Exploring Perceptions of a Localized Content-Sharing System Using Users-as-Beacons

Nazmus Sakib Miazi, Heather Lipford, Mohamed Shehab

Exploring Perceptions of a Localized Content-Sharing System Using Users-as-Beacons

Nazmus Sakib Miazi[1], Heather Lipford[2], and Mohamed Shehab[2]

[1] Northeastern University, Boston, MA, USA
m.miazi@northeastern.edu
[2] The University of North Carolina at Charlotte, Charlotte, NC, USA
{richter,mshehab}@uncc.edu

Abstract. We envision a unique social interaction system, 'users-as-beacons' built upon Bluetooth Low Energy (BLE) beacon technology, that could provide potential privacy benefits. It leverages BLE to employ the user devices to act as mobile beacons. Its potential applications include community-based social networking, localized advertising, and instant reviewing. To evaluate the potential for this system and inform design, we conducted an exploratory interview study of 27 participants of a hypothetical localized content-creating system. Using a design prototype and multiple scenarios as prompts, we asked questions regarding users' perceptions of the potential benefits and challenges of a users-as-beacons system, focusing in particular on their privacy concerns and needs. Our results indicate that users do perceive the benefit of increased trustworthiness of user-beacons, but do not have expectations of greater location or behavioral tracking privacy. We highlight multiple design challenges of this system in supporting the trustworthy, relevant, and timely sharing of posts between people in a community.

Keywords: Bluetooth Low Energy · Beacons · Users-as-beacons · Internet of Things · Trust · Location privacy · Peer-interaction

1 Introduction

Bluetooth Low Energy (BLE) Beacon technology is primarily used for indoor location estimation and providing contextual information with low energy consumption and low-cost mobile beacons. BLE is widely adopted by a vast range of industries. For example, in 2016, 93% of U.S. baseball stadiums had been equipped with beacons to facilitate visitors finding seating locations, restrooms, and other facilities[1]. With over 90% of smartphones being BLE enabled[2], there are a variety of systems that potentially can be built on top of this technology. In fact, during the current Covid-19 pandemic, one of the privacy-preserving methods of contact tracing for limiting the spread of SARS-COV-2 infection is through BLE [3, 4], utilizing its ability to detect proximity to other beacons without requiring GPS location. In this paper, we are exploring a potential use of beacons for a social system we refer to as 'users-as-beacons'. This system

will leverage current BLE enabled smartphones by turning them into beacons themselves, which we refer to as a user-beacon. Combined with cloud integration, such a system can become a social web of information. This would enable a unique method of peer-to-peer interactions among users, with potential privacy and trust benefits.

In this platform, whenever user-beacons are within BLE range (100 meters in the open, less indoors), they exchange their unique id's, allowing them to download each other's content from the cloud. We believe a users-as-beacons system can be deployed for a variety of social applications, including:

– *Community-based social network:* Users-as-beacons can be used for a localized social network, such as on a college campus, for circulating news and events throughout the community, or as a method of social posting within localized events and festivals.
– *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.
– *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 crowd-sourcing from, and spreading to, users in a locality.

While a users-as-beacons system can offer functionality similar to existing social platforms or review sites, we believe it 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 users' locations do not need 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 [5]. 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, this potential for face-to-face interaction may raise privacy concerns and requirements for protecting one's identity.

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 no guarantee the beacon is connected to a real person. Moreover, the system could be more physically invasive since, depending on the implementation of the system, users could potentially be physically approached by others in proximity to them. Therefore, this kind of system

will only be worth deploying if the benefits are valued by users when weighed against the potential privacy risks, all of which can be understood through use of the application. To investigate the potential of users-as-beacons applications and inform the design of such a platform, we conducted a formative study of user perceptions of envisioned applications of the system.

This paper explores the following research questions: (i) what privacy and trust benefits do users perceive of social users-as-beacons applications; (ii) what are users' expectations in how they would use such a system; and (iii) what are their privacy concerns or barriers to using such a system? We report the results of two versions of an exploratory interview study involving 27 participants from diverse backgrounds. The interviews were structured around a users-as-beacons design prototype[6] as well as several specific scenarios of the use of the system. Participants were asked about their perceptions in sharing and receiving content from people around them, their envisioned context and motivations of use, and their privacy concerns and expectations.

To summarize, the contributions of this paper are: (i) identifying the potential social applications of users-as-beacons involving mobile user-to-user communication; (ii) user perceptions of the potential benefits and use of a users-as-beacons review application; (iii) an understanding of the privacy concerns and expectations of being a user-beacon; and (iv) the design challenges and initial guidelines for implementing a privacy-preserving users-as-beacons prototype.

2 Application example

One type of application we envision is a crowd-sourced, localized social platform, such as for sharing information at a festival. Figure 1 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. Thus, the receiver can then see Kim's post. Re-

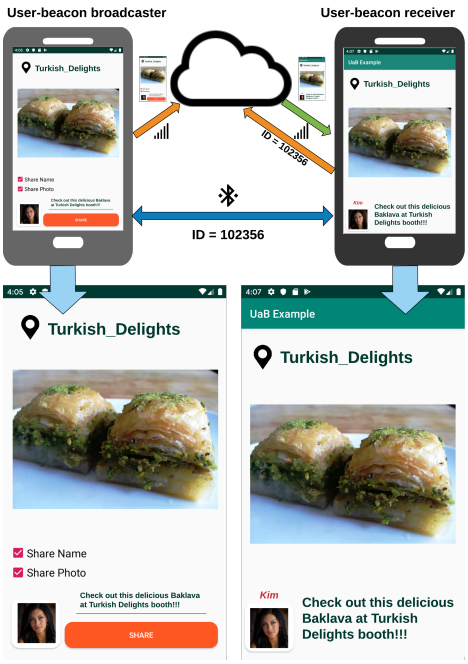


Fig. 1: Example of a 'users-as-beacons' app for creating crowd-sourced and localized posts in a festival.

ceivers 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.

3 Background

3.1 User Generated Content and Review Systems

In users-as-beacons applications, users become content creators, and share their content to their surroundings. Thus, research on user-generated content creation can inform the design of our proposed system. Hansen et al. [7] and Lawrence et al. [8] investigated the effectiveness of consumer-generated content and found that based on its realism, authenticity, and trustworthiness, user-generated content is much more effective than company-created content for advertising. Moreover, user-generated content can engage more people, and create a community of content creators[9–12]. Therefore, amalgamating with BLE to create a localized community of user-generated content creators has strong potential for building trustworthy social interaction.

One key type of user-generated contents that has been investigated are user reviews. Many platforms invest in incentives for reviewers, and sometimes even fake user reviews to appear competitive [13, 14]. Much research has been done on how to identify and mitigate fake reviews in various review platforms, such as Yelp and Amazon. For any kind of review system, the reputation of the users and the reliability of their reviews are very important. [15–17].

One viable application 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. 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.

3.2 Data and Social Privacy in Mobile Systems

Users-as-beacons leverages users' capability of socializing with other users in a mobile environment. Unlike other social networking platforms, where it is imperative to manage one's personal information, in 'users-as-beacons' it is more important to maintain desired peer-interactions. There is a clear tension between reduced privacy risks by not allowing location-tracking, and increased reliability of contents, with potential loss of inter-personal privacy. Hence, it is essential to explore users' perceived comfort around others, as well as concerns regarding data dissemination, behavioral tracking, and privacy more generally.

In current social platforms, users are increasingly getting concerned about their data privacy, even while they are sharing significant amounts of information

with other users [18–20]. As a result, we have seen the increased utilization of privacy settings and cautions about social interaction on popular platforms [21, 22]. Behavioral tracking and targeted advertising on social sites are also important privacy concerns of many consumers [23–26]. As we explore social applications of user-beacons, we expect that similar privacy concerns will also be important factors in the design and adoption of such a system.

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. Users would still be sharing their proximity to surrounding user-beacons. Early studies found that location-based mobile services are often perceived as privacy intrusive, and users want granular control over location settings [27–29]. 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 [30–32]. In contrast to sharing locations with friends, users remain concerned about sharing their locations with advertisers and third parties [33, 34]. 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 [30]. We expect similar location concerns in users-as-beacons, which our study investigates.

Several frameworks have been developed to manage the security and privacy of BLE-based systems. Bello-Ogunu et al developed a beacon privacy manager framework based on user-derived policies and their analysis showed that crowd-sourced privacy managers are effective for managing the privacy of BLE based systems [35]. 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 *Anonycast* [36] to deliver precise location information to pedestrian's smartphones leveraging the crowd-tracking systems while keeping the users anonymous. Schulz et al. developed a security concept to prevent the possibility of requesting tracking and forgery in indoor location tracking beacons [37]. Gao et al. developed a privacy-preserving framework called TrPF [38] to preserve user privacy when the devices are deployed in a participatory sensing environment.

3.3 Proximity-based Peer to Peer (P2P) Applications

Users-as-beacons is an example of a proximity-based peer to peer application, which have been previously investigated with other technologies. For example, Xing et al. developed a P2P proximity-based content sharing application using Wi-Fi [39]. Jung et al. developed a content sharing application to cooperatively download content from Bluetooth access points [40]. Shen et al. developed MobiUS, a collaborative video downloader application to watch high resolution videos over adjacent mobile devices [41]. And, Beach et al. developed WhozThat, a platform to share context-aware personal identification information to lower the barrier to social discourse [42].

However, none of these previous examples involve trusted reviews and social exchanges, particularly in a BLE-based interaction scenario. The only similar application scenario was introduced very recently with Covid-19 contact tracing. Several countries and organizations have created contact tracing systems to limit the spread of the SARS-COV-2 virus on top of BLE, as a decentralized, privacy-preserving proximity tracing system [3, 4, 43]. The privacy benefits of using BLE for contact tracing have made it reliable and effective. In this paper, we describe a more social use of this technology, which poses very different trade-offs between utility and privacy.

3.4 Users' Perceptions of BLE Beacons

Our idea of users-as-beacons is a system built on top of BLE beacons. Therefore, we now describe how people have already embraced this technology, as well as the privacy concerns and other challenges that have been raised. BLE beacon technology is especially useful for indoor settings, by enabling a plethora of location-based services [44, 45]. 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. [46] 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. Yao et al. identified several factors, including information flow and users knowledge about beacons system, that lead to people's conceptions of the technology and its privacy risks [45]. They suggested that user education is essential to reduce the likelihood of users overlooking real privacy problems, as well as mitigating unnecessary concerns. Bello-Ogunu et al. proposed a crowdsourced beacon rating system to allow users to define fine-grained policies for using particular beacons [47]. Although users-as-beacons is meant to be built upon BLE, the idea of having live user-beacons changes the privacy implications, with less potential for behavior and location tracking, yet increased potential for peer interaction and interpersonal privacy invasions. We seek to understand these perceptions in this paper.

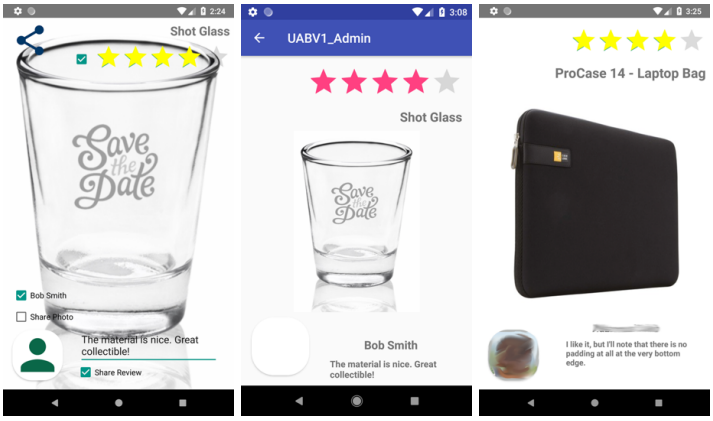
4 Exploring user perceptions

We conducted a user study with 27 participants to explore people's thoughts about a users-as-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 example application domain to conduct the study, because this allows us to explore many different contexts of users' daily lives. We conducted an interview study, using a design prototype to enable participants to have a more concrete understanding of sharing and receiving posts or reviews (Figure

2). We also described several different scenarios that participants might face in using the system as a prompt for additional interview questions. These scenarios and the summary of the interview questions are described below.

Initially, the design prototype 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 users-as-beacons system in other contexts such as restaurant review, social interaction, or event promotion. Thus, we redesigned the design prototype and study scenarios to explore the possibility of deploying the system in more social contexts. We then interviewed 14 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 prototype briefly to the participants. Both of the user study designs were approved by our university IRB.

4.1 User study 1: users-as-beacons in a shopping area



(a) The participant is creating a post

(b) Interviewer received the post

(c) The participant received a post from the interviewer

Fig. 2: Screen-shots of the design prototype built for conducting study 1.

– *Scenario one, signing up and creating posts:* We started the study by asking the participants to register themselves using our design prototype. Then we discussed a shopping mall scenario, asking the participant to select an example product and write and share a review. When the participant shared the post, the interviewer received it (Figure 2b). Then the interviewer showed the participant the receiver's view and asked about their general perceptions of using such a system, and their opinion of sharing their personal information in the reviews.
– *Scenario two, receiving posts:* The participant then received a review from the interviewer (Figure 2c), and was asked about their perceptions of receiving posts from those around them, their intentions about interacting with others, and their perceived motivations for making posts.

– *Scenario three, different places:* The interviewer described a daily life scenario where the user's device is beaconing throughout the day, in various contexts. The interviewer then asked about beaconing in different places and incentives that may impact usage decisions.
– *Scenario four, control over the system:* To understand the participant's reaction toward interacting with other users, 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 and other kinds of desired controls in the system.
– *Scenario five, content types:* Here, the interviewer asked the participant to create a review of sensitive content (underwear), and then asked about the perceived comfort of sharing reviews of different kinds of content, along with the impact of potential incentives.
– *Scenario six, peer influence:* The interviewer described receiving a review of desired content from someone nearby and then questioned participants' expectations for interaction with people around them.
– *Final questions:* Finally, the interviewer asked questions about privacy concerns and potential applications of the system and then ended with a survey of demographics, education, and everyday Internet activities.

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

In the second study, we developed a slightly different design-prototype to investigate users' thoughts on making posts about places, small businesses, restaurants, social causes, and local events. Like study 1, we discussed the system's functionalities and demonstrated how the participant would receive and send reviews, and described several scenarios as part of the interview.

– *Scenario one, registering and receiving posts:* The interview started with the participant receiving two posts from the interviewer, a food review and a service recommendation. Then the interviewer asked the participant several questions related to receiving posts from people around them.
– *Scenario two, creating posts:* The participant used the design-prototype to create two posts, one for a small business and another to promote a social cause. Participants were then asked about their perceptions of reviewing different places, services, or social causes. They also answered questions regarding the different contexts in which they could envision using the system.
– *Scenario three, instant reviews:* The interviewer then described a restaurant scenario where the participant was having dinner and wanted to leave a review. The interviewer asked the participant several questions related to posting reviews and review timing.
– *Scenario four, reviewing small businesses:* The next scenario was about the participant hiring a pest control service. They were then asked about their opinion on reviewing small businesses, their motivation, and the factors they would consider in posting such reviews.

– *Scenario five, contextual controls and preferences:* Like the fourth scenario in the first interview, we described two social situations, then asked questions about interaction with others and participants' perceived needs for controls and preferences over potential interaction.
– *Final questions:* Like study 1, we asked general questions on overall perceptions, privacy, and suggested features and then ended with a survey of demographics, education, and everyday Internet activities.

4.3 Participant Recruitment and Demographics

We recruited 27 participants in total around our university campus, through our institutional research service, and recruiting posts through social media in neighborhood groups. We also utilized Snowball sampling, where initial participants suggested additional participants. After the interview session, each participant was compensated with a $10 gift card. Among the 27 participants, 11 of them were males, and 16 of them were females. Five of them were from the age range 18-24, 19 of them were from range 25-34, and 3 others were of the age 35 and above. The participants were from variety of occupations, including 13 students, physicians, administrators, health educators, and career advisers.

4.4 Analysis

This is an exploratory, formative study to understand the potential behaviors and concerns of users within a UaB system. Thus, we conducted inductive coding for each interview separately, and involved an additional coder for the 2nd interview who had not seen the first codebook. 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 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 discussed and resolved any disagreements. Disagreements were tracked, and inter-rater agreement 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, nine 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 enumerate the participants 1 to 13 for the first set of interviews and 21 to 34 for the second set of interviews.

4.5 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.

5 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 versions 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 with 'a few' describing 2-6 participants, 'some' as 7-13 participants, 'majority' as 14-16 participants, and 'most' as more than 17 participants.

5.1 Receiving posts: benefits and trust

The most immediate reaction of participants to the notion of receiving posts from surrounding people was that it is not likely to be fake and instead would come from real people around them. For example, P30 said, *"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: *"I may receive posts 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 the posts, they also expressed desire for users to not be anonymous so they could know where an opinion came from.

Participants also talked about the types of posts they would be most interested in. In study 1, most participants thought that the product reviews were useful to receive, but only in shopping areas, depending on time and context. They agreed that the most useful posts to receive would be of restaurants and local places. 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.

However, many did not like the idea of promoting social causes. And, they wanted to receive service recommendations only when they needed them. All but three participants said that the relevance and context of the received posts are essential. Thus, most participants talked about customization features to filter the types of posts they are most interested in. A majority of the participants thought that receiving many instant notifications from others could be irritating. P2 said, *"Sometimes I see that people are saturated by posts. 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 [posts] 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."*

Some said that notifications can be very distracting to regular activities, even when they might actually be receiving relevant posts. Thus, the overall message was that the system would need to have different kinds of controls and preferences to filter and block notifications, and to customize or subscribe to different kinds of posts of interest.

5.2 Making posts: interests and concerns

Participants were open to making posts if they liked the product or place and they trust the people around them. P21 said, *"Actually when I am sending my [post], I would think that it might help people around me."* 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 posts, participants stated that they would mostly make posts about restaurants and interesting places. They generally wanted to support small businesses as well, but only a few wanted to use it for social causes or services recommendations.

In many of the participants' opinions, making instant posts was a matter of discomfort. In study 2, when asked about writing a food 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 requires time. *"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?"* P28. Participants also mentioned not writing a post immediately because of potential social interaction that might result. As P31 said, *"I would probably not want [to let people know] instantly. 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, *"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 may feel strange at first to advertise certain products or places, that perception could change if that

became more visible and normal. We asked participants about what incentives would motivate them to use such a users-as-beacons system. Most participants thought that cash back or redeemable points would be a good motivation. Even those with high concerns over negative peer-interaction would think twice if they get incentives. As P31 said, *"I am doing this study because I am getting a gift card, so any incentives are certainly gonna peak interest to an extent."*

In the second study, many participants thought that community feedback such as an upvote, downvote, or comments from the people around who read their posts would increase the appeal to make more posts. P31 commented, *"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 donut can be a good motivation: *"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."* -P27

We wanted to know how the participants felt about sharing their personal information with other users nearby. All felt that it was acceptable to share their first name with the posts. However, most of the participants were cautious about sharing their full name, as that would identify them, and instead would prefer an alias. All but two were hesitant to share their photo. As P2 said, *"It's when you can match a name and a face, I could see potential privacy problems. So, [sharing] photo is a concern."*

Moreover, 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, *"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."*

5.3 Interacting with others: comfort and concerns

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

In study 1, we described an option to delay sharing a post in the shopping area 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. Two of them were even delighted to interact with people. The participants thought 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, *"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..."*

In both versions of the study, we asked the participants about their opinions on beaconing 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 and expressed concerns about sharing too much private information with their colleagues. Only five participants were willing to keep beaconing at home; most felt that 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. 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 digitally posting something.

There was a common feeling against facing the establishment related to making posts about businesses, and that those in authority could interfere when a user is writing opinions. 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; if I fear that the manager might misbehave, they could be angry or something."* Interestingly, in the second study, the participants were also thinking about confronting the restaurant management when they made a food review post. 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."*

5.4 Perceived 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. Participants were particularly concerned because, beyond just their posts, they were not sure what kind of information the app would need to prompt them to write such posts. Thus, behavioral tracking was a big concern (n=11). P1 said, *"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. 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 social 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 accurately 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 improvement in 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 posts. P3 said, *"I would prefer a system that uses a location-based model that can automatically sort this thing out for me. I would like to receive the things related to where I am now. 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 and expressed their fear of being tracked by predators and stalkers. P10 said, *"If I am somewhere, using a beacon, someone can find me. 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 the posts, 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, *"Being spammed will be a concern, it might be overwhelming to receive so many, 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 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.

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. 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 posts, or block posts from other user-beacons. Thus, these issues overlap with needs and challenges of audience management in social media systems more generally.

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 express their opinions 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 in the previous sections, if such a system were to become widespread and normal behavior, then their privacy concerns would be lessened.

6 Discussion and Implications

In this paper, we introduced a potential social system that can be built on top of BLE beacon technology leveraging the ubiquity of BLE enabled smartphones. We envision this system as a privacy-preserving localized information dissemination system. The primary benefits include 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. Moreover, this system will facilitate a localized information sharing system, which will enable potential peer-interactions. We explore user reactions to multiple types of posts, including social posts, product, places, and event reviews.

6.1 Feasibility and applicability of the system

While 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.

Trust: 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 the contents generated by organizations and companies[7, 8]. 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 posts in the system. Thus, users did perceive increased trust, and valued this benefit. This provides motivation that our proposed system is worth further development.

Location privacy: 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 related mobile applications, users did not perceive or value the privacy-preserving nature of users-as-beacons. In this case, the only benefit to the users would be the ability to function if GPS was disabled.

Localization and potential of peer-interaction: We also talked about possible peer-interaction as this system is localized and has the potential to create a local social interaction system. It is highly possible for the users to directly meet people who post nearby and talk about those posts. The participants showed mixed reaction to this possibility. They have not experienced this type of interaction before. On the one hand, it is new and thus, participants were not entirely sure how they would feel about it. Some of them did not perceive it as a benefit, and were thus were worried about their identities being public. On the other hand, other participants appreciated the chance of interactions, as that might make the system reliable, and enjoyed the possibility of a new form of social interaction.

We believe the primary application domain for this kind of system would be a localized extension to current social interaction systems, with increased reliability. Based on our study, this system has potential in localized socialization, reviewing places, event advertising, and supporting businesses and events in particular locations. And, despite some concerns over the potential social interaction with strangers, participants felt that this type of system would be useful mostly in locally constrained areas, such as festivals and events, or restaurants and shopping areas, where posts would also be most relevant and people could trust their peers. Some participants also saw potential benefits in the interaction between community members that such a system could provide.

6.2 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.

Managing 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. Moreover, a user-beacon needs to be there to make posts, but it doesn't mean that it would always be a real person. It still can be faked, for example by a shop, even if it is comparatively harder than in current online systems. While this did not come up a lot in the interviews, users would need to understand this possibility in a real deployment. 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 prototypes, we demonstrated how a post was delivered instantly to another user (the interviewer). Yet, we always envisioned that notifications would need to be delivered intelligently to reduce overload. On the one hand, users benefit from knowing about 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-poster interaction enabled by the system. Many also discussed how they wanted the posts 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, thus trading-off privacy for benefits. Therefore, a key challenge in this system will be to ensure the relevant and timely delivery of the content users receive with an acceptable level of trade-off between benefits and privacy, and investigating which methods can achieve these goals. This relevance may be achievable by restricting the system to very time- or location-constrained contexts, such as particular events.

Managing peer-interaction: Some participants were not at all comfortable with interacting with others as a result of making posts, 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 post 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.

6.3 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 privacy: 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 become habituated to it. 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 privacy-behavior change over time? What concerns will arise as users repeatedly encounter the same people, in the same or different places? What positive and negative experiences will shape user behaviors, and lead to greater or reduced usage?

Within the Covid-19 contact tracing context, Reichert et al.[48], Bell et al.[49], and Tang et al.[50] discuss tools and techniques to prevent privacy threats from the perspectives of patients, potential patients, hospitals, and health professionals. Similar solutions would be needed for future social U-a-B applications, which may be functionally similar yet have different privacy trade-offs.

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 online review platforms rather than more social 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 prototype, 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 testbed for understanding the feasibility and use of users-as-beacons as a localized social interaction platform.

7 Conclusion

We believe that the widespread Bluetooth Low Energy technology provides an infrastructure on which to explore novel systems that may provide both interesting applications and privacy benefits to users. Our exploratory study shows that users do perceive some benefits in a users-as-beacons social system, namely trust and the potential for peer-interaction, yet did not value the increased location privacy and were more concerned about receiving content relevant to them. Our results also demonstrate that there are still many issues surrounding privacy and peer-to-peer interaction that need additional understanding and careful design in order to develop a successful system. We plan to use our results to design and deploy prototypes to examine these issues more deeply, providing insights into the incentives and privacy trade-offs in this novel mobile communication system.

References

1. Greg 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, August 2016. Accessed: 2019-1-22.
2. Smart industry — bluetooth technology website. https://www.bluetooth.com/markets/smart-industry, January 2018. Accessed: 2019-1-15.
3. Decentralized privacy-preserving proximity tracing. https://github.com/DP-3T/documents. Accessed on: 2020-06-02.
4. Jason Bay, Joel Kek, Alvin Tan, Chai Sheng Hau, Lai Yongquan, Janice Tan, and Tang Anh Quy. BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders. *Government Technology Agency-Singapore, Tech. Rep*, 2020.
5. Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. A conundrum of permissions: Installing applications on an android smartphone. In Jim Blyth, Sven Dietrich, and L. Jean Camp, editors, *Financial Cryptography and Data Security*, pages 68–79, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.
6. Elizabeth B.-N. Sanders and Pieter Jan Stappers. Probes, toolkits and prototypes: three approaches to making in codesigning. *CoDesign*, 10(1):5–14, 2014.
7. Sara Steffes Hansen, Jin Kyun Lee, and Shu-Yueh 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.
8. Benjamin Lawrence, Susan Fournier, and Frédéric 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, October 2013.
9. Chris Forman, Anindya Ghose, and Batia 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 September 2008.
10. Hung-Pin Shih, Kee-Hung 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.
11. Alashoor Tawfiq and Baskerville Richard. The privacy paradox: The role of cognitive absorption in the social networking activity. In *ICIS 2015 Proceedings*. aisel.aisnet.org, 2015.
12. Vladimir Zwass. Co-Creation: Toward a taxonomy and an integrated research perspective. *International Journal of Electronic Commerce*, 8 December 2014.
13. Shankhadeep Banerjee, Samadrita Bhattacharyya, and Indranil Bose. Whose online reviews to trust? understanding reviewer trustworthiness and its impact on business. *Decis. Support Syst.*, 96:17–26, April 2017.
14. Michael Luca and Georgios Zervas. Fake it till you make it: Reputation, competition, and yelp review fraud. *Manage. Sci.*, 62(12):3412–3427, December 2016.
15. Amir Fayazi, Kyumin Lee, James Caverlee, and Anna 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.
16. Charla Mathwick and Jill Mosteller. Online reviewer engagement: A typology based on reviewer motivations. *J. Serv. Res.*, 20(2):204–218, May 2017.

17. Dongsong Zhang, Lina Zhou, Juan Luo Kehoe, and Isil Yakut 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, April 2016.
18. Andrew Besmer, Jason Watson, and Heather Richter 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.
19. Hanna Krasnova, Elena Kolesnikova, and Oliver Günther. " it won't happen to me!": Self-disclosure in online social networks. page 343, 01 2009.
20. Yang Wang, Gregory Norcie, Saranga Komanduri, Alessandro Acquisti, Pedro Giovanni Leon, and Lorrie Faith 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.
21. Maritza Johnson, Serge Egelman, and Steven 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.
22. Jessica Staddon, David Huffaker, Larkin Brown, and Aaron 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.
23. Rick Edmonds. People don't want to trade privacy for targeted ads. https://www.poynter.org/news/people-dont-want-trade-privacy-targeted-ads, January 2016. Accessed: 2017-07-11.
24. Tun-Min (Catherine) Jai, Leslie Davis Burns, and Nancy 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.
25. Joseph Turow, Michael Hennessy, and Nora A Draper. The tradeoff fallacy: How marketers are misrepresenting american consumers and opening them up to exploitation. 2015.
26. Heng Xu, Xin (Robert) Luo, John M. Carroll, and Mary Beth Rosson. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, 51(1):42 – 52, 2011.
27. Sunny Consolvo, Ian E Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline 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.
28. Giovanni Iachello, Ian Smith, Sunny Consolvo, Gregory D Abowd, Jeff Hughes, James Howard, Fred Potter, James Scott, Timothy Sohn, Jeffrey Hightower, and Anthony 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.
29. Norman Sadeh, Jason Hong, Lorrie Cranor, Ian Fette, Patrick Kelley, Madhu Prabaker, and Jinghai Rao. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal Ubiquitous Comput.*, 13(6):401–412, August 2009.

30. Michael Benisch, Patrick Gage Kelley, Norman Sadeh, and Lorrie Faith Cranor. Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs. *Personal Ubiquitous Comput.*, 15(7):679–694, October 2011.
31. Sameer Patil, Greg Norcie, Apu Kapadia, and Adam 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.
32. Eran Toch, Justin Cranshaw, Paul Hankes Drielsma, Janice Y. Tsai, Patrick Gage Kelley, James Springfield, Lorrie Cranor, Jason Hong, and Norman 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.
33. Drew Fisher, Leah Dorner, and David 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.
34. Patrick Gage Kelley, Robin Brewer, Yael Mayer, Lorrie Faith Cranor, and Norman Sadeh. An investigation into facebook friend grouping. In *Human-Computer Interaction – INTERACT 2011*, pages 216–233. Springer Berlin Heidelberg, 2011.
35. E. Bello-Ogunu, M. Shehab, and N. S. Miazi. Privacy is the best policy: A framework for ble beacon privacy management. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, volume 1, pages 823–832, 2019.
36. Takamasa Higuchi, Paul Martin, Supriyo Chakraborty, and Mani 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.
37. 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.
38. 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.
39. Bo Xing, Karim Seada, and Nalini Venkatasubramanian. Proximiter: Enabling mobile proximity-based content sharing on portable devices. In *2009 IEEE International Conference on Pervasive Computing and Communications*, pages 1–3, 2009.
40. Sewook Jung, Uichin Lee, Alexander Chang, Dae-Ki Cho, and Mario Gerla. BlueTorrent: Cooperative content sharing for bluetooth users. *Pervasive Mob. Comput.*, 3(6):609–634, December 2007.
41. Jacky Shen, Yanlin Li, Chunyi Peng, and Yongguang Zhang. Mobius: A together-viewing mobile video experience, June 2007. Mobisys'07 Best Demo Award.
42. A Beach, M Gartrell, S Akkala, J Elston, J Kelley, K Nishimoto, B Ray, S Razgulin, K Sundaresan, B Surendar, M Terada, and R Han. WhozThat? evolving an ecosystem for context-aware mobile social networks. *IEEE Netw.*, 22(4):50–55, July 2008.
43. Tracetogether. https://www.tracetogether.gov.sg/. Accessed: 2020-3-15.
44. Ramsey Faragher. An analysis of the accuracy of bluetooth low energy for indoor positioning applications. 2014.

45. Yaxing Yao, Yun Huang, and Yang 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.
46. Anja Thamm, Jürgen Anke, Sebastian Haugk, and Dubravko Radic. Towards the Omni-Channel: Beacon-Based services in retail. In *International Conference on Business Information Systems*, volume 255, pages 181–192, July 2016.
47. Emmanuel Bello-Ogunu and Mohamed Shehab. Crowdsourcing for context: Regarding privacy in beacon encounters via contextual integrity. *Proceedings on Privacy Enhancing Technologies*, 2016(3):83–95, July 2016.
48. Leonie Reichert, Samuel Brack, and Björn Scheuermann. Privacy-preserving contact tracing of covid-19 patients. *IACR Cryptol. ePrint Arch.*, 2020:375, 2020.
49. James Bell, David Butler, Chris Hicks, and Jon Crowcroft. TraceSecure: Towards privacy preserving contact tracing. April 2020.
50. Qiang Tang. Privacy-Preserving contact tracing: current solutions and open questions. April 2020.