Proceedings of the 52nd Hawaii International Conference on System Sciences | 2019

Unpacking People's Understandings of Bluetooth Beacon Systems - A Location-Based IoT Technology

Yaxing Yao
SALT Lab
School of Information Studies
Syracuse University, Syracuse, NY
yyao08@syr.edu

Yun Huang
SALT Lab
School of Information Studies
Syracuse University, Syracuse, NY
yhuang@syr.edu

Yang Wang
SALT Lab
School of Information Studies
Syracuse University, Syracuse, NY
ywang@syr.edu

Abstract

Bluetooth beacon technology is an emerging location-based Internet of Things (IoT) technology, designed to transform proximity-based services in various domains such as retail. Beacons are part of the IoT infrastructure, but people rarely interact with them directly and yet they could still pose privacy risks to users. However, little is known about people's understandings of how beacon-based systems work. This is an important question since it can influence people's perceptions, adoption, and usage of this emerging technology. Drawing from 22 semi-structured interviews, we studied people's understandings of how beacon-based systems work and identified several factors that shaped their understandings or misunderstandings, such as how information flows among the components of beacon systems and who owns the beacons. These understandings and misunderstandings can potentially pose significant privacy risks to beacon users.

1. Introduction

The Internet of Things (IoT) refers to a network of "things or objects, which through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals" [1]. Bluetooth low energy (BLE) beacons are emerging IoT devices that utilize Bluetooth technology to provide location-based services. They have grown in popularity since Apple Inc. introduced iBeacon, an implementation of the BLE protocol [2]. Since BLE beacons offer a highly accurate, low cost and low energy localization service [3], they have been used for many purposes, such as promoting in-store sales to customers [4], enabling smart campuses and homes [5, 6], and tracking class attendance [7]. Figure 1 shows how a typical beacon-based system works. The beacon broadcasts Bluetooth signals with its beacon ID (1). The mobile app detects the Bluetooth signals and the beacon ID, and sends the ID to a cloud server (2). The server will return location-based information based on the ID (3) [8].

In this paper, we focus on BLE beacons because they are the most popular type of beacons in the market. Going forward, we use the term "beacon" to denote the BLE beacon (i.e., the hardware beacon device) and the term "beacon-based system" to denote the whole system depicted in Figure 1, including the beacon device, the cloud server, and the beacon-based smartphone app.

We choose to study beacons and beacon-based systems for two main reasons. First, beacons are part of the IoT infrastructure but people rarely interact with them directly. Instead, people may directly interact with beacon-based apps on their smartphones. In other words, beacons are largely invisible to users. However, beacon-based systems could still pose privacy risks to their users because these systems have the ability to track people's location through Bluetooth [9, 10]. The beacon technology differs from other location-tracking technologies in that it needs a beacon-based app and uses Bluetooth. The inclusion of a beacon-based app makes beacon-based systems more complex because they include both hardware devices (beacons) and user-facing software (beacon-based apps). In addition, most people do not associate location tracking with

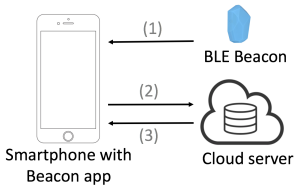

Figure 1. A typical beacon-based system [8]. (1) The beacon broadcasts Bluetooth signals with its beacon ID. (2) The mobile app detects the Bluetooth signals and the beacon ID, and sends the ID to a cloud server. (3) The server will return location-based information based on the beacon ID.

URI: https://hdl.handle.net/10125/59604
ISBN: 978-0-9981331-2-6

Bluetooth. Instead, people associate location tracking with other technologies, such as GPS and Wi-Fi [11]. This means beacon technology allows covert location tracking that people might not be aware of. Second, little is known about people's understandings of how beacon-based systems work. This is an important question because people's understanding can affect their perceptions and use of beacons, making them subject to potential privacy risks.

This paper makes two main contributions. First, our study results shed light on people's understandings or misunderstandings of how beacon-based systems work. These understandings contributed to people's concerns about beacon-based systems. Our results further explored how these understandings might pose privacy risks to ordinary users. Second, we present a number of design implications for making beacon-based systems more privacy-friendly, including user education that targets individuals' misunderstandings of beacons.

2. Related Work

2.1. Beacon and Other Location-Tracking Technologies

Beacon technology is a novel location tracking technology that can enable new location-based services [12]. Bello-Ogunu et al. proposed a system that combined crowdsourcing with beacon usage in stores [8]. This system allows people to mark the sensitivity of an area (e.g., the organic food section) in which a beacon is installed. Store customers can then use the crowd ratings to decide whether to disclose their location information or not [8]. Thamm et al. conducted a survey to investigate the adoption of beacons in the retail sector in Germany [13]. Of the 99 respondents they had, 93% of them owned a smartphone and 58% were familiar with and used Bluetooth, but only 4% knew about beacons and 3% had used them before. After explaining what beacons are and their purposes, 44% of the respondents were either undecided or categorically opposed to the use of beacons [13]. The two main reasons were: (1) an unwillingness to install too many apps and/or receive too many notifications, and (2) the fear of misuse of the collected data [13].

There are many other types of location-tracking technologies. For example, Want et al. developed Active Badge, a seminal system in which people wear badges that would transmit their location to a centralized location service so that their location can be recorded [14]. Wi-Fi is designed to provide local area network access, but it can also be used to track people in indoor positioning systems [15, 16]. Using satellite, Global Positioning System (GPS) has the capability to track people anywhere at anytime [17]. Radio Frequency Identification (RFID) was designed to identify objects through tags and has also been tested for providing indoor localization [18, 19, 20]. Near Field Communication (NFC), a type of High-Frequency RFID, provides indoor localization within a very short range [21]. Visual Light Communications (VLC) use in-store light fixtures to communicate with store apps to provide customer localization [22].

The main reason why we chose to focus on beacons is two-fold. First, beacons are an emerging technology that has gained popularity in a wide range of domains. Second, beacons are part of the computing infrastructure but people rarely interact with them directly and yet beacons could still pose privacy risks to their users.

2.2. People's Understandings of How Technologies Work

Prior research has studied people's understandings of how various technologies work [23, 24, 25, 26]. For example, Wash studied people's perceptions of home computer threats and summarized eight folk models that people held [26]. He defined folk models as mental models that people use to rationale their behaviors in practice but can be incorrect [26]. Four of these models center on viruses and the other four center on hackers [26]. Thatcher and Grey's work revealed people's perceptions of how the Internet works [23]. They identified three typical understandings such as the "User To The World" model in which users' computers are connected to the rest of the world [23]. They also concluded that people's understandings of how the Internet works can be related to their experience with it [23]. Perhaps, the most relevant research to our work is Poole et al.'s study that examined users' perceptions of RFID and their understandings of how RFID works (described as folk theories) [27]. Most of their participants were not familiar with RFID, and the results suggested that people have misunderstandings and concerns about the RFID technology [27]. For example, users were concerned that RFIDs can store their information [27].

To address people's understandings of how technologies work, the method of drawing has been applied successfully. For example, Kang et al. asked their participants to draw their understandings of how the Internet works and came to a similar conclusion that people's understandings of the Internet are related to their technical background and personal experiences [24]. Those who are more technical tend to have a more complex understanding [24]. Yao et al. asked their participants to draw their understanding of

how online behavioral advertising (OBA) works [25]. They identified four folk models that differ by who tracks users' information, where the information is stored, and who selects/sends ads to the users [25].

However, little is known about *people's understandings of how beacon-based systems work*. This is our main research question. It is also an important question because people's understandings of beacons may shape their perceptions and attitudes towards this emerging technology and affect its adoption. The study results can also help inform more privacy-friendly designs of beacon technology.

3. Methodology

Inspired in part by Wash's folk model study [26, 25], we conducted semi-structured interviews to understand people's understandings of how beacon-based systems work. Our research was approved by our IRB.

3.1. Interview Protocol

We started by asking our participants' demographic information, such as age, gender, and education.

Questions about Bluetooth usage. Since beacon-based systems require Bluetooth on users' phones, we asked questions about their experiences in using Bluetooth (e.g., "have you ever used Bluetooth on your smartphone? For what purpose?"). We then asked questions about their attitudes towards apps that require access to Bluetooth (e.g.,"do you have any concerns when using Bluetooth on your smartphones?")

Questions about beacons and usage scenarios. We then focused on beacon-based systems and different beacon usage scenarios. First, we asked our participants whether they had heard of beacons. If they had, we then asked them to explain what beacons and their main functions are. Regardless of their prior knowledge of beacons, we provided a high-level definition of beacons without explaining how they work: "Beacons are small Bluetooth devices that can be used to locate people in order to give people location-based messages" [8].

Next, similar to Wash's mental model study on home security [26], we provided our participants with three hypothetical scenarios in which beacons have been used in reality [28, 3, 7, 29], and we asked our participants to situate themselves in these scenarios. After describing each scenario, we asked our participants whether they would install and use that beacon-based app and why.

Scenario 1 - Shopping Mall: Beacons are used in a mall and when you pass by a store, you can receive alerts on your phone about a discount [28, 3].

Scenario 2 - University Campus: Beacons can be used on a university campus, where you can receive messages about today's seminars or social events when you enter your school building. Beacons can also be installed in a lab or auditorium and can be used to count class attendance [7].

Scenario 3 - Home: Beacons can be used in homes as part of the smart home setting. Suppose there was an app that could automatically turn on the light in a room right before you enter the room, or switch on the TV to your favorite program when you sit on the couch [29].

In the last scenario, beacons can be used with an associated app, which can be used to control smart home devices, so that when the app captures a beacon's signals, it will automatically apply the smart home settings. These scenarios have been reported in the media or explored on the market. They differ by factors such as public/private space in which beacons are used, and the purpose of the location-based notifications (e.g., commercial, educational). They helped the participants understand different use cases of the beacon technology regardless of their prior knowledge of beacons.

Drawing how beacon-based systems work. Inspired by several prior studies [30, 24], we then asked our participants to draw a diagram on a piece of paper illustrating how they think beacon-based systems work in the shopping mall scenario. While drawing, the participants were asked to explain their thoughts, the components and lines, as well as what information they thought of as flowing/transferring among the components. This drawing session allowed our participants to visualize and explain their understandings. At the end of the drawing session, we drew the same beacon system as shown in Figure 1 on a new piece of paper and explained this model of beacons to participants. Once the participants understood how the system works and what type of data might be collected, we asked them whether this understanding had changed their mind on whether they would install/use such an app on their phones and why.

3.2. Participant Recruitment

We recruited and interviewed 22 participants in a metropolitan area in the Northeastern part of the US. We used university mailing lists, Craigslist, and local libraries' email lists to send out the recruitment materials. We also used a snowball sampling strategy, i.e., asked participants to refer our study to their contacts [31]. We deliberately selected participants to ensure the diversity of demographics and backgrounds.

The ages of our participants ranged from 19 to 59 (mean = 32). There were eleven female and eleven male participants. Our participants represented a wide range of occupations, such as students (undergraduates

and graduates), computer engineers (software and hardware), librarians, company managers, a pastor, a housewife, a retired worker and a waitress.

3.3. Data Analysis

Interview data analysis. We audio recorded all interviews upon the participants' permission. We also took notes during the interviews. All the recordings were then transcribed, and all transcripts were analyzed using a thematic analysis [32]. One co-author and two other trained student researchers read transcripts several times to familiarize themselves with the data. Then, the two students coded one interview together at the sentence level and developed a code book. The two students then coded two more interviews independently using the code book. They achieved a Krippendorff's alpha value of 0.81, suggesting very good inter-rater reliability [33]. When they found new codes that were not covered by the code book, they added the new codes. Upon finishing, they reconciled their results and formed a final code book, which consisted of more than 100 unique codes such as "sending notifications," "privacy intrusion," and "database involved." The codes were then grouped into several themes, such as security, privacy, beacon mechanisms, smartphone apps, Bluetooth, and notifications. Finally, we read the corresponding interview quotes to confirm they were grouped into the correct themes and adjusted if grouped inappropriately. For example, "agree to permissions" was first grouped into *security*, but after reviewing the actual quotes, we moved it to *beacon mechanisms*.

Drawings analysis. We adopted Poole et al.'s methodology [30] in analyzing our participants' drawings. We analyzed the drawings by coding all elements in every drawing, i.e., all the components involved, the information flow among the components, stakeholders, and other elements. This process generated 87 unique codes. We grouped all codes into five themes: devices involved, stakeholder involved, communication direction, personal data collection, and personal data storage.

4. Results

Twelve participants did not know beacon. Ten participants had heard of or used beacons. The ratio of people with beacon experiences is considerably more than Thamm et al.'s survey study about people's challenges with beacons in retail, i.e., 4% [13]. Through our introduction questions, all participants formed a reasonable understanding of beacon technology and were able to name many potential applications of beacons. Next, we will describe our main findings.

Table 1. Summary of participants' understandings of how the beacon-based system work in the shopping mall scenario. "-" refers to "no". "Info flow" refers to "information flow among different devices;" "Owner" refers to "who owns the beacons;" "Who Collect" refers to "who can collect users' data."

ID	Gender	Info Flow	Owner	Who Collect
P1	Female	2 way	Store	Store, Maker
P2	Female	2 way	Store	Dev.
P3	Female	1 way	Mall	-
P4	Male	2 way	Dev.	Dev.
P5	Female	2 way	Maker	Not mall
P6	Male	2 way	Store	Mall
P7	Female	1 way	Store	Dev., store
P8	Male	1 way	Store	Dev.
P9	Female	2 way	Store	Store
P10	Male	2 way	Mall	Store
P11	Female	2 way	Mall	Store
P12	Male	2 way	Mall	Mall manager
P13	Male	2 way	Mall	DBA
P14	Female	2 way	-	-
P15	Male	2 way	Maker	Dev.
P16	Male	2 way	Mall	Dev., DBA
P17	Male	2 way	Mall	Mall
P18	Male	2 way	Mall	Mall
P19	Female	2 way	Maker	Mall
P20	Male	2 way	Mall	Mall
P21	Female	2 way	Mall	-
P22	Female	2 way	Mall	Dev., mall

4.1. Understandings of How Beacons-Based Systems Work

We asked our participants to situate themselves in the shopping mall scenario and to draw how the beacon-based system works in this scenario on a piece of paper. Their drawings and explanations varied but tended to focus on the following factors: different components in the beacon system; information flow among the components; whether personal information is collected; where the collected information is stored; who owns the beacon system; who can collect and access the collected data; and who to trust in the beacon system. Our participants' understandings are summarized in Table 1. Below are the results.

Information flow among components. The next factor has to do with how information flow among the components of a beacon system. Our participants were divided in terms of whether the information flow between beacons and users' phones is one-way or two-way. Three participants (P3, P7 and P8) thought

the information flow was one-way. We use "information flow" to refer to sending information about devices or users to a pre-defined destination, thus excluding device broadcasting of Bluetooth signals where there is no pre-defined receiver. In particular, these participants indicated that the beacon will detect the presence of nearby users' phones and send information to the phones but not the other way around. Thus, they did not think there was information collected from users' phones, so they did not have any concerns about the beacons. For example, P3 explained:

"This [beacon] will detect the mobile phone as soon as I [am] in that area wherever this is the range of that Bluetooth [beacon] and it will detect the mobile phone and this will, I will get the information updates...it's one way." (P3)

According to P3, her phone would broadcast its Bluetooth signal only and no other information (such as the phone's location). Once she steps into the beacon range, the beacon would capture the signal from the phone, then send information to the phone. There was no information being transferred from the phone to the beacon, thus the information flow was one-way.

The rest of our participants (19 out of 22) believed that the information flow between the beacon and users' phones was two-way, meaning that the phone would send user data to the beacon, and the beacon would return relevant information (e.g., coupons, product information) to the beacon app installed on the phone. For example, P2 included herself in the drawing (Figure 2) and explained how the information flow was two-way.

"Here's me and I've got my phone and I feel like as I approach like within a certain distance probably if I have Bluetooth on, it recognizes me so I guess I would kind of do one of these, so I've got arrows kind of going back and forth." (P2)

In her understanding, once she turned on the Bluetooth on her phone, her phone was actively sending out a signal which contained her location. After that, the beacon would start sending her notifications and other information based on her location. "Going back and forth" clearly suggested the two-way nature of the information flow. This is a critical misunderstanding held by our participants since in reality (see Figure 1), beacons are merely broadcasting devices that send out Bluetooth signals without capturing any outside signal or information.

Furthermore, 18 out of 19 participants who believed the information flow was two-way also thought that beacons are able to collect information from users. These participants believed that, as their phones got connected with the beacons, the beacons would be able to collect personal information, such as location, phone ID, and other types of information, from their phones.Such collection would be done through users actively confirming the beacon connection or users actively clicking on the location-based notifications. Once the information were collected, our participants perceived that the information would be stored either inside the beacon directly or in database in the cloud.

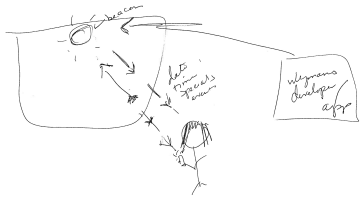

Figure 2. Two-way information flow from P2. The beacon would collect location information from her phone and return coupon information.

It is worth noting that people's perceived view of information flow and personal data collection and storage can potentially affect their concerns. Specifically, the three participants who thought the information flow was one-way did not have any concerns about beacon-based systems, as there was no perceived user data collection. The other 18 participants who thought the information flow was two-way, however, had mixed attitudes toward beacon-based systems because they thought these systems can collect user data. Such mixed attitudes were further influenced by the following factors.

Who owns beacons. Our participants held different views of who owns the beacon. For instance, P18 said,

"I would assume that the store that it was in owned it but if it was in the mall... I guess I would just assume that the mall management put it up themselves but maybe not, maybe it's owned by an outside group that's doing it and then that raises other security concerns because then who's doing that, and what are they monitoring."

He brought up several entities that might own the beacons: the store in which the beacon was installed; the shopping mall; and *an outside group*. He emphasized that if the beacon was owned by outside groups, it would raise other security and privacy concerns for him. This indicated not only his uncertainty of who actually owns the beacon, but also his lack of trust in the third party entities. He said he had no knowledge of the outside group about information collection and processing. This unawareness made him concerned.

P2 instead thought the beacon app developer owns the beacon:

"I think it would probably be whoever, so I guess I didn't think of this part, so I would have to have an app,

so probably whoever was, not the store but whoever built the app I guess." (P2)

She considered that, even though the beacon appeared in the store, the store was not necessarily the owner of it. She felt the owner should be the person/entity that developed the beacon-based app. She considered the app developer as an important stakeholder in the beacon-based system, which was insightful. However, in reality, the app developer might also not own the beacon. This indicates that the ownership of beacons could confuse users, and suggests the potential for clearly communicating this ownership to people may help them make more informed decisions about beacon usage.

Who can collect/access user data. Our participants mentioned various kinds of people that can have access to the collected user data. For instance, P12 thought system administrators, store managers, and database administrators can access the collected user data (Figure 3).

P20 suspected that mall owners, hackers and government agencies may gain access to the collected user data. He explained,

"Now I would also wonder whether people at the mall who own the mall, right, the people who own the mall that they would also potentially have access to that information and then there's always people out here who could hack a server and discover the information and then for us these days you could say could that be the government right, or could that be police department, could that be someone else." (P20)

Here, he was concerned that the aforementioned entities may be able to gain access to their data via legal or illegal means.

Three participants (P2, P3, P20) believed beacon administrators can feed beacons with data, such as coupon information. For instance, P3 thought,

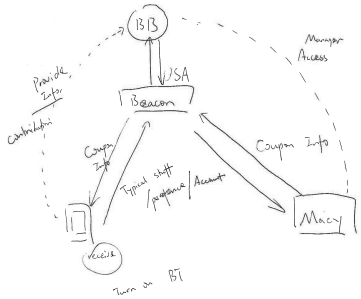

Figure 3. Drawing from P12. All customers' information is stored in the database (the circle at the top). System/database administrators and store managers can access the data.

"There would be like one administrator who is having the access to that Bluetooth [beacon] who can feed this data." (P3)

P3 emphasized the role of an administrator in the beacon ecosystem. This administrator would have access to the beacon only to *feed data* to the beacon. In addition, we found that the trust level between users and these entities could largely affect people's attitudes toward beacons. We will discuss that next.

Who to trust in a beacon-based system. A crucial question for our participants was who to trust in a beacon system. Our participants not only had various levels of trust in different scenarios, they also misplaced their trust in the wrong parties across all scenarios.

All but one participant (P22) felt more comfortable about using beacons in the campus setting than in the shopping mall setting mainly because they trusted the university as an entity. P5 attributed her trust in the university to a safe and secure university campus, and extended this trust to the beacon usage.

"Really no [concerns], because the campus is safe and secure so I don't think there is any harm for students and I think there are a lot of security people in and around the campus, so I think the campus is secure and I don't worry about anyone checking my location so I think it's pretty much safe." (P5)

In a way, the perceived physical safety of the university campus made her comfortable with the data collection by beacons installed on campus. P22, however, held a different opinion. He considered the campus as a more "private" environment, thus he felt uncomfortable with his location being known through the use of beacons.

"That's different for me because it's the school, like it's a part of me, like I'm involved in the school and I think it's a little troublesome that they know where you are because if you're doing something you're not supposed to, I'm not saying I am but they can get you in trouble maybe." (P22)

His concern came from his perception that the university is a part of him, and it was very private. He disliked that he could be subject to campus surveillance enabled by beacons. The surveillance could reveal problematic behavior and get someone into trouble.

We found that our participants, regardless of their prior experiences with beacons, intuitively considered that the beacons were owned by the places where the beacons were installed (e.g., a shopping mall, a university). Then they formed their attitudes towards beacon usage based on their trust toward the places where the beacons were installed. However, this heuristics can be problematic because in reality beacons are not necessarily owned by the places where they are

installed. Besides, given how beacons work (Figure 1), it is the developers of the beacon-based apps, rather than the places, that actively collect users' information.

For example, P9 mentioned that even though her location was tracked, she was still fine with it as she trusted the shopping mall because it is a company.

"Tracking my location around the mall is more safe because it's a company, not a private person." (P9)

However, in this case, the beacon-based app might not necessarily be developed/owned by the shopping mall. Thus, P9 *misplaced* her trust in the company, which made her believe her location being tracked was safe. Such understanding, on the one hand, helped our participants make the decision about whether to accept/use beacons or not; on the other hand, however, it can also pose significant risks to our participants because they tended to confuse about who can actually collect their data and trust the wrong parties.

4.2. Attitudinal Changes after Explanation

As we reported earlier, our participants had various concerns about beacons. However, nearly half of them showed a change in their perceptions or attitude towards beacons after we explained how beacon-based systems actually work. The changes were generally expressed in a positive way, where the participants either felt that their concerns were resolved or they became more open to using beacon-based services. For instance, P2 was concerned about her privacy, saying that she did not want others to know about her behavior at home. After our explanation, she indicated that the one-way communication nature of beacons comforted her.

"I think so, like I say somehow I thought it was kind of a two-way interaction at this point, and knowing that it's not it makes me feel better somehow." (P2)

Other participants who did not have concerns about beacon usages became even more supportive of the technology. For example, P4 became more willing to try the beacon-based app after she realized that there is a central database, which she thought as more secure.

In general, our participants became more positive toward beacons, or were more willing to try beacons and beacon-based apps. These changes of perceptions suggest the promise of educating people about beacons and improving the transparency between beacon-based app developers and end users.

4.3. Summary of Findings

Our findings highlight a few factors that affected our participants' understandings of how beacon-based systems work. Among them, **the information flow among different components** and **who owns the beacons** are two crucial factors. On one hand, participants' understandings of the information flow influenced their understandings of data collection and storage in a beacon-based system; on the other hand, the non-converged understandings of who owns the beacons highlighted the potential of misplacing users' trust to the wrong parties, which may result in significant privacy risks.

5. Discussion

5.1. Ramifications of Misunderstandings

We observed several important aspects that could either cause unnecessary privacy concerns or potentially lead to significant privacy risks. We discuss them below.

Beacons can collect and store user data? One misconception we found was that beacons can collect and store user information. Such misconception can negatively affect people's perceptions of beacons and hinder people from accepting this technology because this misunderstanding can trigger unnecessary privacy concerns (e.g., beacons can collect data but in fact they cannot).

Beacon data collection: pull-based or push-based? Prior literature on location-based services suggests two information delivery mechanisms in this context: pull-based and push-based [34]. Pull-based location-based services require users to initiate the information and service requests based on their location, while push-based location-based services proactively push information to users based on their location [34]. As we explained before, beacon-based systems are push-based.

However, the two-way information flow brought up by our participants were essentially a pull-based mechanism since they thought that they need to actively request or agree before they receive any location-based information or service. Specifically, they either believed that they need to actively connect to a beacon before any of their information is collected or they would receive a notification as confirmation when beacons tried to collect their information. Such misunderstandings pose great privacy risks to users, since many people thought they need to agree to data collection before any data can be collected, yet the reality is that their information, especially location data, can be autonomously collected without their consent.

Who tracks user data via beacon-based systems? One factor that affected some of our participants' decisions on accepting the usage of beacon-based apps even when they knew these apps can track their location

is whether they (i.e., the participants) trust the entities (e.g., a university) that track their location. This suggests that our participants had to figure out who actually tracks them via beacon-based systems.

We observed that our participants adopted heuristics that can misguide them. They often considered the place where the beacon was deployed to be the owner of the beacon. Some participants were concerned about their location being tracked since they did not trust the entity (e.g., shopping mall), while other participants indicated that they would choose to use the beacon since they trusted the entities (e.g., universities) that track their locations. Our participants generally trusted beacon use more in the campus scenario because they believed the beacons were owned by the university, which they considered as a trustworthy organization. In this case, our participants did not worry about their locations being tracked by the university.

However, this misunderstanding could put people's privacy at risk because other entities might also be able to track them. For example, the university might use a beacon-based app developed by a third party, which can also track users. In a more extreme case, since beacons are very small (can be coin-size) and have their own battery, a malicious entity can secretly place beacons on the campus (e.g., hide them in buildings) without the university's awareness. As such, this heuristics can mislead users to trust the wrong parties, and overlook risks that can actually compromise their privacy (e.g., third party beacon-based apps can collect their data).

Can Bluetooth track people's location? Many participants associated location-based notifications with GPS, considering that their location data can be collected only when they enable the GPS on their phone. This implies that our participants either ignored or did not know that Bluetooth could also be used for location tracking [9, 10]. Such belief can also put user privacy at risk because when users think they have disabled sharing of their location data by turning off the GPS on their phone, there is still the possibility that their location data can be collected through Bluetooth beacons.

5.2. Technology Adoption

People's understaindings or misunderstandings could also have an impact on whether to adopt the beacon technology. Literature has suggested that people's perceived risks of technology can affect the technology's adoption (e.g., [35, 36]). For example, Hoffman et al. suggested that users are less likely to make purchases online if they consider the online environment as risky [37]. One reason is that people have little knowledge about how their personal data is used [38]. In the case of beacons, our participants showed different types of concerns associated with their understandings of how beacon-based systems work. For example, participants who believed that the communication between a beacon and a user's smartphone is one-way tended not to have any concerns regarding beacons since they believed that no personal data was collected in the system. Thus, they had a positive attitude towards beacons.

Of those participants who considered the communication between a beacon and a user's smartphone as two-way communication, some believed that their data was collected for temporary purposes (e.g., counting customers) and not stored anywhere where very few people can get access to the data (e.g., store manager), or was stored in the beacon where only limited people could have access to the data (e.g., beacon manufacturer, store manager). These participants tended to have some privacy and security concerns, such as their information being collected for marketing purposes which may end in overwhelming notifications on their phone. Those participants still generally hold a positive attitude towards beacons.

For those participants who believed that their personal data was collected and stored in the cloud services, since they did not know where the data was stored, how the data would be used, and who had access to their data, they tended to have more privacy and security concerns, such as the cloud storage being hacked and their data being accessed by unauthorized personnel. Such understandings resulted in a very mixed attitude towards beacons, which may further hinder beacon technology adoption.

5.3. Design Implications

In the following section, we discuss how our results can inform future user education, user notice, user choice and privacy and security in the context of beacon.

User education. We believe it is crucial that people who consider using beacon-based systems should know the basic concepts and mechanisms of such system. Our rationale is two-fold. First, people's misunderstandings of beacon-based systems can trigger unnecessary concerns and/or pose privacy risks. Second, our study showed a promising sign of user education - after we explained how beacon-based systems actually work by the end of the study, the majority of our participants claimed that many of their previous concerns about beacons were resolved, and they became more positive towards and more willing to use beacon-based systems.

We advocate beacon-based systems should clearly communicate that (1) beacons are broadcasting devices,

(2) beacons are push-based, and (3) beacon apps can collect user information but beacons cannot. Beacon app developers should be transparent about whether they collect user data, and if so, what user data they collect and for what purpose to address people's concerns. We also believed that it would be helpful to tailor the user education to individual users' misunderstandings. For instance, for those who thought beacon can collect their data, user education can emphasize that beacons cannot collect user information but beacon-based apps can.

More broadly, when introducing new technologies, it is important to ensure that users form correct and positive understandings of what the technology can and can not do. Future technologies should also consider to include the user education pieces to eliminate users' unnecessary concerns at the early introduction stage.

User notice. Our study results suggest that many participants were willing to sacrifice their data to a certain degree if they can receive desired benefits from using beacon-based apps. Thus, future beacon-based apps should consider informing users the costs and benefits about beacon usage as a way to promote beacon adoption. For example, an app can inform users that the app will collect their shopping preferences in exchange for more precise location-based promotion notifications.

User choice. The current beacon system mechanism requires users either to accept location-based services and data collection altogether, or completely reject beacon usage. Future beacon-based app designs should consider providing users an *opt-out* option, so that users can keep using the location-based services, but opt out from potential data collection other than their device location if they prefer to. In addition, we suggest that the "location services" per-app configurations (currently only affect GPS localization, such as "Location Service" in iOS) should also apply to beacon-based apps, so that disabling location services should not only disable GPS but also the Bluetooth function in beacon-based apps. By doing so, users who do not wish to be location tracked can limit beacon-based location tracking.

Privacy and security. In terms of beacon design, under the current beacon mechanism, many privacy/security risks exist but could be overlooked. For instance, it is possible that entities could detect beacons in an area and create apps by leveraging those beacon signals to covertly track user locations. If users happen to install their apps, even though the users may intend to share their location with official/legitimate apps, their location may be leaked to the malicious apps without their awareness. To mitigate this risk, future beacon design could consider incorporating security mechanisms such as access control on the beacons to only allow legitimate apps to make use of the beacons (e.g., using beacon IDs). However, they will increase the complexity of the current beacon-based systems.

5.4. Limitations and Future Work

Our study has a few limitations. First, not all our participants knew beacons well, which could limit their assessment of this technology. Nearly half of our participants had heard of or used beacon-based apps before. In comparison, the German survey study had only 4% of their respondents having heard of beacons [13]. We also did not observe any notable differences between those participants who had heard about beacons and those who had not. Thus, we are reasonably confident about the validity of our findings. Future research can look into the differences more deeply through a larger sample. Second, we only provided and studied three beacon usage scenarios. Future research can consider additional and even futuristic scenarios to further investigate people's perceptions of beacons under these scenarios. Third, our results were based on participants' self-reported opinions/data. Future research can explore field deployments or experiments of beacons to examine people's actual usage of beacon-based systems.

6. Conclusion

Beacon is an emerging location tracking technology. We interviewed 22 participants to examine their understandings of how beacon-based systems work. Our participants had many misunderstandings which led them to have unnecessary concerns or overlook risks that can actually materialize. As beacons are gaining popularity, we advocate that user education could be invaluable to help clarify people's misunderstandings, mitigate their unnecessary concerns, and draw people's attention to overlooked but realistic risks.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, pp. 2787–2805, Oct. 2010.

[2] Apple, "ibeacon for developers," 2017.

[3] N. Newman, "Apple ibeacon technology briefing," *Journal of Direct, Data and Digital Marketing Practice*, vol. 15, no. 3, pp. 222–225, 2014.

[4] M. Sturari, D. Liciotti, R. Pierdicca, E. Frontoni, A. Mancini, M. Contigiani, and P. Zingaretti, "Robust and affordable retail customer profiling by vision and radio beacon sensor fusion," *Pattern Recognition Letters*, vol. 81, pp. 30–40, 2016.

[5] A. Shema and Y. Huang, "Indoor collocation: exploring the ultralocal context," in *Proceedings of the 18th International Conference on Human-Computer*

Interaction with Mobile Devices and Services Adjunct, pp. 1125–1128, ACM, 2016.

[6] Y. Huang, Q. Wu, and Y. Yao, "Bluetooth low energy (ble) beacons alone didnt work!," in *Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers*, ACM, 2018.

[7] S. Noguchi, M. Niibori, E. Zhou, and M. Kamada, "Student attendance management system with bluetooth low energy beacon and android devices," in *Network-Based Information Systems (NBiS), 2015 18th International Conference on*, pp. 710–713, IEEE, 2015.

[8] E. Bello-Ogunu and M. Shehab, "Crowdsourcing for context: Regarding privacy in beacon encounters via contextual integrity," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 3, pp. 83–95, 2016.

[9] R. Faragher and R. Harle, "Location fingerprinting with bluetooth low energy beacons," *IEEE journal on Selected Areas in Communications*, vol. 33, no. 11, pp. 2418–2428, 2015.

[10] D. Oosterlinck, D. F. Benoit, P. Baecke, and N. Van de Weghe, "Bluetooth tracking of humans in an indoor environment: An application to shopping mall visits," *Applied Geography*, vol. 78, pp. 55–65, 2017.

[11] A. H. Behzadan, Z. Aziz, C. J. Anumba, and V. R. Kamat, "Ubiquitous location tracking for context-specific information delivery on construction sites," *Automation in Construction*, vol. 17, no. 6, pp. 737–748, 2008.

[12] R. Faragher and R. Harle, "An analysis of the accuracy of bluetooth low energy for indoor positioning applications," in *Proceedings of the 27th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+'14)*, pp. 201–210, 2014.

[13] 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*, pp. 181–192, Springer, 2016.

[14] R. Want, A. Hopper, V. Falcao, and J. Gibbons, "The active badge location system," *ACM Transactions on Information Systems (TOIS)*, vol. 10, no. 1, pp. 91–102, 1992.

[15] S. Woo, S. Jeong, E. Mok, L. Xia, C. Choi, M. Pyeon, and J. Heo, "Application of wifi-based indoor positioning system for labor tracking at construction sites: A case study in guangzhou mtr," *Automation in Construction*, vol. 20, no. 1, pp. 3–13, 2011.

[16] G. V. Zàruba, M. Huber, F. Kamangar, and I. Chlamtac, "Indoor location tracking using rssi readings from a single wi-fi access point," *Wireless networks*, vol. 13, no. 2, pp. 221–235, 2007.

[17] R. Bajaj, S. L. Ranaweera, and D. P. Agrawal, "Gps: location-tracking technology," *Computer*, vol. 35, no. 4, pp. 92–94, 2002.

[18] R. Want, "An introduction to rfid technology," *IEEE pervasive computing*, vol. 5, no. 1, pp. 25–33, 2006.

[19] L. M. Ni, Y. Liu, Y. C. Lau, and A. P. Patil, "Landmarc: indoor location sensing using active rfid," *Wireless networks*, vol. 10, no. 6, pp. 701–710, 2004.

[20] S. Kim, D. Ko, and S. An, "Geographical location based rfid tracking system," in *World of Wireless, Mobile and Multimedia Networks, 2008. WoWMoM 2008. 2008 International Symposium on a*, pp. 1–3, IEEE, 2008.

[21] R. Want, "Near field communication," *IEEE Pervasive Computing*, vol. 10, no. 3, pp. 4–7, 2011.

[22] D. O'Brien, L. Zeng, H. Le-Minh, G. Faulkner, O. Bouchet, S. Randel, J. Walewski, J. A. R. Borges, K.-D. Langer, J. Grubor, *et al.*, "Visible light communications," 2009.

[23] A. Thatcher and M. Greyling, "Mental models of the internet," *International journal of industrial ergonomics*, vol. 22, no. 4, pp. 299–305, 1998.

[24] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler, ""my data just goes everywhere:" user mental models of the internet and implications for privacy and security," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pp. 39–52, 2015.

[25] Y. Yao, D. L. Re, and Y. Wang, "Folk models of online behavioral advertising," in *Proceedings of the Computer Supported Cooperative Work (CSCW)*, ACM, 2017.

[26] R. Wash, "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, (New York, NY, USA), pp. 11:1–11:16, ACM, 2010.

[27] E. S. Poole, C. A. Le Dantec, J. R. Eagan, and W. K. Edwards, "Reflecting on the invisible: understanding end-user perceptions of ubiquitous computing," in *Proceedings of the 10th international conference on Ubiquitous computing*, pp. 192–201, ACM, 2008.

[28] S. Korber, "How retailers are using your phone to tell you: Buy," May 2015.

[29] S. Mittal, "Iot and home automation: How beacons are changing the game," *Beaconstac*, 2015.

[30] E. S. Poole, M. Chetty, R. E. Grinter, and W. K. Edwards, "More than meets the eye: transforming the user experience of home network management," in *Proceedings of the 7th ACM conference on Designing interactive systems*, pp. 455–464, ACM, 2008.

[31] L. A. Goodman, "Snowball sampling," *The annals of mathematical statistics*, pp. 148–170, 1961.

[32] R. E. Boyatzis, *Transforming qualitative information: Thematic analysis and code development*. sage, 1998.

[33] K. Kripendorff, "Reliability in content analysis: Some common misconceptions," *Human Communications Research*, vol. 30, pp. 411–433, 2004.

[34] H. Xu, H.-H. Teo, B. C. Tan, and R. Agarwal, "The role of push-pull technology in privacy calculus: the case of location-based services," *Journal of Management Information Systems*, vol. 26, no. 3, pp. 135–174, 2009.

[35] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS quarterly*, pp. 425–478, 2003.

[36] Y. Wang, H. Xia, Y. Yao, and Y. Huang, "Flying eyes and hidden controllers: A qualitative study of people's privacy perceptions of civilian drones in the us," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 3, pp. 172–190, 2016.

[37] D. L. Hoffman, T. P. Novak, and M. Peralta, "Building consumer trust online," *Communications of the ACM*, vol. 42, no. 4, pp. 80–85, 1999.

[38] C. D. Raab, "The distribution of privacy risks: Who needs protection?," *The information society*, vol. 14, no. 4, pp. 263–274, 1998.