“Beacons Collect Information from Users”: Unpacking People’s Misunderstandings of Bluetooth Beacon Technology

Yaxing Yao
SALT Lab
School of Information Studies
Syracuse University
Syracuse, NY 13244, USA
yyao08@syr.edu

Yun Huang
SALT Lab
School of Information Studies
Syracuse University
Syracuse, NY 13244, USA
yhuang@syr.edu

Yang Wang
SALT Lab
School of Information Studies
Syracuse University
Syracuse, NY 13244, USA
ywang@syr.edu

Abstract
Bluetooth beacon technology is an emerging Internet of Things (IoT) technology, designed to transform proximity-based services in various domains, such as retail and education. While this technology is gaining popularity, little is known regarding people’s understandings or misunderstandings about how beacon-based systems work. This is an important question because people’s understandings of beacons influence their perceptions and attitudes and can affect the acceptance and adoption of this emerging technology. Drawing from a preliminary study of 15 semistructured interviews, we uncovered a number of misunderstandings that our participants had about how beacon-based systems work, such as that beacons can directly collect information from users. Our findings help explain people’s concerns about beacons and provide suggestions for the future design of beacons.

Author Keywords
Beacon, Internet of Things, Misunderstandings, Privacy

Introduction
Bluetooth low energy (BLE) beacons are devices that utilize Bluetooth technology to provide location tracking services. Since beacons offer a highly accurate, low cost and low energy localization service [8], they have grown in popularity since Apple Inc. introduced iBeacon, an

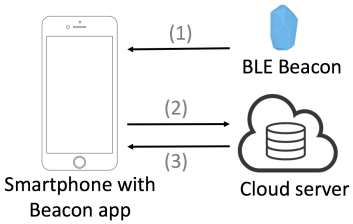

Figure 1: A typical model of a beacon-based system involves three steps: 1) The beacon broadcasts Bluetooth signals with its beacon ID; 2) The mobile app detects the Bluetooth signals, identifies the beacon ID, and sends the beacon ID to a cloud server via the Internet; 3) The server searches and returns location information based on the beacon ID. Mobile apps may collect user's personal data (e.g., users' preferences), and send them along with the beacon ID to the server at Step 2. The figure is inspired by [1].

implementation of the BLE protocol [5]. For example, they have been used for many purposes, such as promoting in-store sales to customers [12], managing building energy consumption [2], organizing crowds at events [3], enabling smart campuses and homes [11, 7], facilitating campus surveillance [10], and tracking class attendance [9].

One important characteristic of beacons is that although they are part of the IoT (Internet of Things) infrastructure, people rarely interact with them directly; instead people directly interact with beacon-based apps on their smartphones. Figure 1 illustrates how a typical beacon-based system works. A BLE beacon actively broadcasts Bluetooth radio signals with its beacon ID, which can be recognized by nearby Bluetooth-enabled smartphones. The signals, received by a smartphone, can be read by beacon-based apps installed on the phone, so that these apps can identify the location of the phone using the beacon ID and can then provide information (e.g., about nearby events) to the smartphone user based on the phone's location.

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 about beacons and can affect the adoption of this emerging technology. For example, there were concerns about people being tracked without their consent when an advertisement company installed beacons in New York City [13].

In this paper, we aim to investigate not only people's attitudes towards beacons, but also their understandings of how beacon-based systems work. More specifically, we interviewed 15 ordinary citizens with diverse backgrounds. We found that our participants misunderstand how beacon-based systems work along several dimensions, such as how information flows among different devices in a beacon-based system and whether personal data is collected. These misunderstandings can pose great privacy and security risks to people.

Method

We designed and conducted a semistructured interview study to understand people's understandings of how beacon-based systems work. Our research was approved by the university IRB.

Interview Protocol

We began the interviews by asking our participants for demographic information, such as their age, gender, education, their Bluetooth usage experience, and their prior knowledge of beacons. 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 whether they had heard of beacons before the study, we then 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" [1].

We then provided our participants with three scenarios in which beacons were used in real situations (i.e., a shopping mall, a smart campus, a smart home) [8, 9, 7], and all have been reported in the media or explored on the market. They differed in whether beacons were used in a public or private space, and the purpose of the location-based notifications (e.g., commercial, educational). Inspired by Wash's study where scenario-based questions were used to understand people's perceptions of how a technology works [14], 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. These scenarios helped the

Beacons send and collect information

"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, 34-year-old male)

Beacons collect personal data

"The beacon collects all the information about which notification you clicked. And then the next time it will refine it and send me those kind of [promotion]." (P5, 23-year-old female)

participants understand different uses of the beacon technology regardless of their prior knowledge of beacons.

Recruitment

We recruited and interviewed 15 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, that is, we asked participants to refer our study to their contacts [4]. We deliberately selected participants to ensure diversity of the pool in terms of demographic characteristics and background.

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 college student, computer engineer (software and hardware), librarian, pastor, housewife, and retired worker. Four participants had heard of beacons or had used beacon-based apps.

Data Analysis

We audio recorded all interviews with 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. One coauthor 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 interrater reliability [6]. 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.

Findings: Misunderstandings

Our findings suggested that our participants held a number of misunderstandings regarding how beacon-based systems work. These misunderstandings include: beacons send and collect information, beacons collect personal data, beacons store user information, and app developers own the beacons. We present the details below.

Beacons send and collect information

Twelve participants held the misunderstanding that the information flow (i.e., communication) between the beacon and users' phones was two-way. They thought that the beacon would collect information that the phone sends out, and return relevant information (e.g., coupons, product information) to the beacon app installed on the phone. For example, in P2's understanding, once she turned on the Bluetooth on her phone, her phone would actively send out a signal which contained her location. After that, the beacon would start sending her notifications and other information based on her location.

Beacons collect personal data

Twelve participants held the misunderstanding that beacons are able to collect information from users. These participants believed that, as their phones were connected with the beacons, the beacons would be able to collect information, such as location, phone ID, and other types of information, from their phones. For example, P5 thought that his shopping preferences could be collected by the beacons too. He thought that when he clicked on the

Beacons store user information

"From my data, I would say yes because every company wants data, customer data, how many people cross and if they have access to my location it's going to be very useful for them at the mall then if you do cross Walmart then of the people that enter Walmart how many people actually bought something from them. So yes, they do store data." (P1, 44-year-old female)

"It's preprogrammed, so like the first time the smartphone comes in contact with the beacon, I think it's like this is the first message to the smartphone, the first time it's in the database or maybe the beacon. The database is inside the beacon...it should be secure." (P15, 24-year-old female)

product or coupon information sent by the beacon, that action signified that he was interested in that type of product, that his product preference would be collected by the beacon and used for sending more targeted notifications in the future. In reality, a beacon-based app collect his data but the beacon cannot.

It is worth noting that people's conception of information flow and personal data collection can potentially affect their concerns. Participants who thought the information flow is two-way have mixed attitudes toward beacon-based systems because they thought these systems collect user data.

Beacons store user information

For participants who thought that the beacons can collect information from users, the next natural question was whether the collected data will be stored and if so where the data is stored. Nine participants held the misunderstanding that their personal information can be collected and stored, although they differed in where they thought the information would be stored. Such understandings are important since they affected participants' perceived concerns about beacons, such as the security of the stored data and who can access it.

Six participants believed that the collected information would be stored inside the beacon. P1, for example, believed that every company wants customer data, and that they collect and store personal data such as phone or user location in the beacon. She believed that through analyzing the customer data, companies would be able to learn more about their customers as well as the market. Thus, she thought the customer data would be stored for this purpose.

P15 held a similar understanding that personal data would be stored in the beacon. However, he explicitly mentioned that there was a database inside the beacon. He believed that after the connection is established, the beacon would send information to his phone, and his phone would return its location to the beacon. This location information would be stored in the database inside the beacon, but he emphasized that the data was secure because he believed only authorized administrators can access the database.

Two participants (P2, P3) also believed that beacons store data, and that beacon administrators can feed beacons with data, such as promotion and coupon information. P3 emphasized the role of an administrator in the beacon ecosystem and said that this administrator would have access to the beacon only to feed data to the beacon.

In general, when participants held this conception that data is stored in the beacons, they were concerned about where the beacon was installed and whether that place was trustworthy and their data was secure. P15 was an exception as he felt the database in the beacon is secure.

App developers own the beacons

Our participants differed in their perception of who owns the beacons. One misunderstanding is that the beacon-based app developer owns the beacon. For example, P2 considered that, even though the beacon appeared in a 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 not own the beacon. This indicates that the ownership of beacons could confuse users, and suggests that clearly communicating the beacon's ownership to people may help them make more informed decisions about beacon usage.

App developers own the beacons

"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, 34-year-old male)

"There would be like one administrator who is having the access to that Bluetooth [beacon] who can feed this data." (P3, 27-year-old female)

Discussion and Future Work

Our findings reveal several misunderstandings regarding beacon devices and beacon-based systems. These misunderstandings pose potential privacy concerns and data security risks to users and can negatively impact the adoption of this new IoT technology. Below, we discuss the implications of our findings and future research that needs further investigation.

Specifically, many participants misunderstood that in beacon-based systems, users need to initiate the information and services requests. They believed that they need to actively connect to a beacon before any of their information is collected. Some participants believed that they would receive a confirmation notification when beacons tried to collect their information. Such misunderstandings suggest great privacy risks to users, since many people felt 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.

Another misconception our participants held is that beacons can store user information. In our study, six participants believed that beacons themselves had the ability to store information. Such misconceptions also negatively affect people's perceptions of beacons since they question whether beacons are secure enough to store their data.

It's worth noting that people's misunderstandings tend to make them fixate on beacon devices themselves, rather than the beacon-based apps. As a result, their threat model focuses on beacons and not the beacon apps. However, in reality, the beacon apps rather than the beacons themselves can collect user information.

We outline a number of design implications for future beacons and beacon-based apps. In terms of beacon design, future beacon manufacturers could consider incorporating security mechanisms such as access control to only allow legitimate apps to make use of the beacons so that users' locations will not be leaked to other malicious apps without their awareness. In terms of beacon-based app design, first, it is important to educate the users regarding the basic concepts and mechanisms of the beacon-based system (e.g., beacons are broadcasting devices, and beacons do not collect users information but the app does, etc.). Second, future beacon-based apps should provide the user with explicit options to opt out from potential data collection.

Our results shed light on future research opportunities on this topic. Specifically, we found that our participants, regardless of their prior experience with beacons, intuitively consider that the beacons were owned by the places where the beacons were installed (e.g., a shopping mall, a university). Their attitudes toward beacon usage was therefore based on their trust in the places where the beacons were installed. However, in fact, beacons are not necessarily owned by the places where they are installed. We will further explore people's trust toward beacon-based systems to understand how trust plays a role in people's privacy and security concerns.

Acknowledgements

This material is based upon work supported in part by the National Science Foundation under Grant No. #1464312 and #1464347. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. This research was also in part supported by a Google Faculty Research Award.

REFERENCES

1. Emmanuel Bello-Ogunu and Mohamed Shehab. 2016. Crowdsourcing for context: Regarding privacy in beacon encounters via contextual integrity. *Proceedings on Privacy Enhancing Technologies* 2016, 3 (2016), 83–95.
2. Andrea Corna, L Fontana, AA Nacci, and Donatella Sciuto. 2015. Occupancy detection via iBeacon on Android devices for smart building management. In *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition*. EDA Consortium, 629–632.
3. Emanuele Frontoni, Adriano Mancini, Roberto Pierdicca, Mirco Sturari, and Primo Zingaretti. 2016. Analysing human movements at mass events: A novel mobile-based management system based on active beacons and AVM. In *Control and Automation (MED), 2016 24th Mediterranean Conference on*. IEEE, 605–610.
4. Leo A Goodman. 1961. Snowball sampling. *The annals of mathematical statistics* (1961), 148–170.
5. Apple Inc. 2017. iBeacon for Developers. (2017). `https://developer.apple.com/ibeacon/`
6. K Kripendorff. 2004. Reliability in content analysis: Some common misconceptions. *Human Communications Research* 30 (2004), 411–433.
7. Shubhi Mittal. 2015. IoT and Home Automation: How Beacons are Changing the Game. *Beaconstac* (2015).
8. Nic Newman. 2014. Apple iBeacon technology briefing. *Journal of Direct, Data and Digital Marketing Practice* 15, 3 (2014), 222–225.
9. Shota Noguchi, Michitoshi Niibori, Erjing Zhou, and Masaru Kamada. 2015. Student attendance management system with bluetooth low energy beacon and android devices. In *Network-Based Information Systems (NBiS), 2015 18th International Conference on*. IEEE, 710–713.
10. Gaurav Saraswat and Varun Garg. 2016. Beacon controlled campus surveillance. In *Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on*. IEEE, 2582–2586.
11. Alain Shema and Yun Huang. 2016. Indoor collocation: exploring the ultralocal context. In *Proceedings of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct*. ACM, 1125–1128.
12. Mirco Sturari, Daniele Liciotti, Roberto Pierdicca, Emanuele Frontoni, Adriano Mancini, Marco Contigiani, and Primo Zingaretti. 2016. Robust and affordable retail customer profiling by vision and radio beacon sensor fusion. *Pattern Recognition Letters* 81 (2016), 30–40.
13. Keith Wagstaff. 2014. New York City Nixes Advertising 'Beacons' in Telephone Booths. *NBC News* (2014).
14. Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. ACM, New York, NY, USA, 11:1–11:16. `DOI: http://dx.doi.org/10.1145/1837110.1837125`