it will still be a challenge to provide users with sufficient awareness of others' access to their personal information and controls to restrict information sharing and maintain privacy in different contexts.

6.4.2 Managing Boundaries

From the previous study, we have learned that there were mixed opinions about peer interactions. Some users were not at all comfortable, yet others embraced the benefits of peer interaction. However, in the iFest, the users' concerns about meeting

others face-to-face was less than the previous study. In fact, several face-to-face interactions happened in the festival setting. The constrained setting of the festival made it viable. Yet, in other contexts, we need to design the system carefully so that peer interaction can remain suitable for the users.

6.4.3 Relevance and Localized Setting

In the previous study, we found that it is vital for the contents to be delivered on time. First of all, the users felt annoyed about too many notifications. Secondly, the users wanted to receive relevant posts, not something that is out of context. And finally, the timing was crucial for content; the users would not appreciate contents that are not valid at the time they received them. In the iFest, people did not mention anything about too many notifications. The main reason was that although many of the participants received many notifications, they were all contextual and helpful. The people came and visited the festival for a common goal, so the posts were relevant. Also, the application was running throughout a limited period. The validity of the contents did not expire until the festival is finished. All these phenomenon contributed to the successful and timely delivery of relevant content throughout the event.

6.5 Summary

In this section, we described the user study we conducted in the iFest. We also discussed our significant findings from the study in section 6.3. We have found that the system works pretty well in the localized festival scenario.

Based on the average number of posts made, the number of times the users opened the notifications, total time spent in the app, and the number of times the favorite

option used by the users, the system utilization was substantial. It means that people found the utility of U-a-B useful in the context of a localized festival environment.

The survey results show similar outcomes. Most of the participants rated the usefulness of the app high (3-4). A large number of users visited places after getting posts related to those places. Although the number of people who interacted with each other was relatively small, the number of people who saw each other posting was large. That means people need time to get familiarized with a U-a-B system to utilize its full potential of social interaction.

From the interviews, we have insightful comments about app usage, peer interactions, and privacy issues. People generally liked the idea of this localized constraint of the app as it delivers a better context. We have seen mixed opinions on privacy, and people talked about several privacy issues related to the system. It needs more research on developing privacy-preserving design guidelines to develop applications using U-a-B.

Both the system utilization, survey results, and the interview opinions from the users proved that the users liked the utility very well, and with a simple to use interface and improved privacy settings this technology is a viable option for a localized social networking system.

In the next chapter, we will discuss the results and their implications. Then we develop design guidelines for future developments.

CHAPTER 7: DISCUSSION AND IMPLICATIONS

7.1 Introduction

In this chapter, I will discuss the overall implications of the U-a-B system in terms of applicability in real life, the appropriate contexts for deploying a U-a-B system, the privacy preservation of the user-beacons, and the design guidelines for future development.

7.2 Revisiting the potential application Scenarios

To begin with discussing the implications, I first revisit the potential application scenarios of U-a-B we initially described. In addition I discuss the applicability of U-a-B in these scenarios.

- Community based social networks: The main idea behind this scenario was to use U-a-B's mechanism to implement a community based localized social networking system. The primary goal was to implement a local proximity based system in campuses or festivals where the users are already in a crowded environment, hence, utilizing the BLE range to communicate. We also discussed the possibility of building up an extension of current neighborhood review systems, such as Nextdoor, utilizing the close proximity of the residents in a neighborhood. This scenario was explored in study 2, and was the kind of system deployed in study 3.

- Localized advertising platform for shopping areas: Another idea was to deploy a U-a-B system in a large shopping area, where there will be a large number of visitors. There U-a-B system can be utilized to disseminate offers from different shops, coupons, and so on. This scenario was used in study 1.

- Instant review platform for shopping areas: Utilizing U-a-B as a method of user generated content sharing in shopping areas was the idea behind this application. Similar to the previous application scenario, in this case the users themselves create reviews and transmit to other users nearby, as a localized instant product review system. We explored this scenario in study 2.

- Crowd-sourced localized platform for reviewing places: We also thought beyond the shopping areas in this application scenario. The primary idea was to deploy a U-a-B system for reviewing places and restaurants, extending current place review systems such as Yelp and Google. We also explored this scenario in study 2.

7.3 Finding the appropriate context

To find the appropriate context for deploying a U-a-B system, we need to think about a few aspects: the localized nature of the technology, the users' needs for communicating with others, and the utilities it can provide better than the current systems. U-a-B is driven by Bluetooth, and the interactions happen within the Bluetooth signal range. The range is limited and to make the interactions among the devices possible, U-a-B systems are only useful when users would be nearby.

The very design of the Users-as-Beacons system requires a localized deployment.

From the previous studies, we have explored the users' perceptions of this localized nature. Study participants like the concept of U-a-B for most of the potential deployment scenarios, except for a few concerns regarding interaction with business management and proximity tracking. However, many users expressed their opinions against receiving all sorts of content, which might be irrelevant and untimely. In study 3, users did not mention any of the concerns about irrelevance or untimely content delivery. The main reason behind that was the nature of the deployment environment, where it was crowded, concise, and people had a common purpose for using it. It demonstrates that if the context is entirely localized, U-a-B works very well.

Another crucial part of a U-a-B system is the possibility of having face-to-face peer interactions. In all the studies, most of the participants anticipated peer-interactions, with mixed reactions. In study 2, most of the participants were anxious about face-to-face interaction with strangers although a few found the idea intriguing. However, in study 3, there was little anxiety, mainly because the notion of trustworthiness was much higher in the festival. The visitors had a common purpose, and it was confined to the festival arena. Therefore, an appropriate context and proper design of U-a-B around it mitigate the anxiety of meeting strangers and may even be viewed as beneficial.

Moreover, in the festival study, most of the participants found the system useful, mainly because they came to visit iFest, and they were receiving posts about points of their interests. Also, they could post as many posts as they wanted using the app, which they probably would not do in more generic social media applications.

Therefore, the U-a-B system gave users a more focused context that made the app useful. Also, the notion of trustworthiness was also echoed in study 3, where the context of the festival was perfect for mutual trust among the user-beacons. Thus, defining the context is very important to reap the potential benefits of a Users-as-Beacons system.

7.4 Privacy implications

In this section, I am going to discuss the overall privacy implications from the work I conducted in this dissertation. In chapter 3, I discussed how users reacted to the content sensitivity and public exposure. In chapter 4, I discussed the overall privacy perceptions for potential use cases of Users-as-Beacons. Subsequently in chapter 6, I discussed how participants reacted to a real life application scenario.

7.4.1 Information disclosure and privacy trade-off

Trustworthiness is one of the major benefits of a Users-as-Beacons system, and a user-beacon must be real and trusted. The users need to develop mutual trust in order to develop a community utilizing U-a-B. This may require disclosure of personal information to express the user's identity and establish trust among other users. Nevertheless, this disclosure might make users identifiable to strangers and leavetheir opinions exposed to the public. In turn, this might necessitate users to trade-off their privacy for reliability and trustworthiness of the system.

Throughout the studies, we investigated participants' opinions about disclosing their personal information to others. In chapter 3 we found the direct effect of incentives in disclosing the private information to others. We have found that incentives

create a new motivation for the users to share their identifiable information to others. Also, users seeing others earning more points by disclosing more information can create a competition effect in a localized environment, and lead people to be willing to disclose information.

In chapter 4 we investigated what information the users think is appropriate to make a user profile reliable in U-a-B, and what is the identifiable information the users would share with others for the sake of realism and trust. Most of the participants did not want to share their full names, as it is greatly identifiable. However, only sharing their first names was acceptable for many of them. The very localized nature of a U-a-B system made many of the users desire to not share their photo. Also, BLE is used to estimate location of the beacons. Hence, tracking a user-beacon is very much possible. There is an existential concern of the users where they might be physically tracked by strangers, and the concern amplifies with sharing their identifiable information.

The opinions of the participants in chapter 4 was on a hypothetical system that we portrayed to the users. In chapter 6 we described a real life deployment of a fully working prototype of a U-a-B system. Once the users experienced a real system their perceptions changed slightly. More people were agreeing to share their name and photo. This would be the result for the festival being a very good fit for a localized proximity based system to be deployed. People found it useful and the people around trustworthy enough to feel safe sharing identifiable information about themselves. The concern about physically getting tracked is still an issue with the system in the festival. However, as the app was only limited to a particular event, the number of users who were concerned was much lower.

7.4.2 Location privacy

One of the biggest benefits of a U-a-B system is that it does not require GPS location to provide contextual information. This also make U-a-B resilient from GPS spoofing. Also, if used in an entirely localized context, a person's daily activities cannot be traced as it can be done using GPS. However, it is not entirely immune to physical tracking through location estimation. The good news is there are plenty of mechanisms that have been researched to prevent BLE users from being traced by implementing preventative security measures, hence ensuring user privacy and security.

In chapter 4 we explored the users' perceptions on the U-a-B being a location privacy preserving way of communicating locally. We described the utility of U-a-B as a non-GPS-based system. Many people understood the utility, however, it did not seem to be a matter of concern to most of them. Most of the participants did not worry too much about their location being tracked by GPS. Hence, they did not particularly value the potential for location privacy. Some of the participants even preferred that their locations be tracked through GPS to get tailored contents based on their locations.

Moreover, in the festival study (chapter 6), the participants were mostly ignorant about location privacy, specifically about GPS tracking. The primary reason behind that was the participants could engage more with their peers and blend into the localized context. Also, they knew that the app was limited to the festival alone, so they were not thinking much about location tracking. In all the studies, there were

a portion of people who did not worry much about location tracking, even some who wanted their location to be tracked for better contextual information.

Thus, in the end, users did not value the location privacy benefits offered by a U-a-B system. Participants still expressed concerns about being tracked, even thought GPS would not be utilized. In certain scenarios, concerns over the relevance of content was more important, leading many to want customization based on their location. Thus, the adoption and use of U-a-B in these social situations may not be dependent on users' location privacy desires.

7.4.3 Managing boundaries in peer-interaction

Peer interaction is a key component in U-a-B based social systems. In a U-a-B system, people interact with others who are within the BLE range; hence it enables the users to communicate with the people nearby. That provides people with two aspects of communicating with peers: (i) virtual one-to-one communication, and (ii) verbal face-to-face discussion with nearby users. Although virtual communication is widespread in other social platforms, the addition of the chance for verbal face-to-face communication gives a new notion of social interaction through the system. It incurs additional privacy issues related to physical proximity to other users.

We investigated the opinions of the users in-depth in chapter 4. We have seen that some of the users raised concerns about the face-to-face interactions in U-a-B, and were reserved about sharing identifiable personal information as a result. One reason behind that was they had not used such a system before. Another reason was that they did not want to encounter strangers talking about posts they made.

Moreover, the fear of being stalked and tracked by malicious users amplified the concerns. Participants also raised discomfort about being approached by business management should they leave comments or reviews about that business. On the other hand, some other users appreciated interacting with other people and saw it as a chance to make new friends.

Interestingly, in chapter 6, we found that most of the people liked the peer interaction. The main reason was that people came to visit the festival for a common goal, and they were receiving useful content. Also, the system was confined to the festival area, and people liked to interact with other visitors within that area. Deploying it to an appropriate environment enabled suitable peer-interaction opportunities, and the users embraced it.

7.4.4 Managing trust

Mutual trust among the users is another key pillar of social networks. It is more essential in the perspective of a U-a-B system, where peer-interaction is expected to be more in person. We investigated the issues related to the trustworthiness among the users in U-a-B. In chapter 4 we discussed that the participants found trust as one of the biggest benefits of a U-a-B system, because in U-a-B it is comparatively more difficult to make fake posts. However, to deliver trustworthy contents, there is a need for sharing more identifiable personal information. So, it creates a tension between the desire to remain private and being able to know and trust other users. Network effects comes into play in this situation. User familiarity and user trust in the system would grow over time with more usage in appropriate contexts.

7.4.5 Motivations and Incentives

Finally, in order for the users to use a Users-as-Beacons system, they need proper motivations. Moreover, without the proper number of users, U-a-B would not have ample user-beacons to operate successfully. So, there is a need for viable motivations in order for a successful deployment of U-a-B. As we have learned from the first study, if we monetize people as incentives to use the system and generate content, the users competitively create content to earn more rewards. According to the findings of the second study, it becomes a matter of discomfort if the timeliness and relevance of the contents are not accurate. In that case, incentives became a significant motivation. Also, there is a tension between sharing more information and earning incentives and people may trade-off privacy with monetary incentives.

However, if the context is well-defined, where the relevance and timeliness of the contents are suitable, the people's perception of the incentives changes. In the final user study, we learned that many participants were motivated to use the system because they were helping each other. Nobody expressed a need for monetary incentives for future deployment. Therefore, the motivation for using a U-a-B system depends much on the context of deployment. If the context is well suited, people appreciate their use and participate without incentives. Nevertheless, it is a challenge to design the deployment for a broader context as well as ensuring proper motivation.

7.5 Privacy preserving design guidelines

From the outcomes of the previous studies, it is evident that Users-as-Beacons is a viable privacy-preserving system having the utility to be deployed in several social

and advertising contexts. However, to make sure it works the way it is intended, we need to design a U-a-B system carefully based on the target environment, coverage area, the users' expectations and needs, and their privacy perceptions. Therefore, In this following, I propose a design guideline for the future development.

- Context
  - Users-as-Beacons is a local proximity-based technology, where each user becomes a user-beacon transmitting IDs toward their vicinity. Thus, the targeted deployment environment should be carefully measured to facilitate proper utility. Therefore, a future developer should carefully identify the context and limit the use of the application within that specific context.
  - Timely delivery of relevant content is essential for the successful deployment of a Users-as-Beacons system. Otherwise, the users might receive content either irrelevant or expired. Therefore, a developer must identify strategies for making content contextual to the user.
  - Peer-interaction is a crucial part of a U-a-B system. There is a tension among numerous users to meet other user-beacons face-to-face. In that case, the users would need proper controls and preferences to limit face-to-face peer interactions. Any developer should consider the applicability of localized peer-interaction within that context, and methods to reduce the likelihood of such interaction if users have concerns about peer interaction.
  - From chapter 6 we understood that U-a-B works very well in a localized setting, like a local festival or event. So it would be a good idea to consider

keeping the context limited to a locality to keep the contents relevant.

  - U-a-B might work very well in a broader context too. However, it is a challenge to keep the contexts relevant if extended beyond a small locality. Therefore, if the application's context is not limited, the developer should provide the users with controls and preferences to customize their interests.

- Security and Privacy

  - The very design of U-a-B requires real BLE enabled devices to be broadcasting, hence it is challenging to create a fake beacon; someone has to be physically at a place to broadcast fake Beacon IDs. Yet, it is possible to deploy fake beacons. Thus, it is essential to implement preventive Bluetooth security measures against fake beacons.

  - BLE being a technology built and run on Bluetooth, it is vulnerable to all Bluetooth vulnerabilities, so is U-a-B. There have been plenty of security and privacy mechanisms to prevent systems from getting hacked through back-doors. Any developer should implement preventive Bluetooth security measures against hacking through Bluetooth back-doors.

  - BLE is primarily used for proximity estimation. So one BLE beacon can be used to track another beacon and measure proximity. Thus, it is very much possible for a user-beacon in a U-a-B system to trace another user beacon if there is not any preventive measures taken. A developer must implement preventive measures against proximal tracking for physical tracking.

  - We have seen that a localized, crowded environment works the best for a

U-a-B system. However, the more localized it gets, the denser the user-beacons in the area become. Thus, it might create some discomfort concerning the disruption of their private space. So the developer should carefully plan the localized contexts for applications to accommodate the user's private space.

– Information disclosure is a crucial part of making the user-beacon contents reliable to other user-beacons. If the environment is constrained and localized, the users find it comfortable and do not worry much about sharing information. However, if the context is beyond a well-defined and limited space, adequate user controls should be implemented over their information disclosure.

7.6 Conclusion

In this dissertation, I have proposed a novel system "Users-as-Beacons," built on top of the current BLE technology. This dissertation's primary goal was to explore the possibility of deploying this system in potential application scenarios, including a localized advertising platform for shopping areas, a crowd-sourced localized platform for reviewing places, and a community-based social network. Throughout the dissertation, I explored the users' perspectives on the system in different contexts, identified the design challenges, designed and developed a working prototype, and deployed it in a localized festival scenario. Finally, I have discussed design guidelines for future development. I will continue to explore the other potential contexts that fit well as a U-a-B system in the future.

REFERENCES

[1] Android studio— android developers. https://developer.android.com/studio. Accessed: 2020-1-15.

[2] Bluetooth is everywhere consumers hang out. https://www.bluetooth.com/what-is-bluetooth-technology/where-to-find-it/consumer-electronics. Accessed: 2017-08-19.

[3] Decentralized privacy-preserving proximity tracing. https://github.com/DP-3T/documents. Accessed on: 2020-06-02.

[4] Gartner says 4.9 billion connected. https://www.gartner.com/newsroom/id/2905717. Accessed: 2019-1-16.

[5] ifestexplore project on github. https://github.com/sakibnm/iFestExploreV2. Accessed: 2020-1-15.

[6] Smart industry — bluetooth technology website. https://www.bluetooth.com/markets/smart-industry. Accessed: 2019-1-15.

[7] Tracetogether. https://www.tracetogether.gov.sg/. Accessed: 2020-3-15.

[8] Brand enforcement program — bluetooth technology special interest gro.... https://archive.is/20131104093347/https://www.bluetooth.org/en-us/bluetooth-brand/brand-enforcement-program, Nov. 2013. Accessed: 2019-1-15.

[9] D. Anthony and L. Patrik. Droidbox: An android application sandbox for dynamic analysis. https://www.honeynet.org/gsoc2011/slot5. Accessed: 2017-07-17.

[10] S. Banerjee, S. Bhattacharyya, and I. Bose. Whose online reviews to trust? understanding reviewer trustworthiness and its impact on business. *Decis. Support Syst.*, 96:17–26, Apr. 2017.

[11] J. Bay, J. Kek, A. Tan, C. S. Hau, L. Yongquan, J. Tan, and T. A. Quy. BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders. *Government Technology Agency-Singapore, Tech. Rep*, 2020.

[12] Beaconstac. What is a bluetooth beacon? how do beacons work? https://www.beaconstac.com/what-is-a-bluetooth-beacon. Accessed: 2019-1-29.

[13] E. Bello-Ogunu and M. Shehab. Crowdsourcing for context: Regarding privacy in beacon encounters via contextual integrity. *Proceedings on Privacy Enhancing Technologies*, 2016(3):83–95, July 2016.

[14] E. A. Bello-Ogunu. *A framework for user-centric privacy management in smartphones regarding bluetooth low energy beacons*. PhD thesis, The University of North Carolina at Charlotte, 2016.

[15] M. Benisch, P. G. Kelley, N. Sadeh, and L. F. Cranor. Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs. *Personal Ubiquitous Comput.*, 15(7):679–694, Oct. 2011.

[16] 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*, SOUPS '10, pages 7:1–7:10, New York, NY, USA, 2010. ACM.

[17] L. Brendon. Location and privacy: Where are we headed on data privacy day? https://blogs.microsoft.com/on-the-issues/2011/01/26/location-and-privacy-where-are-we-headed-on-data-privacy-day/. Accessed: 2017-10-01.

[18] S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge. Location disclosure to social relations: Why, when, & what people want to share. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '05, pages 81–90, New York, NY, USA, 2005. ACM.

[19] M. J. Culnan. " how did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS quarterly*, pages 341–363, 1993.

[20] Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel. Unique in the crowd: The privacy bounds of human mobility. *Sci. Rep.*, 3:1376, 2013.

[21] R. Edmonds. People don't want to trade privacy for targeted ads. https://www.poynter.org/news/people-dont-want-trade-privacy-targeted-ads. Accessed: 2017-07-11.

[22] R. Faragher. An analysis of the accuracy of bluetooth low energy for indoor positioning applications. 2014.

[23] K. Fawaz, K.-H. Kim, and K. G. Shin. Privacy vs. reward in indoor Location-Based services. *Proceedings on Privacy Enhancing Technologies*, 2016(4):901, Jan. 2016.

[24] K. Fawaz and K. G. Shin. Location privacy protection for smartphone users. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 239–250, New York, NY, USA, 2014. ACM.

[25] A. Fayazi, K. Lee, J. Caverlee, and A. Squicciarini. Uncovering crowdsourced manipulation of online reviews. In *Proceedings of the 38th International ACM SIGIR Conference on Research and Development in Information Retrieval*, SIGIR '15, pages 233–242, New York, NY, USA, 2015. ACM.

[26] D. Fisher, L. Dorner, and D. Wagner. Short paper: Location privacy: User behavior in the field. In *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, SPSM '12, pages 51–56, New York, NY, USA, 2012. ACM.

[27] C. Forman, A. Ghose, and B. Wiesenfeld. Examining the relationship between reviews and sales: The role of reviewer identity disclosure in electronic markets. *Information Systems Research*, 19(3):291–313, 1 Sept. 2008.

[28] S. Gao, J. Ma, W. Shi, G. Zhan, and C. Sun. Trpf: A trajectory privacy-preserving framework for participatory sensing. *IEEE Transactions on Information Forensics and Security*, 8(6):874–887, 2013.

[29] J. Gomez, T. Pinnick, and A. Soltani. Knowprivacy: The current state of web privacy, data collection, and information sharing. school of information. *University of California Berkeley. www. knowprivacy. org*, 2009.

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

[31] S. Guha, B. Cheng, and P. Francis. Privad: Practical privacy in online advertising. In *Proceedings of the 8th USENIX Conference on Networked Systems Design and Implementation*, NSDI'11, pages 169–182, Berkeley, CA, USA, 2011. USENIX Association.

[32] 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*, CHI EA '06, pages 833–838, New York, NY, USA, 2006. ACM.

[33] H. Haddadi, P. Hui, and I. Brown. Mobiad: Private and scalable mobile advertising. In *Proceedings of the Fifth ACM International Workshop on Mobility in the Evolving Internet Architecture*, MobiArch '10, pages 33–38, New York, NY, USA, 2010. ACM.

[34] S. S. Hansen, J. K. Lee, and S.-Y. Lee. Consumer-generated ads on YouTube: Impacts of source credibility and need for cognition on attitudes, interactive behaviors, and eWOM. *Journal of Electronic Commerce Research*, 15(3):254, 2014.

[35] T. Higuchi, P. Martin, S. Chakraborty, and M. Srivastava. Anonycast: Privacy-preserving location distribution for anonymous crowd tracking systems. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '15, page 1119–1130, New York, NY, USA, 2015. Association for Computing Machinery.

[36] K. Hill. 'baby monitor hack' could happen to 40,000 other foscam users. https://www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/. Accessed: 2017-10-01.

[37] G. Iachello, I. Smith, S. Consolvo, G. D. Abowd, J. Hughes, J. Howard, F. Potter, J. Scott, T. Sohn, J. Hightower, and A. LaMarca. Control, deception, and communication: Evaluating the deployment of a location-enhanced messaging service. In *Proceedings of the 7th International Conference on Ubiquitous Computing*, UbiComp'05, pages 213–231, Berlin, Heidelberg, 2005. Springer-Verlag.

[38] T.-M. C. Jai, L. D. Burns, and N. J. King. The effect of behavioral tracking practices on consumers' shopping evaluations and repurchase intention toward trusted online retailers. *Computers in Human Behavior*, 29(3):901 – 909, 2013.

[39] K. Joel and M. Michael. Poll: Consumers concerned about internet privacy. http://consumersunion.org/news/poll-consumers-concerned-about-internet-privacy/ . Accessed: 2017-07-11.

[40] M. Johnson, S. Egelman, and S. M. Bellovin. Facebook and privacy: It's complicated. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 9:1–9:15, New York, NY, USA, 2012. ACM.

[41] P. G. Kelley, R. Brewer, Y. Mayer, L. F. Cranor, and N. Sadeh. An investigation into facebook friend grouping. In *Human-Computer Interaction – INTERACT 2011*, pages 216–233. Springer Berlin Heidelberg, 2011.

[42] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall. A conundrum of permissions: Installing applications on an android smartphone. In J. Blyth, S. Dietrich, and L. J. Camp, editors, *Financial Cryptography and Data Security*, pages 68–79, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[43] H. Krasnova, E. Kolesnikova, and O. Günther. " it won't happen to me!": Self-disclosure in online social networks. page 343, 01 2009.

[44] J. Krumm. A survey of computational location privacy. *Pers. Ubiquit. Comput.*, 13(6):391–399, Aug. 2009.

[45] O. Lara. Ad blocker usage is up 30% — and a popular method publishers use to thwart it isn't working. http://www.businessinsider.com/pagefair-2017-ad-blocking-report-2017-1. Accessed: 2017-10-01.

[46] B. Lawrence, S. Fournier, and F. Brunel. When companies don't make the ad: A multimethod inquiry into the differential effectiveness of Consumer-Generated advertising. *J. Advert.*, 42(4):292–307, Oct. 2013.

[47] 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*, SOUPS '13, pages 7:1–7:12, New York, NY, USA, 2013. ACM.

[48] Y. Liu and A. Simpson. Privacy-preserving targeted mobile advertising: requirements, design and a prototype implementation. *Softw. Pract. Exp.*, 46(12):1657–1684, 1 Dec. 2016.

[49] M. Luca and G. Zervas. Fake it till you make it: Reputation, competition, and yelp review fraud. *Manage. Sci.*, 62(12):3412–3427, Dec. 2016.

[50] C. Mathwick and J. Mosteller. Online reviewer engagement: A typology based on reviewer motivations. *J. Serv. Res.*, 20(2):204–218, May 2017.

[51] C. Matthew. 2017 adblock report. https://pagefair.com/blog/2017/adblockreport/. Accessed: 2017-10-01.

[52] A. M. McDonald. Cookie confusion: Do browser interfaces undermine understanding? In *CHI '10 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '10, pages 4393–4398, New York, NY, USA, 2010. ACM.

[53] S. Mittal. Proximity marketing examples: 28 retail companies nailing it with their campaigns. https://blog.beaconstac.com/2016/02/25-retailers-nailing-it-with-their-proximity-marketing-campaigns/. Accessed: 2019-1-22.

[54] S. Patil, G. Norcie, A. Kapadia, and A. J. Lee. Reasons, rewards, regrets: Privacy considerations in location sharing as an interactive practice. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 5:1–5:15, New York, NY, USA, 2012. ACM.

[55] J. Phelps, G. Nowak, and E. Ferrell. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, 19(1):27–41, 2000.

[56] L. Ponemon. Database security 2007: Threats and priorities within it database infrastructure,. http://www.usfsp.edu/gkearns/Articles2/Database_Security_2007.pdf. Accessed: 2017-07-11.

[57] L. Privat. U.s. consumers reject in-store tracking said survey. https://www.opinionlab.com/newsmedia/u-s-consumers-reject-in-store-tracking-said-survey/. Accessed: 2017-10-05.

[58] L. Rainie and M. Duggan. Privacy and Information Sharing. Technical report, Pew Research Center, 01 2016. Accessed: 2017-07-12.

[59] P. M. Regan, G. FitzGerald, and P. Balint. Generational views of information privacy? *Innovation: The European Journal of Social Science Research*, 26(1-2):81–99, 2013.

[60] C. S. The contribution revolution. https://hbr.org/2008/09/harvard-business-ideacast-113.html. Accessed: 2017-07-17.

[61] N. Sadeh, J. Hong, L. Cranor, I. Fette, P. Kelley, M. Prabaker, and J. Rao. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal Ubiquitous Comput.*, 13(6):401–412, Aug. 2009.

[62] T. Schulz, F. Golatowski, and D. Timmermann. Secure privacy preserving information beacons for public transportation systems. In *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, pages 1–6, 2016.

[63] H.-P. Shih, K.-H. Lai, and T. C. E. Cheng. Constraint-based and dedication-based mechanisms for encouraging online self-disclosure: Is personalization the only thing that matters? *Eur J Inf Syst*, 26(4):432–450, 1 July 2017.

[64] J. Staddon, D. Huffaker, L. Brown, and A. Sedley. Are privacy concerns a turn-off?: Engagement and privacy in social networks. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 10:1–10:13, New York, NY, USA, 2012. ACM.

[65] G. Sterling. Report: 93 percent of US baseball stadiums have deployed beacons - marketing land. https://marketingland.com/report-93-percent-us-baseball-stadiums-deployed-beacons-186677, Aug. 2016. Accessed: 2019-1-22.

[66] L. J. Strahilevitz. A social networks theory of privacy. *The University of Chicago Law Review*, pages 919–988, 2005.

[67] A. Tawfiq and B. Richard. The privacy paradox: The role of cognitive absorption in the social networking activity. In *ICIS 2015 Proceedings*. aisel.aisnet.org, 2015.

[68] A. Thamm, J. Anke, S. Haugk, and D. Radic. Towards the Omni-Channel: Beacon-Based services in retail. In *International Conference on Business Information Systems*, volume 255, pages 181–192, July 2016.

[69] 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*, UbiComp '10, pages 129–138, New York, NY, USA, 2010. ACM.

[70] V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum, and S. Barocas. Adnostic: Privacy preserving targeted advertising. 2010.

[71] J. Turow, M. Hennessy, and N. A. Draper. The tradeoff fallacy: How marketers are misrepresenting american consumers and opening them up to exploitation. 2015.

[72] I. Ullah, R. Boreli, S. S. Kanhere, and S. Chawla. ProfileGuard: Privacy preserving obfuscation for mobile user profiles. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, WPES '14, pages 83–92, New York, NY, USA, 2014. ACM.

[73] Y. Wang, G. Norcie, S. Komanduri, A. Acquisti, P. G. Leon, and L. F. Cranor. "i regretted the minute i pressed share": A qualitative study of regrets on facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, pages 10:1–10:16, New York, NY, USA, 2011. ACM.

[74] H. Xu, X. R. Luo, J. M. Carroll, and M. B. Rosson. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, 51(1):42 – 52, 2011.

[75] Y. Yao, Y. Huang, and Y. Wang. Unpacking people's understandings of bluetooth beacon Systems-A Location-Based IoT technology. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[76] D. Zhang, L. Zhou, J. L. Kehoe, and I. Y. Kilic. What online reviewer behaviors really matter? effects of verbal and nonverbal behaviors on detection of fake online reviews. *Journal of Management Information Systems*, 33(2):456–481, Apr. 2016.

[77] V. Zwass. Co-Creation: Toward a taxonomy and an integrated research perspective. *International Journal of Electronic Commerce*, 8 Dec. 2014.

APPENDIX A: Supplementary data for chapter 4

A Demographics of the participants

Tables 9 and 10 show the demographics of 27 participants.

ID	Gender	Education	Occupation	Has computing degree?
P1	Female	Bachelor's degree	Doctoral student	No
P2	Female	Bachelor's degree	Homemaker	No
P3	Male	Post-graduate degree	Doctoral student	No
P4	Male	Bachelor's degree	Graduate student	Yes
P5	Female	Bachelor's degree	Physician	No
P6	Male	Bachelor's degree	Graduate student	No
P7	Female	Some college, no degree	College student	No
P8	Female	Bachelor's degree	Graduate student	No
P9	Female	Post-graduate degree	Career adviser	No
P10	Female	Post-graduate degree	Higher Education Administrator	Yes
P11	Female	Some college, no degree	College student	No
P12	Male	Some college, no degree	College student	No
P13	Female	Post-graduate degree	Program Specialist	No

Table 9: Demographics of the participants in study 1

B Interview Questions

Study 1

- Scenario one, signing up and creating posts: We discuss the functionality of our system to the participant and guide them on how to use the design probe to sign up and create a post. Then we ask the following questions:
  - How do think of the system? How do you think about deploying real users to create this kind of reviews?

ID	Gender	Education	Occupation	Has computing degree?
P21	Male	Bachelor's degree	Graduate student	Yes
P22	Female	Bachelor's degree	Graduate student	Yes
P23	Male	Post-graduate degree	Doctoral student	Yes
P24	Male	Bachelor's degree	Graduate student	Yes
P25	Male	Bachelor's degree	Graduate student	No
P26	Male	Associate degree	College student	Yes
P27	Female	Post-graduate degree	Health Educator	No
P28	Female	Post-graduate degree	Instructional designer	No
P29	Female	Bachelor's degree	Instructional designer	No
P30	Male	Bachelor's degree	Education Administration	No
P31	Female	Post-graduate degree	Instructional designer	Yes
P32	Female	Bachelor's degree	Instructional designer	No
P33	Female	Bachelor's degree	Graduate student	Yes
P34	Male	Some college, no degree	College student	No

Table 10: Demographics of the participants in study 2

  - What comes to your mind when you see the actual post advertised by you popped up on another user's device? Could you explain?
  - What comes to your mind when you see a person recognizes you by looking into an ad they just received?

- Scenario two, receiving ads:
  - What do you think about receiving posts from the people around?
  - How do you feel about your personal information being shared with the ads?
  - What comes to your mind when you see a person recognizes you by looking into an ad she just received?
  - Now that you know I can see your information too, if you had chance,

would you want to customize the ads more?

- Scenario three, different places:
  - Your device will work as a beacon. Also, you will keep earning money if you continue to post to your surroundings. Would you keep it broadcasting when you are in a different shop?
  - What about after shopping, you pay a visit to your doctor?
  - Then, you go to a restaurant to have dinner with friends?
  - What about when you are at your home with your family?
- Scenario four, control over the system:
  - Assume that this rewards program also gives you to control the time, meaning you can say broadcast this ad 5 minutes later to the people around. In the meantime, you can leave the area. Would you do that?
  - You are using the store app from store 'A' and signed up for being a user-beacon. You recently bought a microwave oven, and you did not like it. So you visited the store and returned it. You decided to post that particular product with a proper user review. After posting, you left the store and went to another store. 5 minutes later you got a call from Bob, one of your friends. He told you that he was visiting "A" and received your ad about that microwave oven. How do you feel? Do you feel comfortable with your ads being public in store after you leave? How would you explain?
  - What are the other controls and preferences would you want in the system?

- Scenario five, product types:
  - Do your preferences change based on the product types? What kind of products would you think you would post about?
  - If you earned rewards, would you post all kinds of products? Would it change your mind anyway?
- Scenario six, peer influence:
  - Imagine that you visited a store and went to the health-care aisle. You need to buy an ointment for your skin problem skin problems. However, you suddenly received a post for the same type of ointment you want to buy. You then discovered that the ad was posted by a person standing right next to you. How would you feel?
  - Would you want to talk to them in detail about that product?
  - After watching a person nearby advertising a sensitive product, do you feel encouraged to share your own experience with the product too?
  - If there were rewards, how would that change your mind?
- Final questions:
  - Would you use this system in real life?
  - Are you worried about your privacy being hampered here?
  - Would you explain any specific privacy concern that comes to your mind related to this system? Why do you think that it could happen?

  - Who are you concerned about getting your information?
  - If you can earn redeemable points through advertising, would you consider advertising on behalf of the stores? Could you explain why you would trade off?
  - What are the benefits do you think will you get if you use this kind of advertising methods?
  - Would you advertise it voluntarily considering the benefits you get? If not, why would not you do that?

Study 2

- Scenario one, signing up and receiving posts: We discuss the functionality of the system and guide them to sign up and use the design probe. Then the interviewer sent two posts about a restaurant, and service recommendation. Then they were asked the following questions:
  - What do you think about receiving the ads throughout the day?
  - Would it matter the kind of reviews you might receive?
  - They might be the restaurants, might be services or even social causes? Would that matter?
  - Do you have any preferences over a certain type of reviews?
- Scenario two, creating posts: The participants were asked to create two posts about a small business and a social cause.

  - How do you feel about other people around you receiving the reviews?
  - What do you think of sharing your personal information along with the reviews?
  - You are sharing your username, first name, last name, and photo.
  - Would you want to customize the reviews? What kind of customization preferences would you want there?
  - You can keep the beacon of your device transmitting throughout the day, wherever you go. There could be different kinds of people around you. Would it matter for you wherever you are and what you are doing? E.g., at home, shopping, walking, working out, at a party, etc.?
  - How would you think of writing reviews for small businesses, social causes, or restaurants, services, etc.?

- Scenario three, instant reviews:
  - Assume that you went to a restaurant nearby. You did not like the behavior of the waiter. Would you write a review in that restaurant right away to let other people there know? Why, or why not?
  - If you really liked the experience there, would you do an instant review?
  - What are the contexts do you think the instant reviews could be implemented in?

- Scenario four, reviewing small businesses:

  - Imagine that recently people from pest-control service worked in your home for a bedbug infestation (very good job). They run a small pest-control business. Would you use this platform to write a review and recommend it to people around you?
  - What kind of factors would you consider if you are asked to write a recommendation for that, that will go around with you the whole day?

- Scenario five, contextual controls and preferences:
  - Imagine that you are at a birthday party with your family and friends. How would you feel about being around family and friends and sharing the reviews?
  - How about being in a club around different kinds of people? How would you feel about strangers receiving the reviews? How would you feel about in the possibility that the people in various places may recognize you, or could come and talk to you about the reviews?
  - What are the controls/preferences do you think this system should facilitate to avoid uncomfortable social interactions?

- Final questions:
  - What kind of information would you want to receive about how your reviews are being received and read? Would it make it more or less comfortable to know, how many people receive your reviews, or how frequently? Do you think that would matter?

  - Do you have any concern about your privacy being hampered here? Would you think about scenarios using this system where you might face privacy threats?
  - What are things that might motivate you using this system? What kinds of incentives or rewards would motivate you to use such a system?
  - Would you do it voluntarily for anything? When would you require incentives? When would incentives not matter? What are the aspects do you think the concept of incentives will bring in this system? Is there any situation where no matter how much rewards you get, you would not review?

C Survey questionnaire

- Email address: _____
- Background Questions
  - What is your gender?
    * Male
    * Female
    * Other
    * Prefer not to say
  - What is your age?
    * 18-24
    * 25-34

    - 35-54
    - 55 or more
  - Which of the following best describes your highest achieved level of education?
    - High school
    - Some college, no degree
    - Associate degree
    - Bachelor's degree
    - Post-graduate degree
  - What is your primary occupation? _____

- Familiarity to technology
  - 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
    - Maybe
  - In a scale of 1 to 5, how often do you spend time on the Internet each day? (1: Never, 5: Several times per day)

    2 3 4 5
  - 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 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 retail apps (e.g. Starbucks, Macy's, Best Buy, etc.)
- Used health, wellness, or medical information apps (e.g., MayoClinic, MyFitnessPal, Fitbit, Strava, etc.)

APPENDIX B: Supplementary data for chapter 6

D Demographics of the participants

ID	Your gender:	Are you a student?	Has computing degree?
1	Male	Yes	No
2	Male	Yes	No
3	Female	No	No
4	Male	Yes	Yes
5	Female	Yes	Maybe
6	Male	Yes	No
7	Male	Yes	Yes
8	Male	Yes	Yes
9	Male	No	Yes
10	Female	No	Yes
11	Female	No	No
12	Male	Yes	Yes
13	Male	Yes	No
14	Male	Yes	Yes
15	Female	No	No
16	Male	Yes	Yes
17	Female	No	No
18	Male	Yes	Yes
19	Male	Yes	No
20	Male	Yes	Yes
21	Female	Yes	No
22	Female	Yes	Yes
23	Male	No	No
24	Male	No	Yes
25	Male	Yes	Yes
26	Male	Yes	Yes
27	Female	No	Yes
28	Male	No	Yes
29	Female	No	Yes
30	Female	No	Yes

Table 11: Demographics of the participants in deployment study

E Survey questionnaire

- Email address: _____

- Experience today
  - Did you look for or visit any place after you received a review from others?
    - Yes
    - No
    - Maybe
  - Did you in person see someone who posted a review that you received?
    - No
    - Once
    - Multiple times
  - Did you ever interact/communicate with other users about a post?
    - No
    - Once
    - Multiple times
  - Did you ever interact with someone who received a review you posted?
    - No
    - Once
    - Multiple times
  - What do you think about sharing your photo and username with any of your reviews?
    - I was happy to share both of them

    * Only the username is OK, I do not want to share my photo
    * Only the photo is OK, I do not want to share my username
    * I do not want to share either of them

- The things you would be concerned with an application like this collecting about you:
    * Name
    * Photo
    * Options/ Comments
    * The people you interacted with
    * Your app usage
- Do you have any other privacy concerns about this application?
    * _____
- Was this app useful at iFest?
    * 1: Not at all useful
    * 2: Somewhat useful
    * 3: Useful
    * 4: Very useful
- How useful this app would be at similar festivals or events?
    * 1: Not at all useful
    * 2: Somewhat useful
    * 3: Useful

    * 4: Very useful

- Personal Information
    - Your age: _____
    - Your Gender:
        * Female
        * Male
        * Other
        * Prefer not to say
    - Are you a student?
        * Yes
        * No
    - Do you have a college degree or work experience in computer science, software development, or similar fields?
        * Yes
        * No
        * Maybe