International Journal of Geo-Information

MDPI

Article

Towards Understanding Location Privacy Awareness on Geo-Social Networks

Fatma Alrayes † and Alia I. Abdelmoty *,†

School of Computer Science & Informatics, Cardiff University, Wales CF10 3AT, UK; alrayesFS@cardiff.ac.uk

* Correspondence: a.i.abdelmoty@cs.cf.ac.uk; Tel.: +44-2920-874751

† These authors contributed equally to this work.

Academic Editors: Arpad Barsi and Wolfgang Kainz

Received: 23 December 2016; Accepted: 31 March 2017; Published: 5 April 2017

Abstract: Users' awareness of the extent of information implicit in their geo-profiles on social networks is limited. This questions the validity of their consent to the collection, storage and use of their data. Tools for location privacy awareness are needed that provide users with accessible means for understanding the implicit content in their location information as well as a view of the level of risk to their privacy as a consequence of disclosing this information. Towards this goal, an abstract model of location privacy threat levels is first derived from a user study involving 186 users. This is then used to inform the design of a prototype privacy feedback tool for a location-based social network. Another user study involving 338 users of this network is carried out to test the effectiveness of the proposed design. Findings confirm the strong need of users for more transparent access to and control over their location profiles and guide the proposal of recommendations to the design of more privacy-sensitive geo-social networks.

Keywords: location privacy; privacy awareness; geo-social networks; usable privacy

1. Introduction

'Social privacy' concerns how an individual manages self-disclosures, availability, and access to information about themselves by other people when using social-driven applications [1]. Those concerns are more profound on Geo-Social Networks (GeoSNs)- online social networks with location-sharing facilities—as spatiotemporal user tracks; derived from disclosed location traces, can be used to create detailed user profiles that describe people's interactions in space and time [2]. To manage social privacy on GeoSNs, one needs to understand the level of threat implied by his location information disclosure and be able to relate it to the scope of visibility granted for this information.

In this paper, we focus on user content awareness and in particular location content awareness in relation to privacy on GeoSNs. The map of locations in a user's profile can be used as a key to defining and relating other types of data elements, for example, their interests and activities can be related to the places they visit. Along with temporal semantics, the profile can provide a rich resource of personal and possibly sensitive information. The paper examines the dimensions of location data sharing on GeoSNs and how user awareness is situated in this information space. Levels of threat to privacy are proposed as means of assigning value to the information in this space. To enable location content awareness, design of feedback tools is considered that captures user's attention to both the content they are sharing and to the associated risks.

Few previous studies addressed location awareness and privacy concerns [3–5], and these were mainly questioning users' attitude with respect to sharing their current location information. These studies neglected revealing privacy implications in terms of what personal information can be extracted based on location disclosure and used limited location-sharing applications for their evaluations. This paper contributes a more detailed study that considers awareness with respect to extended user profiles

on the space, time and social dimensions and provides an understanding of how users' perception of their location content influences their privacy concerns and behaviour on GeoSNs.

User studies, in the form of online surveys, are carried out. An initial study is conducted to assess user's attitude to disclosing different aspects of location-related information against different scopes of visibility. Results are used to model the level of threat associated with the disclosure of personal location information. The validity of the model is then tested in another study that examines users' attitude and behaviour in response to explicit awareness of location information content and privacy-related risks.

The rest of the paper is structured as follows. An overview of related work on user profiling on GeoSNs and methods for privacy awareness are given in Section 2. User awareness of the data dimensions on GeoSNS is discussed in Section 3. Results of a first user study are presented in Section 4 and used to derive a model of privacy threat levels. In Section 5, a second user study is carried out to test the proposed model and findings are presented in Section 6. Discussion of the results and some conclusions are given in Section 7.

2. Related Work

One way of viewing GeoSNs is as socially-enhanced Location-Based Services (LBS). The social dimension is the primary attracting factor, with users communicating by announcing their whereabouts and activities to friends. Some GeoSNs incorporate a gamification strategy where users are rewarded for checking into locations with badges and in-game points. This game-play encourages users to revisit the application and contribute checkins, photos and tips. The social dimension is used as a base through which other services can be offered to users, such as discounts and offers in nearby or favourite places. In comparison to LBS, semantic and social information are collected along with the user location track and used to build rich user profiles [6,7]. Such profiles can be used for potentially undesirable purposes that can compromise users' privacy [8]. Here we first start by giving a brief overview of location privacy-preserving mechanisms, discuss methods for location-based inferences from mobility data sets to examine the sort of potential information that can be represented in user profile on GeoSNs, and then examine the design of feedback methods to enable privacy awareness on these networks.

2.1. Location Privacy-Preserving Mechanisms (LPPMs)

A direct method for privacy protection is the setting of privacy controls explicitly whilst using location-sharing applications. Benisch et al. [9] discusses the rich spatiotemporal location-privacy preferences of users and the lack of such dynamic and adaptable privacy control mechanisms in location-sharing applications.

A well-known LPPM relies on the concept of anonymity which is simply isolating the user identity from their personal information. In the case of location information, methods include the mix zones model [10] (employing pseudonyms, instead of traceable user identities, that change dynamically when users enters geographic zones that are not pre-registered to particular applications), k-anonymity [11,12] (spatial and temporal cloaking technique whereby users disclose an adequate level of anonymous location information that can be mapped to k number of users within a region) and fake locations [13] (injecting a fake location into user's location data to reduce the possibility of re-identification). Obfuscation is another method which refers to "the means of deliberately degrading the quality of information about an individual's location in order to protect that individual's location privacy" [12,14,15]. Both anonymity and obfuscation methods have proved to be sufficiently effective for protecting location privacy in the case of sporadic location disclosure [15,16]. However, their effectiveness is relative since none of these mechanisms were fully robust in protecting location privacy against attacks [15]. Anonymity is also not very effective in resisting location attacks when an adversary has access to the location history of a user [13,17]. Whereas much work have considered location

privacy in LBS, the applicability of the proposed methods still need to be considered in GeoSNs where the social dimension add another level of complexity to the spatiotemporal user data [6].

Generally speaking, applying LPPMs in location-sharing applications can impact the quality of service (QoS) for users, limit their experience with the application and consequently limit its usefulness [14,15]. Balancing the QoS with the need for location protection is a challenge that is subject to ongoing research work [18,19].

2.2. Location-Based Inference in GeoSNs

Significant interest can be witnessed in research studying the value and utility of location information on GeoSNs to understand users' behaviour. Some studies looked into accurate identification of user's location from their GPS trails [20,21], as well as using the location of the user's friends on Twitter [22]. Using the user's profile of visited places and socio-historical ties, Gao et al. demonstrated an accurate prediction of next check-in information [23]. Other works investigated the potential inference of social relationships between users of GeoSNs. For instance, co-occurrence between users extracted from geo-tagged Flickr pictures was sufficient for deducing their social ties with high probability [24]. In addition, users' interactions on the network coupled with their location information were used to predict friendship links [22,25].

In the past few years, many research works examined the problem of extracting spatiotemporal movement and activity patterns of users on GeoSNs. Dearman et al. [26] used reviews on Yelp to identify a collection of potential activities in the place reviewed by users. Mobility patterns on Foursquare were the subject of study in [27], who considered popular places and detected transition patterns between place categories, as well as in [28,29], where the distance between consecutive check-ins for users and the returning probability to venues were computed. More recently, studies showed that check-in information can be used to reveal sensitive personal information, including gender, educational background, age and sexual orientation [30,31]. The above sample of studies demonstrates the variety and amount of information that can be derived from user location information on GeoSNs using specialised analysis and mining techniques. Some of this information can also be obvious and inferred directly by visual inference and human intelligence of an attacker, given access to historical spatiotemporal tracks of a user.

2.3. Privacy Feedback and Notifications

Feedback and notifications tools are commonly used for warning users about security and privacy risks on the web. Studies are emerging to assess user awareness of privacy implications and the impact of such tools on the user attitude while interacting with systems [32,33]. Visualization of privacy warnings was found to be effective in increasing user awareness of privacy threats, as demonstrated in while users were more able to access their information and to manage it effectively, if provided with a view of how their profile appeared to other people [34].

The extent of users' awareness and its impact on their attitude and privacy concerns was the subject of many studies. Rader [35] observed the links between limited awareness of possible privacy violations and the usefulness of policy-based privacy solutions, while other studies noted that increased awareness encourages users to utilise stricter accessibility options [36,37]. Similarly, Sadeh et al. [5] found that methods that raise users' awareness about the way their data is used tend to stimulate users to produce more accurate preferences and increase the users' trust in the application. Tsai et al. [4] developed a mobile location-sharing application to investigate how informing users of who can access their location might influence their privacy concerns and attitude. Their findings show that informed users were more comfortable with sharing their location and had less privacy concerns.

The timing of feedback in location-sharing applications was studied in [38], who reported on the influence of real-time feedback on user's attitude—users felt more accountable and were more willing to reject unnecessary location requests. Recently, Patil et al. [3] observed that immediate feedback about location disclosures without an ability to control the disclosures, evoked feelings of over-sharing

and hence recommended the use of proactive techniques for adjusting recommendations to disclosure settings, especially in the case of socially-distant users and when visiting atypical locations.

Usability of privacy notices and feedback tools is also of relevance to this work. The complexity of privacy polices and settings and the need for more accessible tools motivated much research in this area [39,40]. Of interest are studies into users' perception of privacy risk, where visual cues were shown to be useful [41–43], particularly when shown in-context [44].

The above studies generally assume that users's awareness of privacy implications can be studied based on the recognition of the visits users make to places while using the application and the visibility settings they applied. A holistic view of possible inferences that can be made by an attacker, as described in Section 2.2 above, need also be considered to fully appreciate the implications of tracking personal location information.

3. User Content Awareness on Geo-Social Networks

In this section, we examine the question of whether a user is aware of the information they are sharing on GeoSNs. To answer this question, we begin by considering the dimensions of location data, its properties and relationships that can be used to build a user profile (geo-profile) on these networks, and use this information space to analyse user awareness based on their information needs whilst interacting with the GeoSN. On GeoSNs, users intentionally declare their presence in a particular place at a particular time. In some applications, for example, Google and Foursquare, users are able to grant permission for continuous background collection of their spatiotemporal tracks (by "switching on location" on devices). In this section, we examine the dimensions of the data being collected in such systems and the types of information that can be inferred to construct geo-profiles for users. Three primary dimensions to user information on GeoSNs can be identified; 1. the spatial dimension; 2. the social dimension; and 3. the temporal dimension. The places which the user visits are modelled on the spatial dimension. The social dimension refers to the interaction of the user on the social network; with other users or by sharing content: tips, images, etc. The temporal dimension is essentially the time line recording the time stamps of the user's visits to locations. Frequency of visits to geographic places can be used as an indicator of the degree of association with the place, or with the related activities and concepts. A mapping of the time line can be made to cluster specific temporal intervals and study emerging patterns of user activity, e.g., daily patterns (mornings, afternoon, evenings and night), weekends and weekdays, seasons, etc. Within the multi-dimensional composite spatial-social-temporal dimensions-, it is possible to mine a user geo-profile to discover relationships across multiple dimensions. Some examples are as follows.

- When did the user visit a place? How often? How much time did he spend there?
- Where would the user be on (weekday mornings)?
- Which concept/activity does the user normally undertake at a particular time point?
- Which other users/friends is this user normally collocated with on (weekends)?
- Where does the user practice a certain activity with (friends) on (weekday evenings)?
- What is the relationship nature between this user and a particular friend (e.g., housemate)?
- What is the user association with a particular place (e.g., workplace)?
- When is the user normally absent from a particular place during the week?

User's Awareness of a Geo-Profile

Unlike other information stored on a personal profile, for example, an email address or a phone number, user location information on a GeoSN is dynamically updated as the user makes use of the application services. These location tracks are not always visible to the user. When interacting with software system, user's attention is normally task-oriented [45], i.e., she needs only recall information that is relevant to the task at hand. On GeoSNs, a user either consciously shares a particular location or the service automatically captures her location and use it to tag her resources (photos, tags, etc.). In the first case, the user is consciously aware of one single point on the place-time plane, indicating

her presence in the place at a particular point in time and may be aware of the visibility scope she has previously set on her profile, and thus can recall who is she sharing this location with. In the second case, she is not aware of the location capturing activity.

Figure 1 shows a state transition network for a typical task of checking into a place on Foursquare. In state 1 the user specifies her location, then annotates the place by adding tips, images, and links to friends in state 2, and is provided with a feedback screen in state 3 that summarises her interaction. Information required for the task is limited to knowledge of current place location and details of friends co-located in the place. Feedback information is limited to an overview of frequency of visit to the current place, possibly in comparison to the statistics of other friends. This is the case with most other tasks provided by this application. Thus, unless the user intentionally seeks to view their location history, their perception is normally focussed on a small window of their personal location information. The study carried out later in this paper seeks to verify this observation by gauging the extent of information the users recall from their location interaction history in a typical GeoSN.

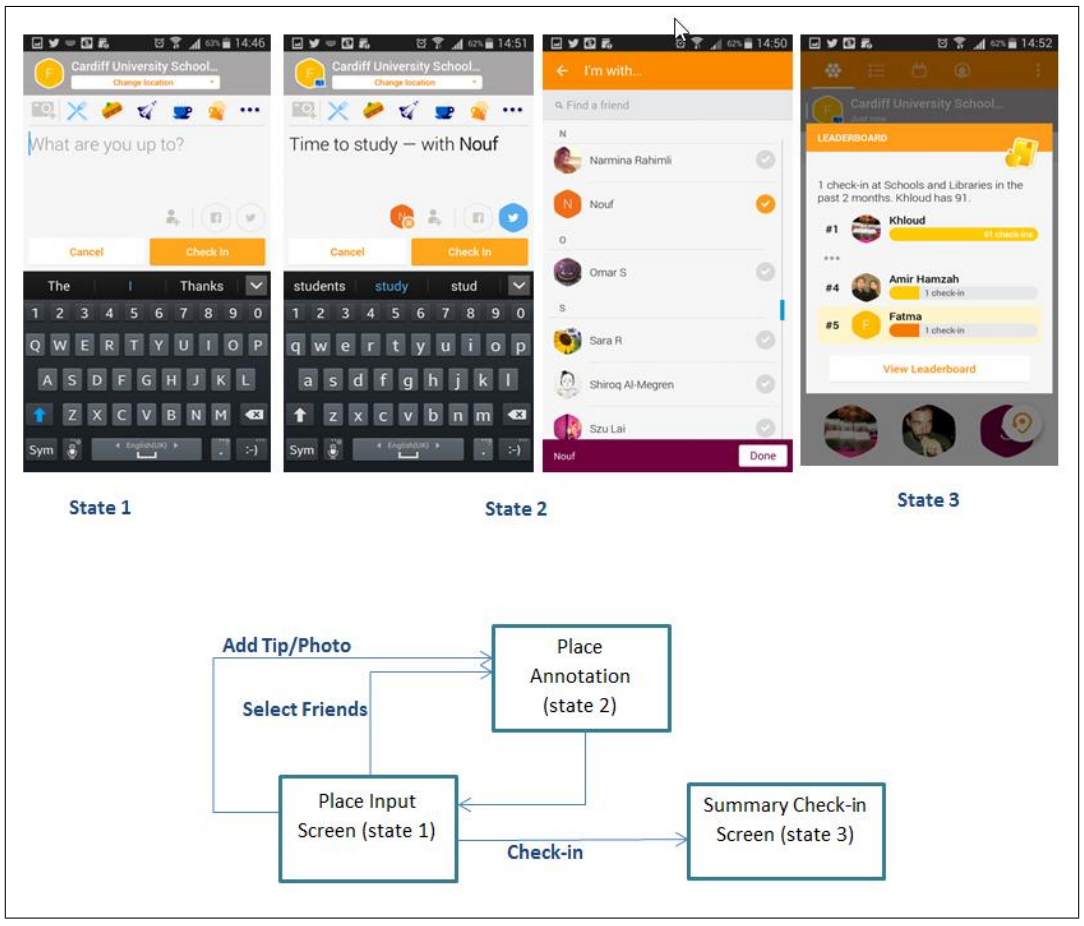

Figure 1. Task analysis for a typical process of checking into a place on Foursquare.

4. Location Privacy Threat Levels

Here a user study is carried out with the aim of understanding a model of the levels of privacy threats as perceived by users of GeoSNs.

4.1. Study Design

A survey is designed to examine the privacy concerns and behaviour of users of online social networks, in particular users' concerns towards their location information. The aim of the study is to

gauge users' perceptions to privacy threats as a consequence of recording their location information of GeoSNs. Three main aspects are addressed in this study; (1) the extent of users' awareness of the terms of use they sign up to when using these applications; (2) their understanding and attitude to potential privacy implications; and (3) how they may wish to control access to their personal information on these applications.

The targeted participants of this study are any users of online social networks who use location features, including adding location to their posts and pictures or checking into places. The questionnaire was developed using Google Forms. It comprises 4 sections (including an initial background section), is presented as a whole and takes roughly about 10 min to complete. Before disseminating the questionnaire, a pilot study was carried out with four volunteers to verify the clarity and coherence of the questions and a token incentive was offered for people who complete the questionnaire. Minor amendments were made as a result of the pilot to the wording and phrasing for the questions. The survey was then disseminated widely within the university to staff and students and was also advertised on social networks through the author's account. A token incentive of 10 Amazon voucher was offered to ten randomly chosen participants who completed the survey.

4.2. Results

The questionnaire data were analysed using the R statistical package and the results are presented below. 186 participants completed the survey of which 60% are young adults in the age group 15–24, divided almost equally between males and females. The vast majority of participants (77%) use location services frequently (several times a day) and 72% of participants use the services in GeoSNs. About 60% use location features on only one application. Adding locations to posts and pictures on Facebook was the most used application, corresponding to 47% of the total number of location services used. This is followed by adding location to tweets on Twitter, photo mapping pictures on Instagram, and checking in on Foursquare representing 17%, 16% and 10% respectively as illustrated in Figure 2. In addition, most of the users noted that they 'sometimes' use geosocial applications with almost a fifth of users 'always' using the location services. Foursquare users are more frequent users of the service than other services and 25% of the users have linked their accounts on different social networking applications.

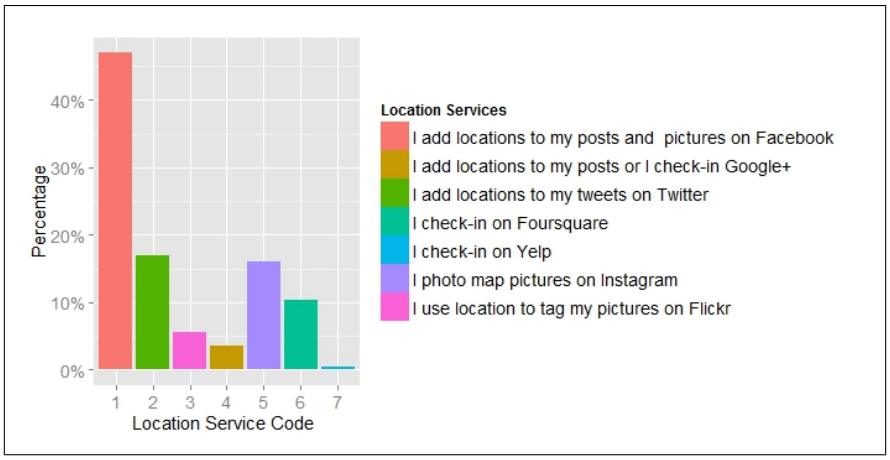

Figure 2. The distribution of location services use amongst the 72% of participants who use GeoSNs.

4.2.1. Knowledge of Terms of Use and Privacy Policies for Social Networking Services

A general question was used to begin with to understand the extent of users' knowledge of privacy policies. The majority of the users (81%) indicated that they haven't read terms of use or privacy policies of the social networking applications they use. Users were then presented with typical statements representing the terms of use relating to location information as follows and were asked to

indicate whether they are aware of the information in the statements. The following statements are representative of the terms of use of all the GeoSNs in question. Results are shown in Figure 3.

1. *Term 1: The application collects and stores your precise location (as a place name and/or a GPS point), even if you mark your location as private, for a possibly indefinite amount of time.*
2. *Term 2: The application can use your location information in any way possible including sharing it with other applications or partners for various purposes (commercial or non-commercial).*
3. *Term 3: If you share your location information, your friends and any other users are able to access and use it in any way possible.*
4. *Term 4: The application can collect other personal information, such as your personal profile information and browsing history from other web applications.*

More than half (59.5%) of users acknowledged awareness of all of the statements and of those 23% have read the terms and policies. Most users (75%) are aware of statement 3, relating to the sharing of information with friends, but are generally unaware of statements 1 and 4, relating to how their location and other information may be collected and stored by the applications. It is interesting to note that frequent users of such application are generally unaware of such statements (49%). Younger users aged between 15 and 34 tend to be more knowledgeable of these polices (60%), but gender does not seem to be a factor in these results.

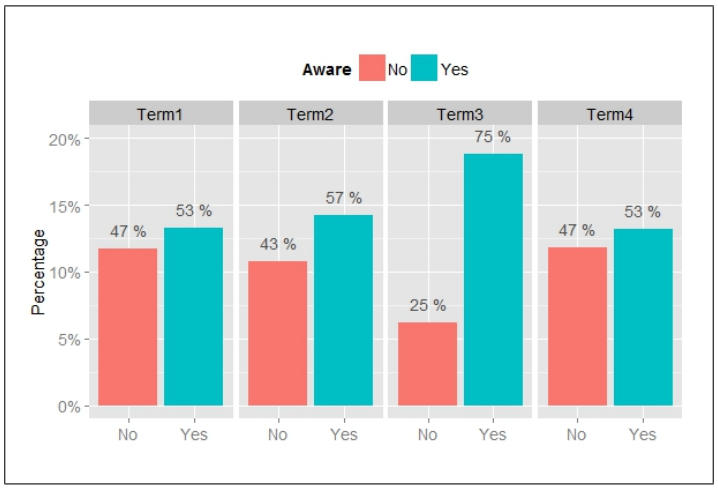

Figure 3. Users' awareness of general terms of use on GeoSNs; grouped by terms.

4.2.2. Perceptions of Possible Privacy Implications

In this section, users' attitude towards the inference by the application of personal information is examined. In particular, the questions aim to gauge users' awareness of plausible inferences about their private places, activities at different times, their connections to other users, and possible knowledge of this information by the application. Participants were presented with 14 statements, shown below and were asked to indicate, for each statement, whether they are aware that the statement is possible and to score their reaction to the possibility of this statement as either 'OK', 'Uncomfortable' or 'Very Worried'. The first twelve statements refer to information that can be derived from the user's location history, which is commonly accessible to 'friends' in most application, if the account is not visible to the public. The last two statements reflect commonly used terms of use, giving the application the right to share the user's data with other users and third parties. The dimension of the data queried is indicated against the statement number (Spatial (Sp), Temporal (T), Social (Sc)). Results are summarised in Figure 4.

- *S1-Sp: I can guess where your home is.*
- *S2-Sp: I can guess where your work place is.*
- *S3-SpT: I know which places you visit and at what times.*
- *S4-SpScT: I can tell where you normally go and what you do on your weekends.*
- *S5-SpScT: I can tell you where you go for lunch or what you do after work.*
- *S6-Sp: I know your favourite store (your favourite restaurant, your favourite coffee shop, etc.)*
- *S7-SpSc: I can guess what you do when you are in a specific place.*
- *S8-SpT: I can guess when you are AWAY from home.*
- *S9-SpScT: I can guess when you are OFF work.*
- *S10-Sc: I know who your friends are.*
- *S11-SpScT: I know when and where you meet up with your friends.*
- *S12-Sc: I can guess which of your friends you see most.*
- *S13-SpT: Other people can know where you are at any point in time.*
- *S14-SpScT: Other people can know what you are doing at any point in time.*

In terms of awareness, users seem to be most aware of statements S1, S2 and S10, regarding the location of home, place of work and friends, representing 88%, 89% and 93% respectively. On the other hand, users are least aware of statements S5, S13 and S14 that relate to other users' knowledge of personal mobility patterns and activities, representing 34%, 37% and 40%. Despite a reasonable level of awareness of the plausibility of these statements, users seemed to be relatively concerned about their privacy. 66% of users were either uncomfortable (41%) or 'very worried' (25%). Over half of the responses to S2 (awareness of workplace-53%) and S10 (awareness of friends-65%) were not concerned.

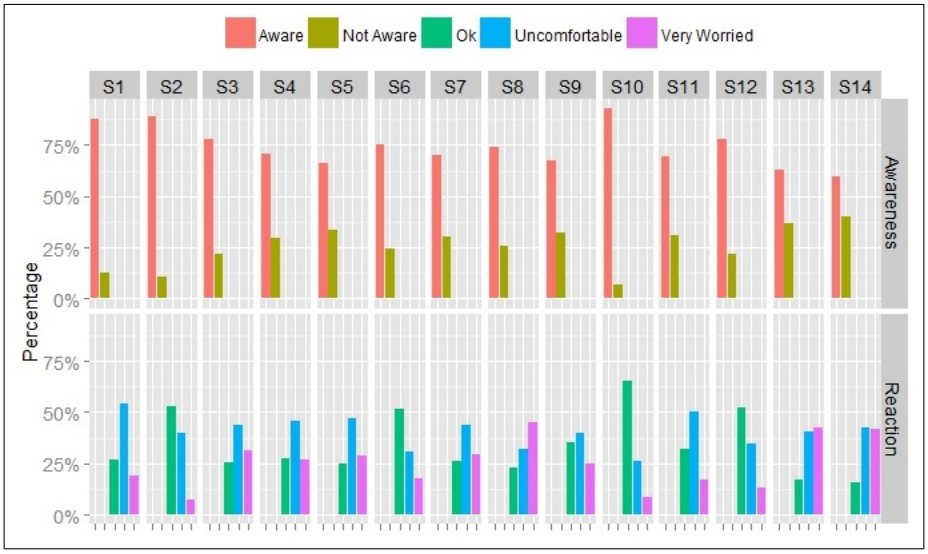

Figure 4. Users' awareness and reaction about potential information inferences; grouped by statement S1–S14.

On the other hand, participants were concerned with S13 and S14 (combined 'Uncomfortable' and 'Very Worried' categories) scoring 83% and 84% respectively. S1 and S11, relating to the location of home and meetings with friends were rated most 'Uncomfortable' corresponding to 53% and 51%, respectively. Statement S8, suggesting the knowledge of the user's absence from home and S13, indicating the possible knowledge of this information by other people presented a significant source of worry to users, with 45% and 42%, respectively indicating that they are 'Very Worried' about these statements. Figure 4 shows the users' awareness and reaction towards the potential information inferences grouped by statement.

It appears that users who read the terms and polices are more aware (by 9%) of the statements, while users who have not read the terms and polices were significantly 'Very Worried' (by 21%) than other users. Indeed, reading terms and policies was found to significantly impact users' awareness of potential inferences (Pearson Chi-Square = 16.637, $p < 0.00001$), and concern levels (Pearson Chi-Square = 16.867, $p < 0.00001$). Moreover, there is a positive correlation between the age of the participant and their level of awareness (Pearson Chi-Square = 46.50, $p < 0.00001$); the level of awareness considerably increases with increase in age group, with the oldest active age group (35 to 44 years) scoring 89%. Yet, younger users, in the age group 15 to 34 years, tend to be relatively less concerned than older users (by 4%). As can be seen in Figure 5, the level of users' concerns increases with the decrease in the frequency of use of the applications (Pearson Chi-Square = 35.636, $p < 0.00001$), where 76% of occasional users are concerned compared to 63% of frequent users. Again, gender does not seem to have any significant influence in this study.

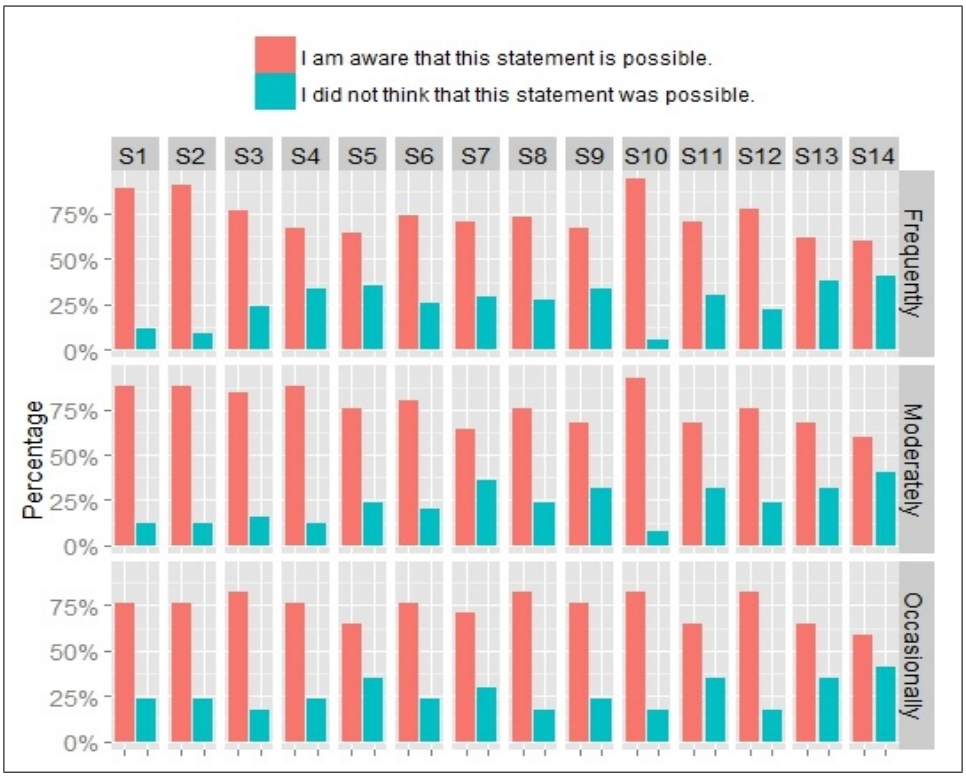

Figure 5. Users' awareness of potential information inferences relative to the frequency of use of the location services; grouped by statement S1–S14.

4.2.3. Attitude to Privacy on Social Networks

The aim of this section of the questionnaire is to understand the users' reaction with regards to using the applications, given the knowledge of potential implications on privacy from the previous section.

61% of users stated that they would change the way they share their location information, 55% of whom are willing to stop sharing their location information completely, with the rest of the group indicating they would share it less often. Frequent users seem to be the most motivated to change their sharing behaviour (13% more than infrequent users), but they are also not willing to stop sharing the information and would prefer to share less frequently than the infrequent users (by 47%). Interestingly, users of location services are more tempted (by 10%) to change how they disclose their location information compared to users who have not used them (Pearson Chi-Square = 18.450, $p < 0.00001$). 57% of the first group of users want to share their location less frequently and 43% are willing to

discontinue disclosing their location data. Younger users (15–34) are more willing to change their usage behaviour (by an average of 18%) and are even more willing to stop sharing location information completely (by an average of 10%) than older users. In this case, it seems that female users are more motivated to change their attitude regarding location disclosure (by 11%) than males, yet 60% of male participants suggested their willingness to discontinue using location services.

4.2.4. Managing Personal Information

In this section, users' views on managing and controlling access to their location information are explored. This includes several aspects related to what information is stored, how it is shared or viewed by the application and by others, and whether users need to manage access to their information. The following statements were presented to the participants who were asked to rate how often they would use them: 'All the time', 'Occasionally' or 'Never'.

- *C1: I would like to be able to turn off location sharing for specific durations of time.*
- *C2: I would like to turn off location sharing when I visit specific types of places.*
- *C3: I would like to decide how much of my location information history is stored and used by the application - for example, use only my check-in history for the last 7 days.*
- *C4: I would like to see the predicted personal information that the application stores about me based on my location information.*
- *C5: I would like to decide how people see my current location - for example, exact place name, or a rough indication of where I am.*
- *C6: I would like to decide who can download my location information data.*
- *C7: I would like to know, and control, which information can be shared with other Web applications.*
- *C8: I would like to make my location information private—seen only by myself and by the people I choose.*

Results are given in Figure 6a and show a significant desire to use these controls for location privacy. Overall, 76% of participants would like to apply those controls 'All the time', 20% are happy to apply them 'Occasionally', and only 4% of users will not consider these controls.

In general, C2, C6, C7 and C8 were most favoured controls, scoring over 97% each of users' responses. Controls C1, C6 and C7 were the controls most chosen to be applied all the time, representing 91%, 88% and 86% of users' responses respectively. It is worth noting that users of different location services have similar acceptance rate for these control. Foursquare and Facebook users have the highest preference for applying the controls 'All the Time', corresponding to 76% and 75% respectively. A negative correlation appears to exist between users' tendency to use these privacy controls all the time and their age group as shown in Figure 6b, where the youngest active age group of 15–24 years old has the highest desire for all-the-time application of controls representing 78% of this group's responses.

As expected, users who are tempted to change their location sharing behaviour have relatively higher motivation to use these controls representing 97% of this group's responses (4% higher than users who are reluctant to change)(Pearson Chi-Square = 81.170, $p < 0.00001$). The factors of gender, whether users read the applications' terms or how frequent they use the social networks seem to have minimal influence on their willingness to use these controls.

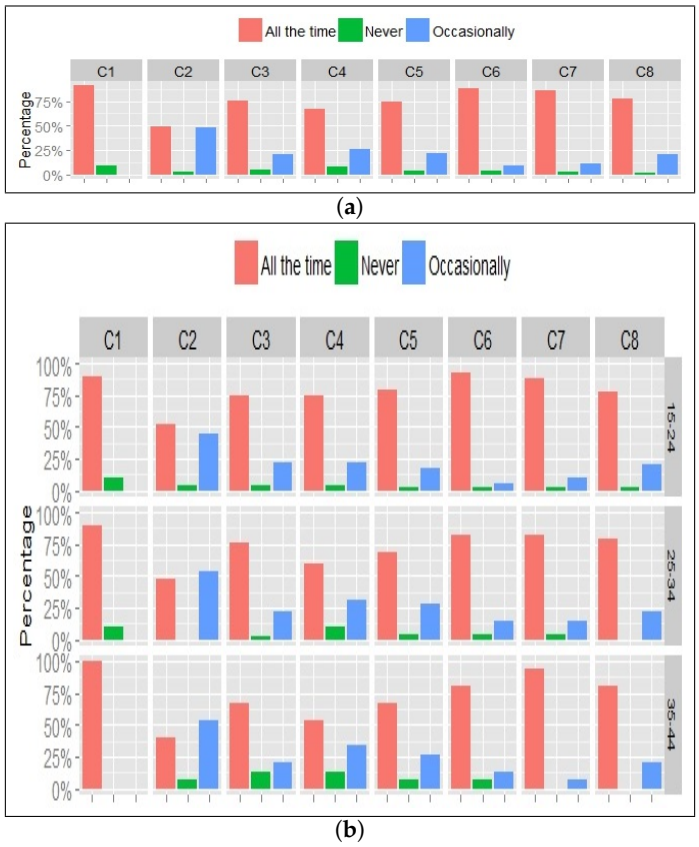

Figure 6. (**a**) Users' desire to use location privacy controls grouped by statement of controls C1–C8; Section 4.2.4, and grouped by age in (**b**).

4.3. Levels of Threat to Location Privacy

The results of the study are used to derive an abstract model of privacy threat levels, which can then be tested in the next section of the paper. Two variables determine the threat to user's privacy, namely, amount and content of disclosed information, and, the visibility scope of the information. Three levels of visibility scope can generally be assumed: (a) private (no access to other people); (b) friends (access only to user's friends); and (c) public (access to others whether inside or outside the social network). The extent of exposure of the user's data can be measured along the data dimensions: spatial; social; spatial-social; or spatial-social-temporal. Guided by the results of the above study, three levels of privacy threats are proposed to represent users' perception.

- Green: safe to disclose the information,
- Amber: caution; disclosing the information can result in moderate privacy implications, and,
- Red: danger; disclosing the information can result in risky privacy implications.

Table 1 is a summary of the level of privacy concern against the data dimensions revealed by the survey above. In Table 2 the values in Table 1 are classified under three categories as follows. In the case of the public scope of visibility, an 'Amber' classification was used with a threshold of $\geq$30% for the 'Uncomfortable' attribute value and a 'Red' classification was used with a threshold of $\geq$30% for the 'Very Worried' attribute value. In the case of friends scope of visibility, an 'Green' classification was used with a threshold of $\geq$40% for the 'Ok' attribute value and an 'Amber' classification was also used with a threshold of $\geq$40% for the 'Uncomfortable' attribute value.

Table 1. Average privacy concern level categorised by the data dimension of the presented inferences.

Dimension	Privacy Concern Level		
	OK	**Uncomfortable**	**Very Worried**
Spatial	*43.9%*	*41.6%*	14.5%
Social	*58.6%*	*30.6%*	10.8%
Spatial-Social	26.3%	*44%*	*29.6%*
Spatial-Social-Temporal	25%	*42.6%*	*32.3%*

Table 2. Classification of privacy threat levels against the dimensions of data.

Dimension	Visibility	
	Friends	**Public**
Spatial	green	amber
Social	green	amber
Spatial-Social	amber	red
Spatial-Social-Temporal	amber	red

4.4. Feedback Design for Location Awareness

To enable user content awareness in GeoSNs, privacy-enhancing feedback and control tools need to be designed and incorporated within the services. The development of such tools need to consider two requirements, (a) which content needs to be communicated to the user? and (b) how (and when) should the content be communicated to the user to satisfy (and enhance) their privacy awareness?

The first question involves considering the communication of three aspects related to a geo-profile. These are as follows.

1. Data content, both captured or constructed. Ultimately, a view of the whole geo-profile data space is possible, including historical data stored and inferred.
2. Visibility (or accessibility) of the geo-profile content to other users. The user needs to be able to know which other users in the network are able to gain access to their data, which types and how much volume of the data are visible.
3. Estimated threat level associated with the geo-profile. An indication of the link between content and visibility can be summarised as a degree of threat to user privacy. Some default estimation mechanism can be used to determine the levels of threat, such as the one described above, but this can be customised by the user, who may be able to indicate more accurately their perception of the value of their own data sets.

Figure 7 is an example of a feedback tool that communicates the three aspects above. The figure shows an icon design for the feedback tool in the form of a location pin with a lock as an indicator for privacy threat. The colour of the icon is used to reflect the level of threat estimated by the system. The icon allows the user to explore their content to understand the basis for the threat indicated. This can be in the form of a concise pop-up window, as shown in Figure 7b that includes: (a) a summary of the current location status; (b) visibility permissions granted; (c) a view of the geo-profile that lists possible constructed information based on this location.

The second question is related to the usability of the design used for the feedback and control tools. Several research works have considered this issue and proposed design principles and frameworks for building privacy-friendly systems [46–49], and highlighted important pitfalls [50] that privacy designers should avoid. The rest of this paper examines the efficacy of such a feedback tool in delivering location awareness to users, while the usability of the design is outside the scope of the current study.

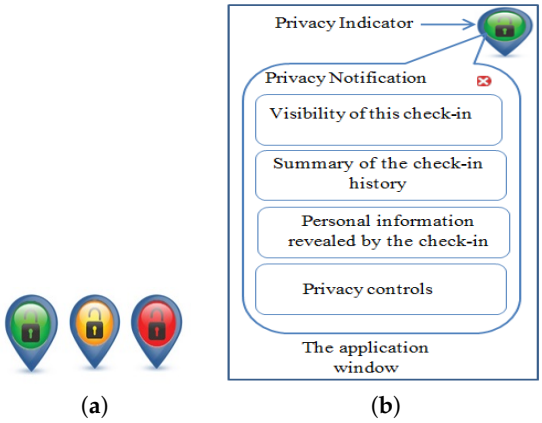

Figure 7. Design of location privacy feedback and control tool. (**a**) Threat level icon design; (**b**) Content exposed for enhancing awareness.

5. Experimental Section

This experiment is designed to evaluate the relationship between the location awareness model presented and users' privacy perception and behaviour on GeoSNs. In particular, the experiment will aim first to explore the impact on a user's perception of privacy due to providing privacy feedback including, (a) The presentation of the geo-profile content, and (b) the use of a privacy threat level indicator. Secondly, the experiment will study the impact on a user's behaviour when sharing his location data online due to his perception of privacy, resulting from the introduction of the privacy feedback with and without offering privacy controls.

5.1. Method

The Location-Based Social Network (LBSN) Foursquare was chosen as a platform for this study. It is a fairly popular LBSN that provides a typical example of GeoSNs, and as such has been used in several previous studies in the literature [21,27,51,52].Using a public GeoSN for evaluation provides more accurate insights of the general user's privacy attitude and bahaviour rather than using restricted location-sharing applications (e.g., [3–5]). Foursquare offers place discovery and recommendation services based on users' location and previous visits to places (check-ins). User's friends have access to his place profile, and the user is also able to grant access to other users who visit the same places in his profile. A user can also opt out from background location tracking and from behaviourally targeted ads.

The experiment took the form of an online user study that utilises realistic scenarios of using the Foursquare checking-in application. Screenshots of the application were presented to the participants describing different scenarios. The scenarios were designed for checking-into places to cover different patterns of data exposure along the spatial, social and temporal axes. Simulated feedback is provided 'just-in-time' when needed during task execution and visibility of the information to 'friends' or 'public' is explicitly presented in the pop-up privacy notification window. On the spatial axis, patterns of presence as well as absence from places were used and on the social axis, patterns of co-location with friends as well as of interest in certain concepts and activities, that may be inferred as a consequence of visiting the place or sharing a tip in the place, were used. Six scenarios were presented in random order with two conditions, as shown in Table 3. First, the scenarios are presented with feedback only and then presented again with actionable controls over the information disclosed. We opted for within-subjects design, since we were interested in capturing the impact of privacy awareness with and without controls, whilst reducing the error variance associated with individual differences (e.g., [33,53]).

Table 3. Summary of the check-in scenarios used.

Scenario	Privacy Level	Visibility	Inferred Information
1	Amber	Public	Social
2	Amber	Friends	Spatial-Social
3	Green	Friends	None
4	Red	Public	Spatial-Social-Temporal
5	Red	Public	Spatial-Social
6	Amber	Friends	Spatial-Social-Temporal

5.2. Procedure

The user study is an online survey with four main sections. The first section collects the participants' demographics, captures their experience using social networks, and observes their location privacy concerns, awareness and behaviour when using them. This is to allow a comparison to be made of those variables after the experiment.

The second section is the feedback-only section. Six check-in scenarios are presented to the user. In every scenario, the normal Swarm Swarm is the checking-in application for Foursquare. check-in screen is presented with the check-in task details and a location privacy icon displayed on the top left corner. A second screen is presented showing the location awareness pop-up window that would appear if the user were to click on the privacy icon, as shown in Figure 8a. In what follows, red, yellow and green were refer to location privacy threat levels.

(**a**) (**b**)

Figure 8. A sample of the location awareness notice with a yellow privacy threat indicator in the (**a**) feedback-only scenarios; (**b**) feedback and control scenarios.

The set of questions in this section are designed to capture the impact of the information on their privacy awareness and concern, their agreement with the choice of level threat associated with information and finally whether they would modify their check-in in any way if given the option to do so.

In the third section, the same check-in scenarios are used, but with the location privacy window now providing control options as well. Participants were offered the opportunity to delete any of the information elements presented from their geo-profile (by modifying the user data in a way that makes deriving the presented information element is impossible), to change the visibility of the check-in or opt to abort this check-in all together, as shown in Figure 8b.

The final section examines the participants' perception with regards to their personal privacy, their need to be aware of the contents of their geo-profile and their need to control access to their data, as a consequence of participating in the study. Moreover, questions were used to gauge their reaction towards the location awareness tool proposed and its usability.

Pilot tests were conducted on three research students in the school and three Amazon Mechanical Turk workers who met the participation criteria (discussed in next section) in order to ensure the clarity

and coherence of the user study. The tests provided valuable feedback on the structure and wording of the survey.

5.3. Recruitment and Participants

The experiment was conducted in May 2015. Participants were recruited using Amazon Mechanical Turk (MTurk) and were confined to those who use the Foursquare/Swarm application and check-in frequently (not less than three times a week on average). This was necessary to enable the participants to realistically relate themselves to the scenarios presented and to use their experience with the application when commenting on privacy implications. The MTurk workers also need to have 95% or more approval rate for at least 500 tasks to be able to participate to make sure that they provide valid feedback according to the study instructions.

Of the 363 who entered the study, 25 workers were excluded with the qualification test. Three hundred thirty-eight participants undertook the study, completed it in 23 min on average and were compensated $1.5 each. The demographics questions revealed that most of the participants were young people (mean = 30.29, SD = 6.45), with slightly more male participants (57%) than female ones (43%). Furthermore, the majority were from North America (59.2%) and Asia (34.6%).

6. Findings

Analysis of the survey data and presentation of the results were achieved using R statistical programming language, and SPSS was used for applying Friedman, McNemar-Bowker, Cochran's Q and Spearman's rank correlation tests. An overview of participants' social networking experience and pre-study privacy concerns is presented first, followed by analysis of the results from the check-in scenarios section and finally the post-study reflection on privacy perception and evaluation of the location awareness tool.

6.1. Pre-Study Phase

A pre-study evaluation of the participants' privacy concerns on the application was conducted to understand the relationship between their level of experience with the application, their location sharing behaviour and their privacy concerns. Most of the participants were moderate users (check-in several times per week) (57.6%), while the rest were frequent users (check-in once or more per day) (42.4%). In addition, most participants would enable location services on their mobile devices (52% enable them frequently (always on) and 43% enable them moderately (when required by an application)).

Accessibility to the user personal data by other users is a primary privacy concern. This is commonly controlled by defining the visibility of one's profile in the privacy settings within the network. 'Friends' on Foursquare are granted access to the full location history and thus can potentially have access to a complete geo-profile. However, it is interesting to note that people will accept friendship requests from strangers and in fact, may not be fully aware of their friendship links. This idea was examined in the questionnaire where participants were asked if they actually know all of their friends (or would accept friendships with users whom they do not know), and revealed that only 31.7% of users know all their friends (44.4% know most of them, 23.4% know some of them).

While 64% of participants think check-ins can be dangerous, most stated that they currently feel safe using Swarm (87%). Although this observation may seem contradictory, the sense of safety attributed to the application may be related to the ignorance of the amount of information stored by the application and its possible consequences. This fact was noted in their response to a question on which aspects of their location history were they able to recall; about 47% were able to recall only one aspect and 2.7% remember nothing of their history. Moreover, 71% of participants thought that the privacy settings provided were sufficient to protect their privacy, but many (46.15%) also admitted to not checking their privacy settings for a long time.

6.2. Check-in Scenarios Phase

Here the results of the questions from sections II (feedback only) and III (feedback and control) of the study are presented.

6.2.1. Impact of Content on Privacy Perception

Sufficiency of The Content Provided

Following every scenario, two questions were used to gather users' perception of the sufficiency of the information content provided to convey privacy risk and the effect of the information on their privacy concerns. Most of the participants reported that the tool sufficiently indicated the privacy risks associated with the check-in scenarios, as shown in Figure 9. The agreement was highest in the red level scenarios, followed by yellow and green (representing 77%, 68%, and 63% respectively).

The content presented have a clear impact on the participants' privacy concern based on the threat level of the check-in scenario (Friedman Chi-Square = 91.227, $p = 0.000$), where participants were mostly concerned about their privacy in the red level scenarios as expected, followed by yellow and green (representing 72%, 55%, and 45% respectively). There is also a positive correlation between the participants' concern level with the threat level of the check-in scenario (Spearman rank correlation = 0.245, $p = 0.000$). Hence, the more threat the location disclosure poses, the more concerned the participants are on their privacy.

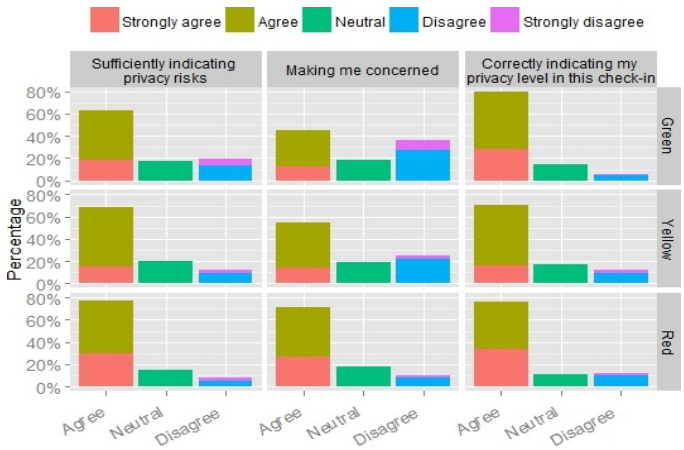

Figure 9. Effectiveness of the tool in conveying privacy risk; grouped by threat level.

Perception of Threat Level Estimation

A high level of agreement (>75% overall) is reported by participants with the threat level indicator presented in every scenario (green: 80%, yellow: 76%, and red: 71%), whereas on average only 10% think the tool should indicate a different threat level. Of the 10% who disagreed with the threat level indicated, some thought that the threat is understated (it should be higher), as explained in their comments ("This seems like a fairly high degree of access to information" and "The application is profiling me and allowing any random person to know these things about me. That's extremely scary"), while others felt that the privacy setting provided by the application were enough to neutralise the threat ("Only my friends will see my details" and "I am protected by my privacy settings").

6.2.2. Impact of Content on User Behaviour

Figure 10 demonstrates the effect of content awareness on the attitude of users to modify their behaviour. On average, over 50% of users chose to modify their check-in action in some way, whereas

the rest either chose to abort the check-in completely (28%) or would proceed without making changes (22%).

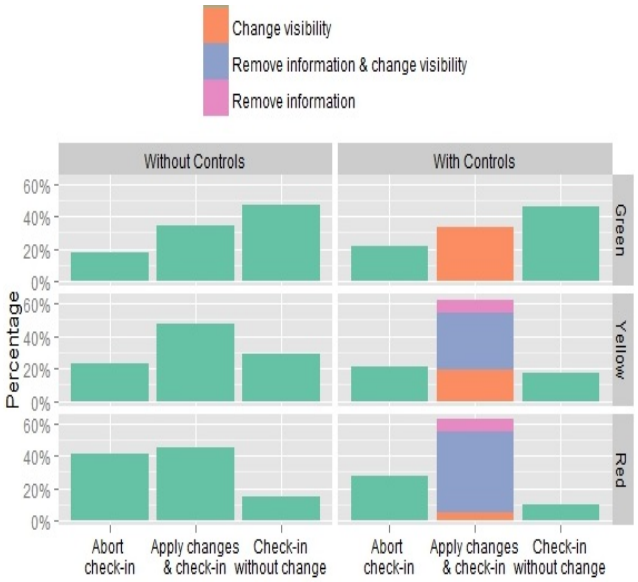

Figure 10. Check-in decision with and without the privacy controls; grouped by the threat level indicator.

Scenarios with actionable control options significantly impact check-in behaviour (McNemar-Bowker = 91.495, $p = 0.000$), where the tendency to modify the check-in increased by 14% in the control scenarios (feedback only: 44%, feedback and control: 58%). In addition, with the control options, users were less likely to abort the check-in (by 7%), presumably as they were given more options to modify their information content. Users were rather conservative when choosing the control options, with 63% choosing to both remove the inferred information from their profile and change the visibility of their check-in, and the remaining group chose to either change the visibility (25%) or to remove the inferred information (12%).

Impact of the Threat Level Indicator on Behaviour

The threat level presented has a significant impact on the participants' check-in behaviour (Cochran's Q = 33.566, $p = 0.000$). In particular, participants were equally willing to apply changes to their check-ins in the red (54%) and yellow (55%) threat levels, and less so with the green level (34%). Similarly, aborting a check-in was mostly evident with the red level scenarios 34%, followed by yellow and green (22%, and 20% respectively). As would be expected, 'proceed with no changes' option was more evident with the green level scenarios, followed by yellow and red (representing 47%, 23%, and 12% respectively).

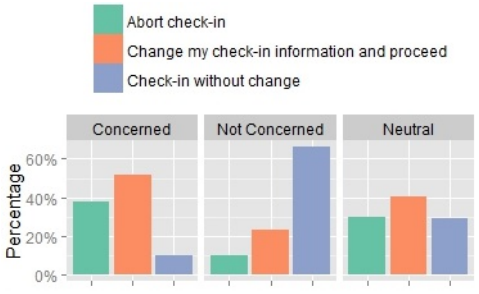

Figure 11. Users' attitude to checking-in after using the privacy tool; grouped by level of privacy concern.

Privacy Concern and Behaviour

It is useful to observe the impact of the level of privacy concern on the actions participants chose to perform (Cochran's Q = 254.628, $p = 0.000$), as presented in Figure 11. Participants who reported concern about their privacy were the most willing to modify their check-in information or to abort the check-in (52% and 38% respectively), followed by the group who were neutral about the privacy concerns (41% and 30% respectively). Note that the group who reported no privacy concern were still willing to modify their check-ins and abort the check-in scenarios (23% and 10% respectively). A positive correlation was noted between the participants' level of concern and their check-in attitude, where higher levels of concern resulted in an increased tendency towards modifying the check-in information or aborting the check-in (Spearman rank correlation = 0.405, $p = 0.000$).

Support in Decision-Making

Here we question how the participants' decided to modify their check-in actions as a response to the feedback and control conditions. Control scenarios were found to more significantly influence the decision to take action (McNemar-Bowker Test = 19.466, $p = 0.000$), where 41% (compared to 33%) of participants strongly agree that control scenarios were helpful in decision-making compared to the feedback condition. The difference was more pronounced in the red threat level scenarios as shown in Figure 12.

Figure 12. Support for decision-making based on the availability of privacy controls; grouped by threat level.

Behaviour Analysis

Figure 13 shows the distribution of participants' control actions in relation to particular aspects of their geo-profiles. Most participants decided to remove some of the shared information and to change the visibility of their check-in. The majority chose to remove reference to sensitive places (82%), followed by a reference to their interests (77%), their favourite friends (67%), patterns of visit (66%), and current absence from sensitive places (64%). Overall, 50% of the participants chose to change the visibility of their check-ins when controls were provided, as shown in Figure 10.

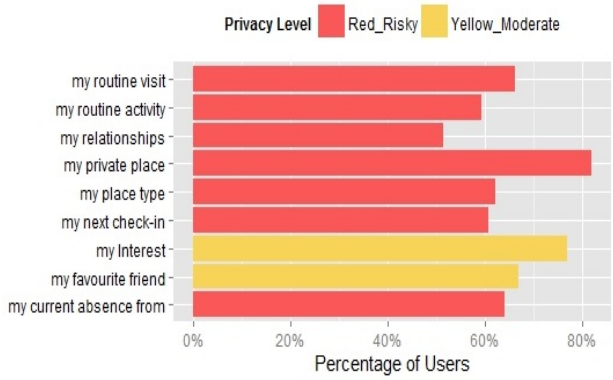

Figure 13. Distribution of the user's choice of information to be removed from their profile in the red and yellow threat levels scenarios.

6.3. Post-Study Phase

The overall effect of location awareness on privacy concern was measured in post-scenarios questions (Cronbach's $\alpha = 0.78$) and results are shown in Figure 14. The figure confirms the assumptions made at the start of this study, where a significant portion of participants (66%) were not aware of the possible information content in their geo-profiles and (71%) underestimated the privacy risk associated with their check-in activity. Similarly, (76%) reported that they are now more concerned about their location privacy (47% of those were strongly concerned), and 8% were not concerned.

Comparing privacy concerns before and after the study (check-in scenarios with the privacy feedback), it was clear that the tool has a significant impact on the level of privacy concern of participants (McNemar-Bowker Test = 284.520, $p = 0.000$), where a strong negative correlation between the concern level before the scenarios was noted (Spearman rank correlation = -0.829, $p = 0.000$). As a consequence, most participants (84%) also suggested that the experiment will impact the way they use Swarm in the future ("will be more cautious").

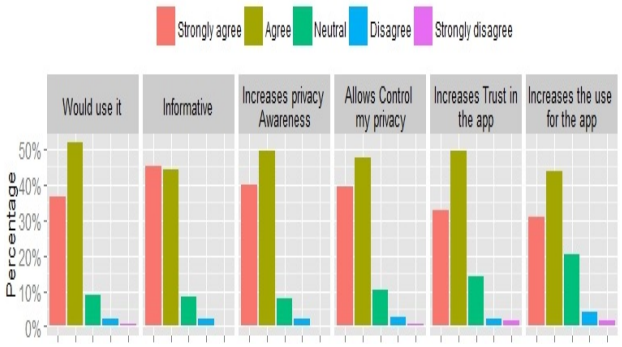

Figure 14. Privacy perception after using the tool.

7. Discussion and Conclusions

User's awareness of the consequences of sharing their location online is rather limited. The reason is twofold: firstly, due to the limitations in our abilities as humans to attend to and recall information that are not needed directly to the task at hand, thus we will not seek to recall details of our spatiotemporal profiles when checking-in a place, and secondly, due to the limited support offered by the social networks to enable users' perception of their information content.

This paper addresses this problem by (a) analysing the scope of privacy threats on geo-social networks, along the spatial, temporal and social dimensions of data in geo-profiles; (b) proposing the design of feedback tools that project a view of the level of threat associated with the disclosure of

location information; and (c) testing the implication of presenting the feedback on users' perception of privacy concerns and their attitude towards sharing their location data on social networks.

The experiments revealed that privacy concerns when sharing location information are grounded, as users are not generally aware of the extent of the information they are sharing or who is able to access their information. The results also pointed to the fact that users trust the applications they use, despite believing that there are risks associated with sharing their location data.

However, as users become more educated about the associated threats to their personal privacy, results show that they are willing to modify their behaviour significantly (similarly to what was noted in [3,5,36,37]), possibly leading to limiting their use of the service (by hiding their profiles) or deserting it all together (aborting checking-in). This contrasted what Tsai et al. [4] found that willingness to share increased when knowing who viewed the user's location which might be due to the limited awareness offered (accessibility rather than content awareness). Some recommendations from the above study for the design of privacy-sensitive GeoSNs can be summarised as follows.

- The network needs to provide a transparent interface to the user's geo-profile, allowing the user the opportunity to explore both their captured data and the information inferred from the data.
- Users need to be able to remove or modify the contents of their geo-profiles.
- Users need to be guided on how to optimise their geo-profiles for privacy, i.e., the network service can suggest which aspects of the profile are redundant and may be removed and which aspects are essential for maintaining a quality of service.
- In terms of social privacy, some model of privacy threat needs to be adopted and used to help the user attend to and take appropriate control actions to protect their privacy.
- Privacy polices need to present a clear model of what data are captured, its purpose, as well as the sorts of information that could be mined and stored in the user profile.
- Users should be told which bits of information from their geo-profile will be shared with 3rd parties and should be given the opportunity to make an informed consent on these decisions.

With regards to the methodologies adopted in this research, it is worth noting some limitations that may have affected the validity of the results. The study relied on MTurk as a convenient means for providing the pool of participants. Appropriate screening of participants' characteristics was used, but this may not have fully avoided recruiting some who may wrongly claim required levels of experience and use of the application. The level of experience of the MTurk worker is an important factor in their appreciation of how the application works and the amount of information that may be collected about them, and could therefore influence their ability to answer the questionnaire. MTurk offers a highly valuable approach to data collection, but given its possible limitations [54], it is important to validate the results through other approaches, e.g., by conducting interviews with a representative sample of users.

Also, static scenarios of the application use were adopted in the second experiment to gauge users' perception and attitude to privacy. Whilst the users were initially primed and made aware of the prototypical nature of the test, the scenarios are admittedly limited in nature compared to realistic use of a working system. Thus the test environment may have influenced the choices users made in response to the questions asked. There are normally tradeoffs to be made when choosing a user-based experimental methodology, related for example, to the representativeness and size of sample used or the level of intrusiveness of the test. Hence, it is also important to employ other approaches in the future, for example, user observation or experience sampling, to compare and validate the results of this experiment. Future work will look further into the design aspects of the proposed feedback and control tools, in particular, the scope of information to be revealed and its timing with respect to task performance, and will seek in-depth evaluation of the usability aspects of the design.

Acknowledgments: The authors would like to thank the anonymous reviewers for their helpful and constructive comments that greatly contributed to improving the quality of this paper.

Author Contributions: F. Alrayes and A. I. Abdelmoty conceived and designed the experiments; F. Alrayes performed the experiments and analyzed the data; F. Alrayes and A. I. Abdelmoty wrote the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Tang, K.P.; Lin, J.; Hong, J.I.; Siewiorek, D.P.; Sadeh, N. Rethinking location sharing: Exploring the implications of social-driven vs. purpose-driven location sharing. In Proceedings of the 12th ACM International Conference on Ubiquitous Computing, Copenhagen, Denmark, 26–29 September 2010; pp. 85–94.
2. Alrayes, F.; Abdelmoty, A. Privacy concerns due to location sharing on geo-social networks. *Int. J. Adv. Secur.* **2014**, *7*, 62–75.
3. Patil, S.; Schlegel, R.; Kapadia, A.; Lee, A.J. Reflection or action?: How feedback and control affect location sharing decisions. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Toronto, ON, Canada, 26 April–1 May 2014; pp. 101–110.
4. Tsai, J.Y.; Kelley, P.; Drielsma, P.; Cranor, L.F.; Hong, J.; Sadeh, N. Who's viewed you? The impact of feedback in a mobile location-sharing application. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Boston, MA, USA, 4–9 April 2009; pp. 2003–2012.
5. Sadeh, N.; Hong, J.; Cranor, L.; Fette, I.; Kelley, P.; Prabaker, M.; Rao, J. Understanding and capturing people's privacy policies in a mobile social networking application. *Pers. Ubiquitous Comput.* **2009**, *13*, 401–412.
6. Vicente, C.R.; Freni, D.; Bettini, C.; Jensen, C.S. Location-related privacy in geo-social networks. *IEEE Internet Comput.* **2011**, *15*, 20–27.
7. Mohamed, S.; Abdelmoty, A.I. Computing similarity between users on location-based social networks. *Int. J. Adv. Intell. Syst.* **2016**, *9*, 542–553.
8. Shokri, R.; Theodorakopoulos, G.; Le Boudec, J.Y.; Hubaux, J.P. Quantifying location privacy. In Proceedings of the 2011 IEEE Symposium on the Security and Privacy, Oakland, CA, USA, 22–25 May 2011; pp. 247–262.
9. Benisch, M.; Kelley, P.G.; Sadeh, N.N.S.; Cranor, L.F. Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs. *Pers. Ubiquitous Comput.* **2011**, *15*, 679–694.
10. Beresford, A.R.; Stajano, F. Location privacy in pervasive computing. *IEEE Pervasive Comput.* **2003**, *2*, 46–55.
11. Sweeney, L. Achieving k-anonymity privacy protection using generalization and suppression. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.* **2002**, *10*, 571–588.
12. Gruteser, M.; Grunwald, D. Anonymous usage of location-based services through spatial and temporal cloaking. In Proceedings of the 1st International Conference on Mobile Systems, Applications and Services, San Francisco, CA, USA, 5–8 May 2003; pp. 31–42.
13. Krumm, J. A survey of computational location privacy. *Pers. Ubiquitous Comput.* **2009**, *13*, 391–399.
14. Duckham, M.; Kulik, L. A formal model of obfuscation and negotiation for location privacy. In Proceedings of the International Conference on Pervasive Computing, Munich, Germany, 8–13 May 2005; pp. 152–170.
15. Krumm, J. Inference attacks on location tracks. In Proceedings of the International Conference on Pervasive Computing, Birmingham, UK, 26–27 July 2007; pp. 127–143.
16. Shokri, R.; Theodorakopoulos, G.; Danezis, G.; Hubaux, J.P.; Le Boudec, J.Y. Quantifying location privacy: The case of sporadic location exposure. In Proceedings of the International Symposium on Privacy Enhancing Technologies Symposium, Waterloo, ON, Canada, 27–29 July 2011; pp. 57–76.
17. Duckham, M.; Kulik, L. Location privacy and location-aware computing. *Dyn. Mob. GIS* **2006**, *3*, 35–51.
18. Mokbel, M.F.; Chow, C.Y.; Aref, W.G. The new casper: Query processing for location services without compromising privacy. In Proceedings of the 32nd international conference on Very large data bases. VLDB Endowment, Seoul, Korea, 12–15 September 2006; pp. 763–774.
19. Shokri, R.; Theodorakopoulos, G.; Troncoso, C.; Hubaux, J.P.; Le Boudec, J.Y. Protecting location privacy: Optimal strategy against localization attacks. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, Raleigh, NC, USA, 16–18 October 2012; pp. 617–627.
20. Cheng, Z.; Caverlee, J.; Lee, K. You are where you tweet: A content-based approach to geo-locating Twitter users. In Proceedings of the 19th ACM International Conference on Information and Knowledge Management, Toronto, ON, Canada, 26–30 October 2010; pp. 759–768.

21. Pontes, T.; Vasconcelos, M.; Almeida, J.; Kumaraguru, P.; Almeida, V. We know where you live? Privacy characterization of foursquare behavior. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing, UbiComp '12, Pittsburgh, PA, USA, 5–8 September 2012; pp. 898–905.
22. Sadilek, A.; Kautz, H.; Bigham, J. Finding your friends and following them to where you are. In Proceedings of the fifth ACM International Conference on Web Search and Data Mining, WSDM '12, Seattle, WA, USA, 8–12 February 2012; pp. 723–732.
23. Gao, H.; Tang, J.; Liu, H. gSCorr: modeling geo-social correlations for new check-ins on location-based social networks. In Proceedings of the 21st ACM International Conference on Information and Knowledge Management, Maui, HI, USA, 29 October–2 November 2012; pp. 1582–1586.
24. Crandall, D.; Backstrom, L.; Cosley, D.; Suri, S.; Huttenlocher, D.; Kleinberg, J. Inferring social ties from geographic coincidences. In Proceedings of the National Academy of Sciences of the United States of America, San Diego, CA, USA, 25 October 2010; Volume 107, pp. 22436–22441.
25. Scellato, S.; Noulas, A.; Mascolo, C. Exploiting place features in link prediction on location-based social networks categories and subject descriptors. In Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Diego, CA, USA, 21–24 August 2011; pp. 1046–1054.
26. Dearman, D.; Truong, K. Identifying the activities supported by locations with community-authored content. In Proceedings of the 12th ACM International Conference on Ubiquitous Computing, Copenhagen, Denmark, 26–29 September 2010; pp. 23–32.
27. Noulas, A.; Scellato, S.; Mascolo, C.; Pontil, M. An empirical study of geographic user activity patterns in foursquare. In Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media, Barcelona, Spain, 17–21 July 2011; pp. 70–73.
28. Cheng, Z.; Caverlee, J.; Lee, K.; Sui, D. Exploring millions of footprints in location sharing services. In Proceedings of the International Conference on Weblogs and Social Media, Barcelona, Spain, 17–21 July 2011; Volume 2010, pp. 81–88.
29. Preotiuc-Pietro, D.; Cohn, T. Mining user behaviours: A study of check-in patterns in location based social networks. In Proceedings of the Conference on ACM Web Science, Paris, France, 2–4 May 2013; pp. 306–315.
30. Rossi, L.; Musolesi, M. It's the way you check-in: Identifying users in location-based social networks. In Proceedings of the Second Edition of the ACM Conference on Online Social Networks, Dublin, Ireland, 1–2 October 2014; pp. 215–226.
31. Zhong, Y.; Yuan, N.J.; Zhong, W.; Zhang, F.; Xie, X. You are where you go: Inferring demographic attributes from location check-ins. In Proceedings of the Eighth ACM International Conference on Web Search and Data Mining, Shanghai, China, 2–6 February 2015; pp. 295–304.
32. Malandrino, D.; Scarano, V.; Spinelli, R. Impact of privacy awareness on attitudes and behaviors online. *Science* **2013**, *2*, 65.
33. Balebako, R.; Jung, J.; Lu, W.; Cranor, L.F.; Nguyen, C. Little brothers watching you: Raising awareness of data leaks on smartphones. In Proceedings of the Ninth Symposium on Usable Privacy and Security, Newcastle, UK, 24–26 July 2013; p. 12.
34. Anwar, M.; Fong, P.W. A visualization tool for evaluating access control policies in facebook-style social network systems. In Proceedings of the 27th Annual ACM Symposium on Applied Computing, Trento, Italy, 26–30 March 2012; pp. 1443–1450.
35. Rader, E. Awareness of behavioral tracking and information privacy concern in facebook and google. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS), Menlo Park, CA, USA, 9–11 July 2014.
36. Fire, M.; Kagan, D.; Elishar, A.; Elovici, Y. Social privacy protector-protecting users' privacy in social networks. In Proceedings of the SOTICS 2012: Second International Conference on Social Eco–Informatics, Venice, Italy, 21–26 October 2012; pp. 46–50.
37. Emanuel, L.; Bevan, C.; Hodges, D. What does your profile really say about you? Privacy warning systems and self-disclosure in online social network spaces. In Proceedings of the CHI'13 Extended Abstracts on Human Factors in Computing Systems, Paris, France, 27 April–2 May 2013; pp. 799–804.
38. Jedrzejczyk, L.; Price, B.A.; Bandara, A.K.; Nuseibeh, B. On the impact of real-time feedback on users' behaviour in mobile location-sharing applications. In Proceedings of the Sixth Symposium on Usable Privacy and Security, Redmond, WA, USA, 14–16 July 2010; p. 14.

39. Kelley, P.G.; Bresee, J.; Cranor, L.F.; Reeder, R.W. A nutrition label for privacy. In Proceedings of the 5th Symposium on Usable Privacy and Security, Mountain View, CA, USA, 15–17 July 2009; p. 4.
40. Wang, N.; Grossklags, J.; Xu, H. An online experiment of privacy authorization dialogues for social applications. In Proceedings of the 2013 Conference on Computer Supported Cooperative Work, San Antonio, TX, USA, 23–27 February 2013; pp. 261–272.
41. Zhang, B.; Wu, M.; Kang, H.; Go, E.; Sundar, S.S. Effects of security warnings and instant gratification cues on attitudes toward mobile websites. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Toronto, ON, Canada, 26 April–1 May 2014; pp. 111–114.
42. Shi, P.; Xu, H.; Zhang, X.L. Informing security indicator design in web browsers. In Proceedings of the 2011 iConference, Seattle, WA, USA, 8–11 February 2011; pp. 569–575.
43. Bravo-Lillo, C.; Komanduri, S.; Cranor, L.F.; Reeder, R.W.; Sleeper, M.; Downs, J.; Schechter, S. Your attention please: Designing security-decision UIs to make genuine risks harder to ignore. In Proceedings of the Ninth Symposium on Usable Privacy and Security, Newcastle, UK, 24–26 July 2013; p. 6.
44. Maurer, M.E.; De Luca, A.; Kempe, S. Using data type based security alert dialogs to raise online security awareness. In Proceedings of the Seventh Symposium on Usable Privacy and Security, Pittsburgh, PA, USA, 20–22 July 2011; p. 2.
45. Roda, C. Human attention and its implications for human–computer interaction. In *Human Attention in Digital Environments*; Cambridge University Press: Cambridge, UK, 2011; p. 11.
46. Bellotti, V.; Sellen, A. Design for privacy in ubiquitous computing environments. In Proceedings of the Third European Conference on Computer-Supported Cooperative Work, Milano, Italy, 13–17 September 1993; pp. 77–92.
47. Langheinrich, M. Privacy by design—Principles of privacy-aware ubiquitous systems. In *Ubicomp 2001: Ubiquitous Computing*; Springer: Berlin/Heidelberg, Germany, 2001; pp. 273–291.
48. Friedman, B.; Lin, P.; Miller, J.K. Informed consent by design. In *Security and Usability*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2005; pp. 495–521.
49. Adams, A.; Sasse, M.A. Privacy issues in ubiquitous multimedia environments: Wake sleeping dogs, or let them lie. In Proceedings of the INTERACT, Edinburgh, UK, 30 August–3 September1999; Volume 99, pp. 214–221.
50. Lederer, S.; Hong, J.I.; Dey, A.K.; Landay, J.A. Personal privacy through understanding and action: Five pitfalls for designers. *Pers. Ubiquitous Comput.* **2004**, *8*, 440–454.
51. Lindqvist, J.; Cranshaw, J.; Wiese, J.; Hong, J.; Zimmerman, J. I'm the mayor of my house: Examining why people use foursquare-a social-driven location sharing application. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '11, Vancouver, BC, Canada, 7–12 May 2011; pp. 2409–2418.
52. Jin, L.; Long, X.; Joshi, J. Towards understanding residential privacy by analyzing users' activities in Foursquare. In Proceedings of the 2012 ACM Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, Raleigh, NC, USA, 15 October 2012; pp. 25–32.
53. Almuhimedi, H.; Schaub, F.; Sadeh, N.; Adjerid, I.; Acquisti, A.; Gluck, J.; Cranor, L.F.; Agarwal, Y. Your location has been shared 5,398 times! A field study on mobile app privacy nudging. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Korea, 18–23 April 2015; pp. 787–796.
54. Goodman, J.K.; Cryder, C.E.; Cheema, A. Data collection in a flat world the strengths and weaknesses of mechanical Turk samples. *J. Behav. Decis. Mak.* **2013**, *26*, 213–224.