Content Analysis of Privacy Management Features in Geosocial Networking Application

Syarulnaziah Anawar, Yeoh Wai Hong, Erman Hamid, Zakiah Ayop
Faculty of Information and Communication Technology
Universiti Teknikal Malaysia Melaka
Melaka, Malaysia

***Abstract*—Geosocial networking application allows user to share information and communicate with other people within a virtual neighborhood or community. Although most geosocial networking application include privacy management features, one the challenge is to improve privacy management features design. To overcome this challenge, the adaptation of privacy-related theories offers a concrete way to comprehend and analyze how the privacy management features are used as tangible research results that facilitate user and system developer in understanding privacy management. This paper attempt to propose a standardized privacy management features in geosocial networking application from market perspectives that could be utilized by researchers and application developers to demonstrate or measure privacy management features. The objective of this paper is two-fold: First, to map the theoretical constructs guided by Communication Privacy Management (CPM) theory into privacy management features in geosocial networking application. Second, to evaluate the reliability of the proposed features using content analysis. Content analysis is performed on 1326 geosocial networking apps in the market (Google Play store and App Store) to determine the reliability of the proposed privacy management features through inter-coder reliability analysis. The primary findings of the content analysis show that many of the privacy management features with low reliability are from Boundary Turbulence construct. Furthermore, only 6 out of 13 proposed features are deemed reliable, namely, specific grouping, visibility setting, privacy policy, violation, imprecision and inaccuracy. The proposed privacy management features may aid researchers and system developers to focus on the best privacy management features for improving geosocial networking application design.**

Keywords*—Privacy management; communication privacy management theory; social network; geosocial network; content analysis

I. Introduction

Geosocial networking application has gain increased popularity over the years that allow information sharing and communication between peoples. The difference between geosocial network and traditional social network is its location-aware capability. Geosocial networking combines real-time location-reporting capabilities with traditional social network functionality [1]. Geosocial networking applications provide its service by utilizing a number of techniques, such as geocoding, geotagging, and geolocation [2]. These capabilities enhance the functionality of social network. For example, user can update their current location status by using the "Check-in" feature.

However, disclosing user and location information can lead to several privacy risks. According to [1], some of the privacy concerns in geosocial networking are location, absence, and co-location privacy. Location privacy concerns on how detailed the location information that a user wishes to disclose, absence privacy concerns on the absence of privacy violation when the location information reveals user's absence on specific location, while co-location privacy concerns on the "tagging" feature in geosocial network. User's effort is very important in managing privacy sensitivity values in order to achieve higher privacy level and result [3]. Some of the user privacy aspects must be compromised because location information is essential in geosocial networking, and the application should provide automatic support in determining real-time location of the users.

The aim of this study is to propose privacy management features for geosocial networking application. Recognizing substantial challenge in incorporating theoretical privacy constructs into geosocial networking application design, this study attempts to propose a standardized privacy management features that could be utilized by researchers and application developers to demonstrate or measure privacy management features. By doing so, researcher will have better understanding on how most market players manage user privacy in geosocial network and then adapt the reliable privacy features into geosocial networking applications.

This paper presents the analysis of privacy management features and describes the content analysis performed on geosocial networking apps in the market. This paper is set to address research question: "What are the suitable privacy management features to represent the theory-privacy constructs in a geosocial networking application?". The rest of the paper is organized as follows: The first section explains how the privacy constructs are conceptualized as IT artifacts by mapping the constructs derived from Communication privacy management (CPM) theory into privacy management features. Next, this paper presents the data collection method in order to draw suitable sample of geosocial networking application to be evaluated in the content analysis. Finally, the proposed privacy management features are evaluated using inter-coder reliability analysis, highlighting reliable features that contributed positively to future privacy management design.

II. Related Work

Privacy management has been studied widely in the research area of social networking. Although most social

networking applications include privacy management features, the advantage of privacy management is not well understood by social networking users due to poor design of privacy management in the social networking applications [4]. Therefore, one of the most significant research in this area is to improve privacy management features design. Including users into application design is challenging because they should be well-informed about the geosocial networking applications in order to be part of the decision making process to achieve the anticipated application's goal [5].

To overcome this challenge, the adaptation of privacy-related theories offers a concrete way to comprehend and analyze how the privacy management features are used as tangible research results that facilitate user and system developer in understanding privacy management. Some studies have investigated the role of theory driven privacy constructs in privacy management. One of the earlier effort can be seen in [6], where they offer analysis of privacy management practice and the usability aspect of the privacy management. Their work adopted Adaptive Structuration Theory (AST) to establish reliable predictors of online privacy management in social setting. These predictors are particularly useful in measuring user appropriation; which refers to the process of technology adoption and adaptation by user.

Cho [7] applied Communication privacy management (CPM) theory to examine the influence of cultural differences among Facebook users from the US, Singapore, and South Korea in privacy management strategies. On the other hand, Wilkinson [8] has developed a User-Tailored Privacy by Design framework drawn from Privacy by Design philosophy, that combines multiple privacy management features into a single intelligent user interface. In the context of geosocial networking, [9] provide a comparative privacy analysis of several existing geosocial network, and provide discussions on privacy and security recommendation to enhance the protection of privacy in geosocial networking. However, they do not offer substantial recommendation on privacy management features design.

Some studies have investigated the role of theoretical foundation in improving privacy management design from user perspectives. [10] has established content analysis that emphasize on potential damage to users through information security and privacy infringements in mobile health apps. However, there is lack of studies that analyze privacy management features particularly in geosocial networking from market perspectives. Designing the privacy management features from market perspectives may provide knowledge on how the privacy features is taking part in actual practice in geosocial networking application. Consequently, the privacy management features may then be evaluated as part of the tangible results of the theoretical constructs understudy.

III. Conceptualizing Privacy Constructs as IT Artifacts

The challenge in investigating theory-driven privacy management in geosocial networking application is how to conceptualize the privacy management theory into an IT artifact. This study perceives the importance of an IT artifact to provide a tangible research results in order to reach practitioners and stakeholders in the social networking. In the context of this study, the IT artifact is presented as a set of features in social networking application that can be used as building blocks to enforce privacy management among the users. The adaptation of the theoretical foundation offers a concrete way to comprehend and analyze how privacy are used as tangible research results that facilitate users' behavior. The privacy management features are derived by mapping the theoretical conception in the theoretical constructs through various tools in an existing social networking application.

A. Privacy Management Constructs

This study integrates constructs from prominent theory in privacy management, Communication privacy management (CPM) theory as the underlying theoretical foundation for the content analysis conducted in this study. CPM [11][12] is primarily focused on how the decisions of revealing or disclosing private information are made by people. In CPM, privacy is considered to be a process of opening and closing a boundary to others [11]. Margulis [13] regarded CPM as "the most valuable privacy theory for understanding interpersonal computer-mediated communication". As geosocial networking is an integration of location-aware services with online social networks. The services pose substantial privacy threats: user location information may be tracked and leaked to third parties [14]. Therefore, obfuscation is also included as one of the privacy management constructs that could be studied to determine its influence on privacy against neighbor in this study.

The following discussion will examine how these constructs could be applied to social networking, especially to privacy management behavior as guided by CPM theory [11]:

1) Privacy rule characteristics: Refers to how people obtain rules of privacy and understand the properties of those rules to decide how information will be shared. When rules are applied, people may create imaginary or metaphorical boundaries, around their information .

2) Boundary coordination: Refers to when there are multiple parties creating boundary, the information is considered co-owned. All the co-owners should have same understanding on how the privacy should be managed. Coordination of boundaries of privacy and disclosure by the coowner of information based on boundary permeability, linkage, and ownership.

3) Boundary Turbulance: Refers to turbulence among co-owners when rules are not mutually understood and when the management of private information comes into conflict with the expectations of each owner.

4) Obfuscation: Refers to how private information is presented in a falsified manner through data masking. To achieve this, data are deliberately scrambled to inhibit unauthorized access to sensitive materials.

B. Mapping Privacy Constructs into Privacy Management Features

This study first mapped the previously defined privacy constructs into privacy management features. All privacy management features represent each construct and correspond

to mobile geosocial networking setting in order to maintain coherency of this study. Table 1 illustrates how four constructs in the study: Privacy Rule Characteristics, Boundary Coordination, Boundary Turbulence, and Obfuscation could be applied to geosocial networking setting. A list of privacy management features that represent the constructs in geo-social networking application is identified in Table 1. The privacy management features are mapped by reviewing relevant literature on application of CPM theory in mobile application development and conducting discussion with two mobile apps developers.

TABLE I. MAPPING OF PRIVACY CONSTRUCT INTO PRIVACY MANAGEMENT FEATURES

Construct	Feature	Description
Privacy Rule Characteristics	Service access	Feature that allows user to choose whether to allow services, e.g. location service, "find my friend" service to access device data.
	Specific grouping	Feature that allows user to create/join user group for specific communication, i.e. interest based, relationship based.
Boundary coordination	Visibility setting	Feature that allows user to choose who can see their private information.
	Activity Log	Feature that allows user to review who can see their activity.
	Tagging	Feature that allows user to manage the information they are tagged in.
Boundary turbulence	Classification	Feature that allows user to classify another user's role from their perspective.
	Privacy policy	Feature that declares the terms and regulations on information privacy that user needs to obey.
	Education	Feature that educates user the proper ways to control their privacy.
	Notification	Feature that notifies users to control their privacy.
	Violation	Feature that allows user to take action against privacy-violated content/user.
Obfuscation	Imprecision	Feature that allows user to lower the detail of private information disclosed.
	Inaccuracy	Feature that allows user to provide false information to protect their privacy.
	Vagueness	Feature that allows user to include linguistic terms i.e. "near", "around" in providing their information.

IV. PROPOSED PRIVACY MANAGEMENT FEATURES

In this section, the proposed privacy management features are explained in details. These features will be used further in the content analysis on existing geosocial networking applications.

A. Service Access

Service access is a feature that allows the application to access the services of mobile device such as GPS location data, contact information etc. to retrieve data and use it on application. In social network, users can share self-generated content, as well as data and information that is automatically obtained from embedded sensors in mobile device [15]. Most mobile social networking applications show a popup dialogue requesting permission to access location information from the user. Some applications only provide a notification message to notify on automatic acquiring of user location information without allowing users' control over that process [16]. These accesses sometimes are done without user's conscience. Without proper management, the location tracking service might violate user's privacy. Therefore, a privacy feature that allows user managing the service access is needed.

B. Specific Grouping

Specific grouping feature allows user to create a group within a social network based on interest, hobby etc. People prefer to use closed-type social networking services which allow certain participants, who are only invited to the group, to communicate together on a basis of small groups, such as family, friends, alumni, and school clubs. This feature motivates user to utilize social network more as it promotes better quality of interaction and privacy.

C. Visibility Setting

The concept of visibility is widely discussed in regards to social networking privacy [17]. Visibility refers to level of easiness for other peoples to view user profile, information, or posts. Generally, the higher visibility of user information to other peoples, the lesser users' control over their privacy. As most social networking platforms offer association and connectivity, users have the ability to view other users' profiles directly or through a common connection. Therefore, a geosocial networking application should offer visibility setting feature as a privacy-preserving mechanism that support users' controlling decisions regarding who can view their information such as location information or being 'nearby' as named in many application [16].

Fig. 1. Proposed Visibility Setting based on Onion Metaphor.

Onion metaphor from Social Penetration Theory [18] will be adapted in this feature. Figure 1 illustrates the visibility setting illustration which adapts the idea of onion metaphor. The outer layer shows lower privacy level thus leads to disclosure on more common audience. While the inner layer shows higher privacy level and the disclosure is more on specific target.

D. Activity Log

Activity log is a feature that allows user to review their activities in social network. Many geosocial networking users are not aware that a deleted post is not permanently removed from the geosocial networking platform and still can be accessible due to the ease at which information can be saved, shared, and reposted [17]. Some geosocial networking platforms do not offer users' control over their activity stream, making them unaware of all the events that are added to their activity stream, nor who has access to their activity stream [17]. Generally, activity stream can be referred as the timeline or feed that display all of a particular user's activities such as posts, share, and likes. In addition, access control option over sensitive information like location history and health data is an essential requirement in geosocial networking application. For instance, it is important for a user to have access control option, that able to control friend's view of the availability duration of users' locations history when they visited several locations during a certain period of time [16].

E. Tagging

In order to facilitate personal information sharing users' interactions, most geosocial networking application provide four basic functionalities including publishing, recommending, tagging, and pushing [19]. Tagging functionality enables a user to make a reference to their friends' usernames when the user publishes social activities in their account, thus motivating users' interactions. However, this feature introduces the ownership of such information belongs to multiple users. The co-owners will have the responsibility and right in managing the privacy of that information. Therefore, a privacy feature is needed to manage the privacy of tagged information. It is complicated as it involves many users. Turbulence can be happened easily if the privacy is not well coordinated.

F. Classification

Geosocial networking users can be classified into several profile based on their privacy preferences [20]. As a result, users may not demonstrate same behaviours when regulating their privacy management strategies. Consider Anne, a user who is concerned about her privacy, but at the same time likes to make her whereabouts known to her friends. She may wish that at certain circumstances her location information will be viewed only by a selected close friends. For instance, when she is at home with her mother on weekends morning. Therefore, user classification is needed to help user in disclosing the information to correct audience. The difference between this feature and specific grouping is that how user classify others will not affect other people's experience, while specific grouping is based on a collective understanding among multiple users.

G. Privacy Policy

An online privacy policy is a statement that informs users how a service provider handles (e.g., collect, use, access, control) users' personal information [21]. Upon joining or signing up for a geosocial networking application, a user must agree to the privacy policy provided by the application provider. Previous study [22] has emphasized the important role of privacy policy in users' perceived privacy. When a privacy turbulence happens, an inexperienced social network user can refer to privacy policy to understand the choice he has to overcome the turbulence.

H. Education

Many social network users report difficulties in managing their privacy settings [23]. Therefore, privacy experts suggest that users must be given exhaustive control over their privacy to help them regulate their privacy boundaries. In the context of geosocial networking, privacy education is often manifested in the form of notifying users of information sharing practices. The notification is done through textual notices embedded in privacy authorization dialogues [24], and visual icons [25]. In addition, tips about a privacy feature may serve as a helpful reminder to the user prior knowledge [26].

I. Notification

Notification is a feature that provides a popup message to remind users on their incompleteness of privacy configuration or potential privacy risk. The lack of knowledge and awareness of various security tools and option available in smartphones is one of the main contributing factor of data breaches that implicated users' privacy. One of the notification approaches to support privacy decisions is privacy nudging. Nudges refers to soft paternalistic intervention that influence user behavioral and decision making, while allowing user privacy decision to be revised if their expectation is not met [27]. As nudging acknowledges that subtle differences in application design can possibly affect users, nudges are usually in a form of persuasive cue and were embedded in a notification through feedback, defaults, norms, and saliency of features [28]. These notifications help users to better understand their privacy right and configuration, and increase their awareness on privacy threats.

J. Violation

Geosocial networking application must implement certain counter measures when user or data privacy is violated. To suit the context of this study, the scope of interpersonal privacy protection behaviours is broadened to the management of relational boundaries (e.g. friending, and unfriending), territorial boundaries (e.g. untagging posts or photos or deleting unwanted content posted by others), network boundaries (e.g. hiding one's friend list from others), and interactional boundaries (e.g. blocking other users or hiding one's online status to avoid unwanted chats) [29].

K. Inaccuracy, Imprecision, and Vagueness

[30] suggested three types of imperfection that can be used in location information, namely, inaccuracy, imprecision and vagueness. In the context of location privacy, inaccuracy refers to providing different location information instead of the real location. Imprecision refers to providing location information

in the form of region to represent the real location, and vagueness refers to using linguistic terms like "far from" or "near" in the conveyed location.

V. Data Collection Methods

To select suitable application for this study, all related existing application in the mainstream digital distribution platforms which are App Store by Apple Inc. and Google Play Store are reviewed. In App Store, Social Networking category is chosen. Total number of existing applications is 246. For Google Play Store, two categories were emphasized: Social and Communication. For each category, in the Top Free section, it lists 540 related apps which is free and have the most download. Most app developers distribute their apps in both platform. To overcome the duplication problem, the duplicated apps in Play Store will be excluded.

A. Inclusion and Criteria

To obtain the most suitable sample, all related apps are filtered by applying inclusion and exclusion criteria. By doing so, it is expected to improve the study results. General exclusion and inclusion criteria were established to limit the scope of apps being evaluated.

Table II shows the inclusion criteria that will be used in this study. First two criteria have been used in identifying the app pool. For price, the app should be free to use as there is no necessity to use paid apps for academic study. Download count indirectly shows how large the social network userbase is. Although it might not be an accurate measure as it does not reflect the number of active users, it implies the number of users who tested the app. Due to this reason, these apps have research value. This study set the minimum threshold for download count as 100,000. To ensure the app is functioning in Malaysia, the location in App Store and Google Play Store was set as Malaysia. Although these apps are under Social and Communication category, some of them do not actually serve for social purposes. Therefore, this study include only social network/social discovery app.

TABLE II. Inclusion Criteria

Criteria	**Condition**
Type of OS supported	iOS/Android
Category	Social/Communication
Price	Free
Download Count	More than 100,000
Availability in Malaysia	Yes
Type of service	Social network/ Social discovery
Language	English

Among the apps searched with keywords, apps will not be reviewed if it meets one or more of the exclusion criteria. Firstly, the apps for dating and purposes will be excluded because the proposed privacy features are for geosocial network and it is decided to be inappropriate to test these features in these apps. They do not serve as a fully functional social network. The apps which is served for adult only or LGBT community are excluded as these apps contains sexually explicit content and unhealthy communication. Also, there are many apps which is only served as an additional service to a social network. For instances, Facebook Lite, Facebook Mentions, Facebook Groups are the add-on apps for Facebook. Therefore, these type of apps are excluded as well.

B. Data Sampling and Collection

Inter-coder reliability analysis is used by employing independent coders to evaluate the proposed privacy management features and get the same conclusion [31]. The reason to measure reliability is to demonstrate the trustworthiness (truthful) of the proposed features. Coders received the two-phase training and guidance from the researcher and they will evaluate the same case (apps) to maintain consistency in evaluation.

Three coders are involved in the content analysis. The coders evaluate the privacy features in the sample and code the finding in either "1" for existing feature or "0" for non-existing feature. Before content analysis starts, the coders are required to attend a training to get familiar with the coding purpose and procedure.. Two applications which are Google+ and BeeTalk have been selected as training material. The code represents the opinion of coder, in whether the feature is existing on the application. For Google+, there are differing opinions on Classification feature among coders. Meanwhile for BeeTalk, there is a perfect agreement among all features. Coders are advised to review their answer with each other to identify the cause of disagreement. If it is due to carelessness, coders can re-code their result to reach agreement.

ReCal3 ("Reliability Calculator for 3 or more coders") [32] is an online utility that is used to calculate the inter-coder reliability coefficients for nominal data coded by the coders. The coding result will be entered into an Excel and uploaded to ReCal3. It will then calculate the reliability of the feature. Reliability means how far the agreement among coders. Higher reliability means the coders have more similar expectation and idea on that feature. This study accepts the privacy feature based on the acceptance level of reliability coefficient. The rejected features will be discarded from the study.

Based on the comparison among reliability coefficients, Krippendorff's Alpha is the best statistic to use in this study as it has tougher standard on determining the reliability of variable. It is important to ensure the privacy features are reliable in order to conclude that such privacy features are agreed by multiple persons on their characteristics. The difference of Krippendorff's Alpha with other statistic techniques is that it includes observed and expected disagreement. Consequently, it provides more accurate approximation of reliability. It also has three benefits which makes it a better statistic. First, it can be used for any number of coders. It also can be used for any sample sizes and different type of variables. The "bootstrapping" system allows alpha to replace missing value with existing values samples form. Alpha value of 0.667 is the minimum acceptable limit.

C. Data Screening

Figure 2 shows the process of screening the most suitable apps for this study. During the initial screening phase, Google Play Store has significantly more apps than App Store. This is

due to two categories (Social and Communication) were selected into the screening process. Meanwhile App Store only has categorized all the related apps into Social Networking, therefore the number of apps appeared to be lesser.

Firstly, the applications are evaluated based on inclusion criteria. As the result shown, 230 out of 246 apps in App Store have been selected for inclusion. Meanwhile Google Play Store has only 261 out of 1080 apps selected. This is because Google Play Store has many apps that do not related to social network or social discovery, especially in Communication category which only has 30 apps included for next phase. Then the included applications are filtered based on exclusion criteria as shown in Table III.

From Table III, it can be seen that most of the applications are either add-on based on social network or social network manager. These add-ons are used to enhance the functionalities of existing social network. For example, Facebook Groups allows user to manage their group in Facebook better than using the Facebook app itself. Social network manager is used to manage different social network in one platform. User can receive information and notification from different social network in one app. It provides convenience to the users who have multiple social network accounts. Finally, duplicate apps in Google Play and Apps Store that are similarly named from the same developer were removed from the dataset, leaving 65 apps for content analysis. The content analysis of the apps were examined in the next section.

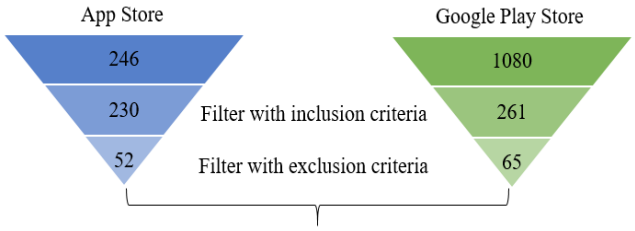

Fig. 2. Data Screening.

TABLE III. INCLUSION CRITERIA

Criteria	App Store	Play Store
Purpose	28	35
Audience Target	12	16
Nature of Service	138	155
Total	178	196

VI. RESULTS AND DISCUSSIONS

A. Inter-Coder Reliability Analysis

Table IV shows the result of the inter-coder reliability analysis. The result shows that six out of 13 proposed features are agreed by the coders to be reliable. The accepted features are specific grouping, visibility setting, privacy policy, violation, imprecision and inaccuracy.

TABLE IV. RESULTS OF INTER-CODER RELIABILITY ANALYSIS

Feature	Krippendorff's Alpha	Result
Specific Grouping	0.747028862	Accepted
Visibility setting	0.673782157	Accepted
Violation	0.709551657	Accepted
Imprecision	0.673782157	Accepted
Inaccuracy	0.754934211	Accepted
Privacy policy	0.757657902	Accepted
Education	0.533431571	Rejected
Notification	0.530925926	Rejected
Vagueness	0.260912698	Rejected
Service access	0.180339632	Rejected
Activity log	0.48760181	Rejected
Tagging	0.569097294	Rejected
Classification	0.527827293	Rejected

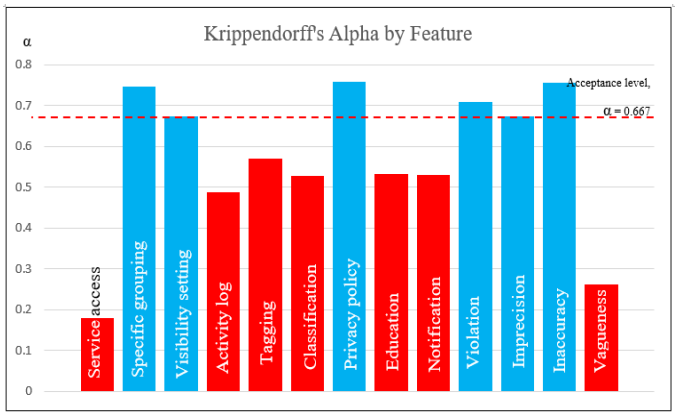

Fig. 3. Proposed Privacy Features based on Krippendorff's Alpha.

Figure 3 shows the bar chart of content analysis result. Based on the Figure 3, it can be seen that that many of the privacy management features with low reliability are from Boundary Turbulence construct as prevalence in most cases is low.

B. Discussions

Based on the inter-coder reliability analysis, the result shows that six out of 13 proposed features are agreed by the coders to be reliable. The accepted features are *specific grouping*, *visibility setting*, *privacy policy*, *violation*, *imprecision* and *inaccuracy*. From the findings, it can be seen that privacy policy feature is the most agreeable privacy feature as it has the highest reliability values (α=0.757657902). Privacy policy can be found in almost every application as it is required by law to protect user. Due to that, it is undeniable that privacy policy is a must-have feature in geosocial networking application.

Specific grouping feature is a privacy feature that allows user to define the user group to disclose information with. Based on the result, it shows a high reliability as well (α=0.747028862). This study views it as a reliable feature that cannot be neglected when developing a social network, especially for neighbourhood. User should be allowed to define smaller group within neighbourhood based on e.g. interest, hobby. By doing so, it protects the privacy of user as some information like body health conditions are sensitive to disclose, even to whole neighbourhood.

However, service access feature has a very low result value (α=0.180339632). After discussing with coders, the problem is identified. It is hard to define whether the feature is existing in an application. Some applications will prompt a popup message asking for permission to access services such as messaging and location [15]. The aforementioned privacy feature is not included in this study as the setting is done on the operating system level. This study consider such privacy feature exists only if the application provides options for user to decide whether to allow application to access service. This study put an emphasis in privacy features implementation on application level to provide a guideline for potential practitioner. However, coders are unsure on such feature existence as they have different opinion on the definition. Therefore, the agreement is very low.

Visibility setting feature allows user to define their information is visible to whom. This privacy feature is very common among social networking application as it is widely discussed in regards to social networking privacy [16]. Every private information in social network should be allowed to define its visibility by its owner. However, many social networks did not provide this feature on every information provided by user. This can be seen as the limitation of the development of social network. Nonetheless, this privacy feature is agreed by the coders as a reliable feature due to the results (α=0.673782157), which is slightly above the acceptance value. Figure 4 shows the example on how the visibility setting should be implemented in creating an event in neighbourhood geosocial network.

Fig. 4. Example of Visibility Setting Feature.

Activity log has low reliability values (α=0.48760181). The feature is rejected mainly due to its lack of existence in many applications. The purpose of this feature is for users to review their activity on social network to check whether any of them violates their privacy e.g. disclosed information to wrong audience. This feature provides a safety measure to revert their mistakes in order to protect their privacy. However, many applications do not implement this feature. This may imply the value of this feature is not worthy to develop. Therefore, this study does not make this an exception from rejection.

The purpose of tagging is to manage the tagged information to achieve privacy control. Therefore, a privacy mechanism is needed to manage this tagged information. However, this feature's alpha did not meet the acceptance level. Based on coder's opinion, there is a number of applications does not provide tagging function or could not identify the feature as some applications only allow including other users in messaging but not information sharing. Due to this reason, disagreements happened and the reliability value became low (α=0.569097294).

Violation is a feature to manage the privacy violated user or content. This feature acts as a counter measure for user to react on the violation. When a turbulence in a relationship happens, users can choose to revise the relationship. User can either choose to negotiate with that user, remove that relationship, or block that user without notifying. There are many ways to handle privacy violation. If that user is causing irritation or harm to the public, reporting to authority can be done. It can be seen that this feature is very important in managing privacy. It shows high reliability values (α=0.709551657) as well.

Classification is a feature to classify the user into type such as friend, family, close friend, etc. It works similar to specific grouping except it emphasizes on defining user type and works as a personal list of multiple types of relationship. Based on the coding result, the existence of this feature is low. Also, based on the feedback of coders, they had a tough time on identifying the feature as they confused it with specific grouping. These factors contribute to low reliability values (α=0.527827293).

Education consists of any material that provides knowledge to user on privacy management. This includes tutorial on privacy configuration, FAQ (Frequently Asked Question), privacy guideline, etc. This feature is analyzed to be not reliable mainly due to differing opinions of coders. One of the coders thought that some education feature was not enough to be identified to be education, while the others thought many of the privacy features are education-tailored. Scenario like this caused disagreements and led to low reliability value (α=0.533431571). Also some studies found that educational tips could be considered annoying by users [33]. Therefore, this feature will be excluded in this study.

Notification is a feature that provides a popup message to remind users on their incompleteness of privacy configuration or potential privacy risk. It shows low reliability values (α=0.530925926). Based on coders' feedback, it is said that identifying the occurrence of this feature is difficult as these reminders usually appear after the user using the application for some time. Therefore, the coder who received notification would identify this feature as exist, and vice versa. In addition,

some studies [33] have found that using notification such as nudges would likely cause annoyance among users, which may hinder effective deployment of privacy nudges.

Imprecision allows user to lower the details of disclosed information. Fr instance, instead of full house address, user can choose to disclose the approximate area of living only. This feature provides option to cater different user privacy requirement. By doing so, user can still be expected to provide truthful information willingly as they can choose what they wish to disclose. However, this feature's reliability values (α=0.673782157) are just barely passed the acceptance level. This is due to some disagreement among coders that the idea of imprecision might exist in an application, but not for all the information. imprecision feature might occur in personal information but not location information. Therefore, in the same application, the coders might have different opinion on the existence of imprecision. However, this study does not reject this feature even though it might not be actually reliable. Figure 5 shows an example of imprecision technique application that is viable in geosocial network. To protect the user's location privacy, user can choose to lower the details about his location information.

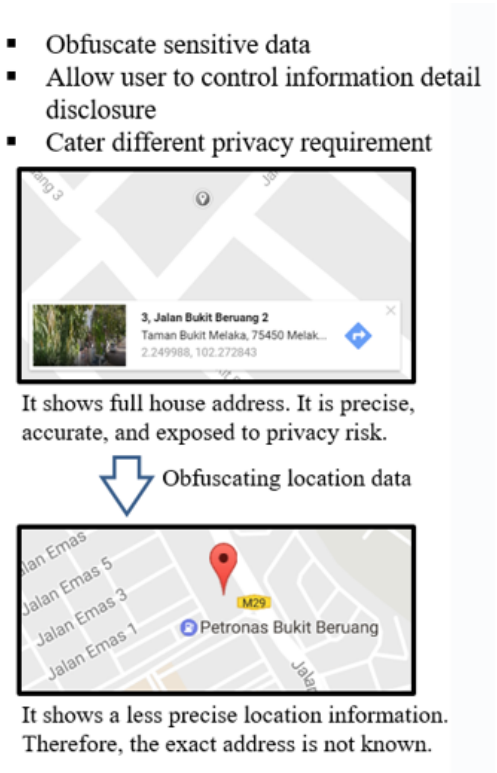

Fig. 5. Example of Imprecision Feature.

For inaccuracy feature, the reliability values (α=0.754934211) are the second highest among all the features. This feature is defined as "feature that allows user to provide false information to protect their privacy". The coders consider inaccuracy feature exist if the application does not validate the information entered by user and enforce to obtain the information from sensor (e.g. location data by using GPS location). Therefore, the coding process of this feature was lenient if based on the definition. Nonetheless, this feature is still playing a significant role in managing the privacy. By providing inaccurate information to protect their privacy, user can prevent unwanted attention from other users. For example, a user wishes to conceal the fact that he is hospitalized as to prevent their neighbours from knowing and causing potential harassment. He updates his location information by manually input some tourism spots so that his neighbours may assume he is on vacation. In a more technical way, inaccuracy can be done in location privacy by showing a location shifted away from the actual coordination. This masking technique provides convenience to the user in protecting their privacy.

Vagueness is a feature that allows user to include linguistic terms i.e. "near", "around" in providing information. This feature has a very low reliability value (α=0.260912698) probably due to two reasons: 1. Its inexistence in most applications. 2. Coders' difficulty in identifying the feature. Most applications do not provide an option for user to enter these approximation terms. When user provides imprecise or inaccurate information, the information must have a value. This is the nature of how computer applications and database work. By providing a vague information, it leads to difficult data handling and processing, where cannot be handled by most applications. They can only provide such vague information as a suggestion based on user's input. Therefore, this feature is rejected.

VII. Conclusion and Future Work

In summary, this paper presented privacy management features that represents theoretical constructs derived from Communication Privacy Management theory. To provide empirical evaluation of the proposed features, a content analysis was performed on 1326 geosocial networking apps from the market. After data screening, 65 apps were analyzed using inter-coder reliability analysis. The primary findings of the content analysis showed that many of the privacy management features with low reliability are from Boundary Turbulence construct as prevalence in most cases is low. The findings show that that 6 out of 13 proposed features are deemed reliable. The reliable privacy management features are specific grouping, visibility setting, privacy policy, violation, imprecision and inaccuracy. The proposed privacy management features may aid researchers and system developers to focus on the best privacy management features for improving geosocial networking application design. Consequently, it will provide an insight on how most market players implement privacy management in geosocial networking and then adapt the reliable privacy features into geosocial networking applications.

In general, this study found 7 out of 13 privacy features with low inter-coder reliability. Based on the Krippendoff result. The low value of alpha may not necessarily reflect low level of agreement, but due to the prevalence of privacy features in all apps is very low. Therefore, the reliability of this study can be improved by corroborating other prominent privacy theories in the research of managing online privacy as present study only includes four privacy management processes in the model. In addition, further extension of this work may include the use of mix-methodology such as case study, or phenomenology to further analyze and gain more

insight on privacy management in geosocial network application. Case study can be conducted by using an existing popular geosocial networking application as a case, then collecting the data about user experience. This is required to investigate and accommodate reliability issues in the present study and highlight specific user behavior with privacy features, that may be used to confirm and increase the reliability the proposed privacy management features.

ACKNOWLEDGMENT

This paper is funded by Global Commission on the Stability of Cyberspace (GCSC) Grant (GLUAR/HGCC/2018/FTMK-CACT/A00015). A high appreciation to Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka (UTeM) for facilitating the work done in this paper.

REFERENCES

[1] C. R. Vicente, D. Freni, C. Bettini, and C. S. Jensen, "Location-related privacy in geo-social networks," IEEE Internet Computing, vol. 15, no. 3, pp.20-27, 2011.

[2] S.L. Low, S. Anawar, Z. Ayop, M. R. Baharon, E. Hamid, "Self-organized Population Segmentation for Geosocial Network Neighborhood", International Journal of Advanced Computer Science and Applications, Vol. 9, No. 9, pp. 230-235, 2018.

[3] G. Lugano, and P. Saariluoma, "To Share or not to share: Supporting the user decision in Mobile Social Software applications," International Conference on User Modeling, Springer, Berlin, Heidelberg, pp. 440-444, July 2007.

[4] C. A. Dwyer, and S. R. Hiltz, "Designing privacy into online communities," Proceedings of Internet Research 9.0, Copenhagen, Denmark, October 2008.

[5] S. Anawar, G. P. Ananta, Z. Z. Abidin, Z. Ayop, and S. Yahya, "Conceptualizing autonomous engagement in participatory sensing design: A deployment for weight-loss self monitoring campaign," In 2013 IEEE Conference on e-Learning, e-Management and e-Services (IC3e), pp. 111-116, Dec 2013.

[6] C. Dwyer, S. R. Hiltz, M. S. Poole, J. Gussner, F. Hennig, S. Osswald, and B. Warth, "Developing reliable measures of privacy management within social networking sites," In 2010 43rd Hawaii International Conference on System Sciences, IEEE, pp. 1-10, Jan 2010.

[7] H. Cho, B. Knijnenburg, A. Kobsa, and Y. Li, "Collective Privacy Management in Social Media: A Cross-Cultural Validation," ACM Transactions on Computer-Human Interaction (TOCHI), vol. 25(3), pp 17, 2018.

[8] D. Wilkinson, S. Sivakumar, D. Cherry, B. P. Knijnenburg, E. M. Raybourn, P. Wisniewski, and H. Sloan, "Work in Progress: User-Tailored Privacy by Design", 2017.

[9] S. Gambs, O. Heen, and C. Potin, "A comparative privacy analysis of geosocial networks," In Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS, pp. 33-40, Nov 2011.

[10] T. Dehling, F. Gao, S. Schneider, and A. Sunyaev, "Exploring the far side of mobile health: information security and privacy of mobile health apps on iOS and Android," JMIR mHealth and uHealth, vol. 3(1), 2015.

[11] S. Petronio, "Communication boundary management: A theoretical model of managing disclosure of private information between marital couples," Communication Theory, vol. 1(4), pp.311-335, 1991.

[12] S. Petronio, "Boundaries of privacy: Dialetics of disclosure," Albany, NY: State University of New York Press, 2002.

[13] S. T. Margulis, "Three theories of privacy: An overview," In Privacy online, Springer, Berlin, Heidelberg, pp. 9-17, 2011.

[14] B. Carbunar, R. Sion, R. Potharaju, and M. Ehsan, "Private badges for geosocial networks," IEEE Transactions on Mobile Computing, vol. 13(10), pp.2382-2396, 2014.

[15] A. S. Teles, F.J.D.S. e Silva, and M. Endler, "Situation-based privacy autonomous management for mobile social networks," Computer Communications, No. 107, pp.75-92, 2017.

[16] R. Ajami, N. Al Qirim, and N. Ramadan, "Privacy issues in mobile social networks," Procedia Computer Science, No. 10, pp.672-679, 2012.

[17] J. Fox, and J.J. Moreland, "The dark side of social networking sites: An exploration of the relational and psychological stressors associated with Facebook use and affordances," Computers in Human Behavior, No. 45, pp.168-176, 2015.

[18] I. Altman, D. Taylor, "Social penetration: The development of interpersonal relationships," Holt, Rinehart and Winston, NewYork, 1973.

[19] Y. Li, Y. Li, Q. Yan, and R.H. Deng, "Privacy leakage analysis in online social networks," Computers & Security, No. 49, pp.239-254, 2015.

[20] P.J. Wisniewski, B.P. Knijnenburg, and H.R. Lipford, "Making privacy personal: Profiling social network users to inform privacy education and nudging," International Journal of Human-Computer Studies, No. 98, pp.95-108, 2017.

[21] N.F. Awad, and M.S. Krishnan, "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization," MIS quarterly, pp.13-28, 2006.

[22] Y. Chang, S.F.Wong, C.F. Libaque-Saenz, and H. Lee, "The role of privacy policy on consumers' perceived privacy," Government Information Quarterly, 2018.

[23] H.R. Lipford, A. Besmer, and J. Watson, "Understanding Privacy Settings in Facebook with an Audience View," UPSEC, 8, pp.1-8, 2008.

[24] B.P. Knijnenburg, and A. Kobsa, "Making decisions about privacy: information disclosure in context-aware recommender systems," ACM Transactions on Interactive Intelligent Systems (TiiS), vol. 3(3), p.20, 2013.

[25] J.Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti, "The effect of online privacy information on purchasing behavior: An experimental study," Information Systems Research, vol. 22(2), pp.254-268, 2011.

[26] H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L.F. Cranor, and Y. Agarwal, "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, pp. 787-796, ACM , April 2015.

[27] S. Kankane, C. DiRusso, and C. Buckley, "Can We Nudge Users Toward Better Password Management?: An Initial Study," In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems, p. LBW593, ACM, April 2018.

[28] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L.F. Cranor, S. Komanduri, P.G. Leon, N. Sadeh, F. Schaub, M. Sleeper, and Y. Wang, "Nudges for privacy and security: understanding and assisting users' choices online," ACM Computing Surveys (CSUR), vol. 50(3), p.44, 2017.

[29] P.J. Wisniewski, A.K.M. Najmul Islam, H.R. Lipford, and D.C. Wilso, "Framing and Measuring Multi-dimensional Interpersonal Privacy Preferences of Social Networking Site Users," Communications of the Association for information systems, vol. 38(1), 2016.

[30] Y. Liu, Z. Yang, X. Wang, and L. Jian, "Location, localization, and localizability," Journal of Computer Science and Technology, vol. 25(2), pp.274-297, 2010.

[31] H.E. Tinsley, and D.J. Weiss, "Interrater reliability and agreement," In Handbook of applied multivariate statistics and mathematical modeling, pp. 95-124, 2000.

[32] D.G. Freelon, "ReCal: Intercoder reliability calculation as a web service," International Journal of Internet Science, vol. 5(1), pp.20-33, 2010.

[33] L. Jedrzejczyk, B.A. Price, A.K. Bandara, and B. Nuseibeh, "On the impact of real-time feedback on users' behaviour in mobile location-sharing applications," In ACM Proceedings of the Sixth Symposium on Usable Privacy and Security, p. 14, July 2010.