Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Computer Science 10 (2012) 672 – 679

Procedia Computer Science

The 9th International Conference on Mobile Web Information Systems (MobiWIS)

Privacy Issues in Mobile Social Networks

Racha Ajami, Nabeel Al Qirim, Noha Ramadan

Rashaaj@uaeu.ac.ae, Nalqirim@uaeu.ac.ae, Noha-ramadan@uaeu.ac.ae
Faculty of Infomration Technology , UAE University, Al-Ain, UAE

Abstract

Smart mobile devices and an abundance of social mobile applications are emerging that facilitate different interactions between friends and business people. Despite this growing momentum in such social networks; privacy loops as a concern amongst users. The increasing number of users of such applications in general and location-aware applications more specifically, surges the likelihood of security breaches. This is due to the increasing number of users of such applications and to the nature of established trust amongst such users. In this research, we will address such privacy concerns considering the users' points-of-view and their acceptance of such applications highlighting the most common types. The research will elucidate some of the suggested mechanisms to endorse users' trust in social interactions.

Keywords: Mobile social networking, privacy; location-based devices; social network applications.

1. Introduction

It is interesting to witness the revolutionary development in mobile technology from mere devices to complete voice calls to intelligent devices (smart phones) that can process large and multimedia applications carried out by a computer such as office tools, wireless connection and internet browsing. Communicating wirelessly with social network sites or any application over the internet has further attracted the attention of the community. However, like any technology, one of the prominent side effects of such an approach is that it compromises the users' anonymity and makes it more susceptible to eavesdropping, spoofing and wormhole attacks. Whether the mobile device is a part of a Peer-to-Peer (P2P) mobile social network system or a client-Server mobile social network system, the identity of the user is not that anonymous. In P2P social network systems the user can be tracked by collecting the logging date and time of detecting a user's social network identification (ID) and creating a history of visited locations of the users. Because Client-Server system has an access to the social network user's names of nearby users, it compromises the users' anonymity by exposing the user's location for each device connected to that system.

Location-Based Mobile Social Applications (LBSAs) provide services to users by relaying on location information and coordination. It enables users to locate and meet friends in nearby locations and even reminding users by getting a reminder from friends and family when passing by a certain location. As LBSAs provides social recommendation by users to their friends and collaborative content downloaded for users with limited bandwidth, the likelihood of large-scale privacy breaches is expected to occur. LBSA uses applications in Smartphones to pinpoint users' location information and send them to an "un-trusted" third-party server that will provide required services to the user.

doi:10.1016/j.procs.2012.06.086

This research will elucidate aspects related to such security issues, and aims to answer the following main questions:

- What are the main mobile social networking applications?
- What are the most common users' identity and privacy concerns of mobile social networks?
- How to enhance mobile social networks security to endorse trust in mobile social networks?

Section 2 will introduce the idea of Mobile Social Networking and its applications, privacy criteria and people's attitude towards it. Section 3 will discuss location-based application and its different types. Section 4 includes three approaches that will help in endorsing trust in mobile social networks. Section 5 includes a comparison of the discussed approaches and Section 6 highlights some open issues and security needs that were not covered by the approaches we studied. In Section 7 we conclude the paper and summarize our observations with including some remarks and future research directions.

2. Mobile Social Networks

Millions of users are increasingly using always-on always-carried mobile devices to access the internet and social networking applications. Web 2.0 provided applications that facilitated user interaction and content access and generation.

2.1. Mobile Social Networks Applications (SNAs)

In considering applications provided by web2.0 such as Mobile Social Networks Applications (SNAs), Chen and Rahman[1] categorized thirty one applications provided by Apple App. Store as Social Network and grouped them into four categories. First is the Mobile front-end applications represented here by applications similar to desktop applications like MySpace and Facebook that endorse trust amongst friends only and doesn't support interactions between non-friends. Second is the Content Sharing Applications that allow users to share multimedia files (image, voice and video) such as PhotoShare and Twinkle that allow interactions between nearby (non-friend) users. Third is the Neighborhood Exploring Applications which rely heavily on locations and anonymous interaction. It also allows users to find, comment, share, and upload multimedia files between users that can become friends and maybe meet later on. The Last is Mobile-Specific SNAs that are designed specifically for mobile interaction and community such as Avatar and Bluepulse that focus on SMS and email communication, and Loopt and Limbo that allows the display of friends' locations, activities and making comments about visited locations.

2.2. Privacy Criteria of mobile SNAs

Privacy designs for Mobile SNAs are established based on four steps, Capture, Construction, Accessibility and Purposes [13, 14]. Capture discuss the kind of information that is been collected from the mobile device. The majority of mobile SNAs show a popup dialogue asking for permission from the user to access location information. Other applications show a message indicating the automatic acquiring of location information without allowing users' control over that process. Construction criteria discuss what happens to users' information after collecting it. Mainly the action depends on the application beings used, the location information is either retained on the users' device or send externally to another one. Even for applications where the information is stored locally, at some point, it will be transmitted to a larger network or system for additional processing and better use of the service. Moreover, for services as Neighborhood services the information is sent and retained externally. Accessibility discusses who can access users' information after its being collected, which differs as well as from one application to another. Neighborhood exploring applications keep the information in the service provider and allow the accessibility by it where users do not have control over the distance between them and those who can discover their location. Finally, Purpose questions how the information will be used later. Demiris et al. [14] showed that privacy concerns increase with the use of cameras and image capture devices. Moreover; they found that participants emphasized on the need to have control over the system by being able to turn it on and off and determine who has access over their collected information.

2.3. People's Attitude towards Sharing

Nowadays sophisticated mobile phones can surf the internet, capture video, pictures (e.g. third generation mobile phones). Mobile data services are increasing exponentially which could be accessed by mobile social software applications (MoSoSo) which are software that support interaction among mobile users by providing anytime/anyplace coordination and convergence, connecting people with similar interests and profiles, and enhancing mobile social games [15]. Many mobile social network applications are available in the market nowadays such as MamJam, Rummble, Dodgeball, Plazes and Jambo [16].

On the human social behavior level, people usually trade their privacy when they trust the parties they share their information with. The amount of information shared depends on the level of trust among them. When analyzing the trade-offs between privacy and trust amongst users, Lugano and Saariluoma [2] explained that users go through 5 steps: first, the user decides whether to trade privacy or not. Second, users determine the minimal damage then they compute the gain from trust. After that, the trade will take place if the gain is greater that the damage. Finally, users select the set that cause minimal loss.

The selection of the set of friends depends mainly on three things, the user, the message and the recipient. The simplest way to assess the sensitivity of data to a specific user is to ask the user to assigns the privacy-sensitivity of each data-item that could be shared through the mobile device. After completing that step, the application generates the user profile that consists of two parts, public and private ones. The public section is accessed by others, whereas the other part is hidden or used by the user to personalize applications. It is claimed that the application is requiring an effort by the user to set the privacy sensitivity values for each item and each contact. But it is acceptable to compromise users' effort for few times to get a higher quality result and privacy level. Privacy is an essential concept, and automatic support for the users' decision will help reaching that even if time and effort will be compromised. [2]

3. Location-Based Applications

Location-based applications involve tracking peoples' location to provide them with many required services. There are mainly two types of location-based services: location-tracking services that rely on tracking peoples' location by other parties such as cellular service providers or other peers nearby, and position-aware services that rely on the devices' knowledge of their position. Barkhuus et al [18] found that people usually have more privacy concerns with location-tracking services than with position-aware services, in spite of the fact that both services are nearly using the same technology. Location-Tracking services can identify users' location in many ways; the simplest way is to determine the location by approximating it with a known location of another device as the cellular telephone tower or devices in a shorter-range network as Bluetooth. Another method is to measure and calculate latencies between communicated signals. Location tracking method has an advantage of not requiring any extra equipment from the user. Based on all the research made on location-based computing, privacy was the essential concern. When it comes to mobile location-based services, identity is at the core of privacy issues that might include social security number, full name and residency.

To ensure security and users' privacy, and to reduce and eliminate the risk of a large-scale privacy braches; the un-trusted third-party application should be used by the LBSAs to store encrypted data only, and move the application to the client devices. Puttaswamy and Zhao [3] solved this problem by suggesting that users need to exchange cryptographic keys with their friends in an offline social network where those keys will be stored in their mobile devices. Whenever a user needs to exchange or send information, it should be encrypted with the previously shared keys with friends. In Melinger et al [4] users can verify if a message is generated by a friend or not. If yes, then the message will be decrypted. By doing so, users' location is kept private from all non-friend users and servers by moving the application to the client device, encrypting the sent messages, and having the third-party servers as bridge that will help in delivering encrypted data.

Most of recent research studies emphasized on the fact that high degree of privacy is essential to mobile and location-based application users. Minch's study [5] highlighted this issue and showed that people were less concerned about their privacy while using location-based services as long as the service being used is useful. The same study examined 16 participants of different ages and background-knowledge of mobile usage, and found that the usefulness of the service has a positive relation with the likely to be found as an intrusive one. Most of the users were not overly concerned about their privacy while using such services but the concern was higher for location-tracking services than location-aware ones. Barkhuus and Dey [6] conducted a study to figure out the attitude of a number of different users towards navigation services. The results showed that most users did not mind having a service that pushed

information to them (e.g. Advertisements and tags) as long as that service or information was helpful and beneficial to them in a certain situation. Moreover, the result showed that location-aware services are recommended and would be used in emergency situations or in unfamiliar environment but still the service should inform the users of what kind of information is collected about them, how it is used, who will be using it and give the ability to users to control what information is released about them at a certain time.

One of the first models of social network technologies was Socialight. This model had two main services provided, "Friend Locator", and "Tap & Tickle". Find locator tracks user's current location and displays friends and friends of friends that are physically close to the user. After locating a friend, a user can communicate a gesture with friends by controlling the length of a vibration on their phone to "tap" or "Tickle" a friend [4].

4. Mobile Social Network Mechanisms

The internet interconnects the whole world which makes it more difficult to secure information by traditional technical solutions and to assure users' privacy. However, defining the concept of privacy is not that easy. Tomlinson, Yau and MacDonald [17] combined different resources to generate a uniform definition of privacy. They mentioned that privacy is the combination of Solitude, Intimacy, Reserve, and Anonymity. In the following, Different Social Networks Security Mechanisms and approaches are introduced, which could help enhance users' privacy while being a part of a social network via mobile devices.

4.1. Identity Servers and Anonymous Identifiers (AIDs)

This approach provides certain functions that link anonymously a user with his/her location for use by third-party applications. The user's identity will be hidden while requesting information and applications from social network websites. This privacy protection can take place when adapting the approach of Identity Server and its Anonymous Identifier. [7]

The process starts when the user securely contact the IS to request an AID, the AID will be generated with a cryptographic hash function and send it to the user's device. When another device establishes a connection with that device (device A) through a Bluetooth or a Wi-Fi connection, the generated AID will be shared between the two devices. To establish another connection with another device, device A will repeat the same process to get a new AID for the new device.

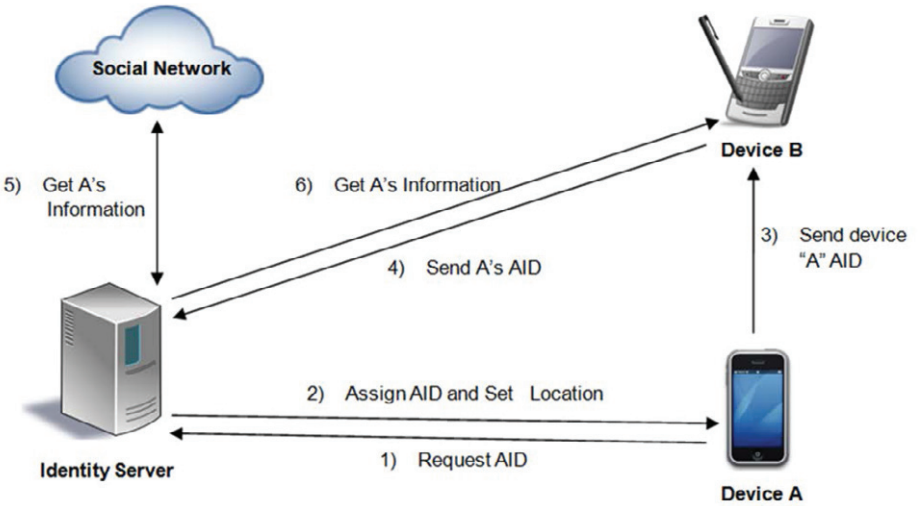

Fig. 1. Identity Server and Anonymous Identifier mechanism process to link a user anonymously while using a third-party application.

When device B gets the AID, it will retrieve the required information from the Social network Profile through the IS. After getting user's A preference and information, the IS will delete the AID of device A from the list of the AIDs associated to device A, then sends the request back to device B. To ensure efficiency, multiple AIDs will be associated to one device to make it able to establish many connections and the same time, but to prevent the AIDs list per device; a timeout period is set. When an AIDs time is out, IS will remove it from the device's associated list. In addition to protecting the anonymity of the user's location, this application prevents eavesdropping by encrypting all network traffic that flows from the devices to the IS and vice versa. However, this implementation of this approach was tested in the limitation of the range between the devices that are being authenticated and sharing the AIDs to retrieve requests from social network sites. [7]

4.2. Virtual Individual Servers for Mobile Devices

It is essential to have total control over a device that will be used to upload contents to social networking sites or any other third-party service. Virtual Individual Servers (VISs) is a virtual machine that runs on computer infrastructure with high availability utilities [8]. One of the most important advantages of VIS is providing long-term availability. In centralized third-part services the user depends on the availability and existence of the provider. In contrast, VIS users can make a complete VIS image backup and resume whenever is convenient. In addition, VIS helps in improving user's privacy by giving the users control over their private data and what information they allow to be shared. Moreover, VISs provide flexibility to the owner to install software packages and set their own preferable configuration options and functionality. Running and controlling wide range of user's data in one centralized third-party server set the users as victims to large-scale privacy breaches. VIS is resistant such breaches because each user own his administrative domain. Also, VIS has an advantage over the mobile device that directly shares data, in which VIS is not limited to energy constraints of those devices sunning off batteries.

One of the applications of VIS is the Participatory Sensing. Mobile devices nowadays are embedded with different sensors as GPSs and Cameras that help in collecting a wide range of data that can be used in many applications. However, the user in there has a little control of what information is collected from owned device as well as affecting the device performance and battery life due to the number of applications that will be running of the user's device. In VIS scheme, the user uploads to collected raw data only once to its VIS which has all the required application and interact on behalf of the user with the sensing server according to the predefined user's specification and limitation. [8]

Problems with VISs are very limited compared with all the benefits provided. One problem is that users need to manage their own virtual machine and taking full responsibility of that. Cost is a problem as well, in which the user will need to pay for the computing resources that is needed by their VISs.

4.3. Re-socializing Social Networks

Nowadays; online social networks (OSN) are developing with a rapid increase of online social network users. Users Requirement analysis have to be done in order to fulfill their requirements such as: Information Self Determination which requires that user's profile and personal content may not disclosed to any other users than the trusted contacts, as a result of that all communication must ensure security against man in the middle attacks. A manageable secure mechanism is required to publish a selected profile attributes depends on the trusted contacts, control profile personal data, and the ability to terminate the own online social network account. Strong trust relationship is an another requirement which limits the maximum length of the chain of trust to one-hop relationships, however the user is able to contact with two-hop relationships; but user shouldn't publish profile information of his one-hop relationship. Profile availability is another requirement, online social networks worth nothing if the published profile information is not accessible at all, so the secure and the privacy of online publication is needed to allow access to data while its owner is offline. Mobility Support is an additional requirement as users needs special supports for mobile devices which currently suffer from limited bandwidth, computing power, and problems with complex user interfaces. [9]

As a result of these requirements a novel decentralized multi-domain OSN design [9] is posited here. It is based on the separation of OSN into the following three domains: Social Webspace, Social Mobilespace, and Social Homespace. To connect with other users there are two proposed basic schemas: out-of-band invitation (OOB) and Coupling. In OOB; users A & B ,for example, agree on a PIN code or password, user A sends an e-mail to user B

containing link to OSN, exchanger address, link public key with some explanatory text. User B can send a message to user A which consist of a new link public key, exchanger address, with secure message authentication code, then user A will refresh the key, then a secure channel will be established so both users will be ready for secure communication.

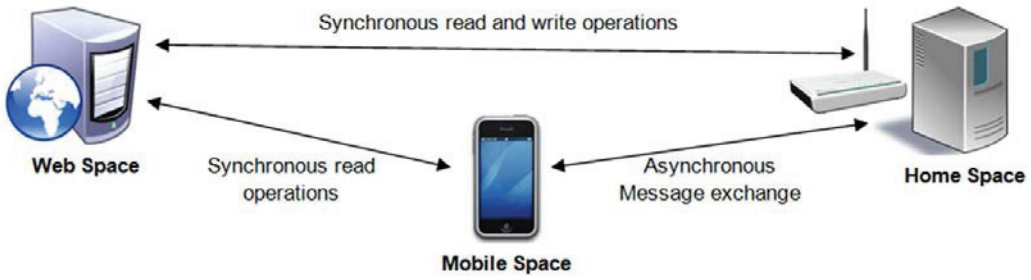

Fig. 2. Decentralized Multi-domain SNS design

Whereas in Coupling; User A sends a coupling request to user B & C which contain parts of B & C profiles which are marked as a public, user A will receive both responses and then the encrypted messages will be forwarded to user B & C, user B & C will perform a key refresh in order comply with strong trust relationship. As user A knows about the link public key which applied during the coupling, it depends on the trust level between A & B and B & C then the key refresh can be trusted without another OOB process. Coupling Mechanism supports the idea of organizing groups by a virtual network user who are taking the role of user A.

5. Comparison and Discussion

We surveyed some of the existing Mobile Social Networks Security Mechanisms and approaches. These approaches will be evaluated based on their performance in respect to the challenges and constraints such as: Flexibility, Operator protection, User's anonymity, and Provider's existence independency.

Table1: Mobile Social Networks Approaches

Project Name	Flexibility	Operator protection	User Anonymity	Dependency
AIDs	Some	Yes	Yes	No
VISs	Some	Some	Some	Yes
Re-Socializing Online Social Networks	Some	Yes	N/A	No

Anonymous Identifiers (AIDs) [7] that are provided by Identity Servers (IS) connects a user anonymously and hides users' identity while requesting information and applications from social network websites. The design is semi-flexible in terms of not requiring much contribution by users. Just in the preliminary setting stage, the user is asked to set an ID and a password to be saved in the IS. On the other hand, design flexibility is limited in terms of limiting the user to a certain range to get out benefits by limiting the application use to a certain range of a Wi-Fi or Bluetooth connection. The approach protects users' information and identity from unauthorized users, which in turn, will maintain users' anonymity. However, this approach is depending on the social network providers' existence to maintain users' information as well as to finalize the initial setting step which required users' ID to generate the IS password.

Virtual Individual Servers (VISs) [8] are virtual machines that run on computer infrastructure with high availability utilities used to upload contents to social networking sites or any other third-party service. VISs provides users with

the ability to get a complete image backup of the information and resume whenever needed regardless of the providers' existence; as a result, VISs provides independence from the social network service provider. Moreover, in VISs users' has the flexibility in adding or removing functions based on their convenience; however there is a need to manage their own machines and afford the cost for the computing resources used by their VISs. Users' Anonymity and Protection from the service provider are not fully achieved in the default situation, however, the user can install arbitrary operating package and set their own configuration options to achieve the anonymity target.

Re- Socializing Online Social Networks approach [14] is a novel decentralized multi-domain SNS design which complies with user requirements. It supports flexibility as users have two main schemas to connect with other users which are out-of-band invitation (OOB) and Coupling, The design is flexible somehow in terms of not requiring much involvement by the users. All the communications, requests, and messages are encrypted with a secure message authentication code, so the operator itself provides the required protection. This approach depends on the availability of providers. Although social web space must be always online as social home space & mobile space cannot be available permanently; it doesn't provide a backup for the users' information available on the social network service provider. As a result, users' profile and information existence depends on the provider existence.

6. Open research issues

Social Networks are one of the main current applications that are being used to share information and contact people across different locations. The studied mechanisms are focusing on securing users' privacy in Social Network Applications (SNA). There is a need for a security mechanism that secures users' activities and operates the main purposes of SNA at the same time, because almost all of the available Smartphones don't support the following privacy issues.

Location-based application in Smartphones should be enhanced in a way that protects users' privacy. A privacy mechanism is an essential requirement that should be added to support the users' controlling decisions regarding who can view their locations or being 'nearby' as named in many Smartphones. For example; if user 'A' is a friend with the users 'B', 'C' and 'D'. User 'A' would like to share his location with his/her entire friends list except 'C', then it is required to have that privacy's option flexibility. Moreover it is required to force a control option over viewing location history . For example if user 'A' visited several locations during a certain period of time; then it is required to have a privacy option that control the availability duration of users' locations history to edit how much friends can view. These privacy and security mechanisms should be applied to Smartphones without limiting them for specific connection ranges; it should be applicable in different types of connections such as Wi-Fi, Bluetooth and different smart phones' subscription packages, to ensure a high-level of users' privacy while using Mobile Social Network Applications. In general, having higher security measures might affect system performance in terms of speed and response time. Such tradeoff was not addressed in any of the surveyed models.

Most of the breaches that affected users' privacy were due to the lack of awareness and knowledge of different security options and tools in available Smartphones. Security awareness update messages or alerts can be circulated periodically for all users to increase their awareness of SNA privacy threats, and available mechanisms and tools that can help enhancing their information privacy.

7. Conclusion

Due to its infancy, this research looked into a scarcely researched topic, Mobile SNAs and its main implications namely security. Accordingly this research attempted to elucidate aspects relating to SNAs with respect to security such as highlighting effective security designs for SNAs. This depends at large on the user's attitude toward such SNAs and whether they would accept trading their private details in most-of-the-times entrusted environments. The research then extended the SNA argument to location-based applications and discussed different SNAs security mechanisms and approaches and portrayed how such approaches could help in enhancing users' privacy. The use of mobile devices and their advanced applications facilitate relationships and interactions between friends who visit the same places or had been in near-by areas. However, as seen in this research, to provide proper applications for users, it is necessary to consider the privacy factors while adding such features into mobile devices. What this research attempted to emphasize and explain here is that there are little measurements established to address many of the security concerns and mechanisms to endorse user trust over mobile social networks.

References

1.G. Chen and F. Rahman, Analyzing privacy designs of mobile social networking applications, In Proceedings of the IEEE/IFIP International Symposium on Trust, Security and Privacy for Pervasive Applications (TSP), Shanghai, China, 2008.

2. G. Lugano , P. Saariluoma, To Share or not to share: supporting the user decision inMobile Social Software applications, In Proceedings of the User Modelling conference, Corfu, Greece, 2007.

3. K. P. N. Puttaswamy and B. Y. Zhao, Preserving privacy in location-basedmobile social applications, in Hotmobile'10 Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, Ohio, USA, 2010.

4. D. Melinger , K. Bonna, M.Sharon, M.SantRamet, Socialight: A Mobile Social Networking System, In Proceedings of the 6th International Conference on Ubiquitous Computing, Nottingham, England, 2004.

5. R. P. Minch, Privacy issues in location-aware mobile devices, In Proceedings of the 37th Annual Hawaii International Conference on System Sciences, Hawaii , USA, 2004.

6. L. Barkhuus and A.K. Dey, Location-based services for mobile telephony: a study of users' privacy concerns, In Interact 2003, ACM Press , Zurich, Switzerland, 2003.

7. A. Beach, M. Gartrell and R. Han, Solutions to Security and Privacy Issues in Mobile Social Networking, In Proceedings of the International Conference on Computational Science and Engineering, Vancouver, BC , Canada, 2009

8. R. Cáceres, L.Cox, H. Lim, A. Shakimov, A. Varshavsky, Virtual individual servers as privacy-preserving proxies for mobile devices, In Proceedings of the MobiHeldconference , New York, USA, 2009.

9. M. D¨urr, M. Werner and M. Maier, Re- Socializing Online Social Networks, In Proceedings of the 2010 IEEE/ACM International Conference on Green Computing and Communications and 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing, Washington, DC, USA, 2010.

10. E. Kaasinen, User needs for location-aware mobile services, In Personal and Ubiquitous Computing, 2003.

11. N. Sadeh, J. Hong, L. Cranor , I. Fette, M. Prabaker , Understanding and capturing people's privacy policies in a mobile social networking application, Personal and Ubiquitous Computing, Forthcoming, 2008.

12. C. Mancini, K. Thomas, Y. Rogers, B. A. Price, L. Jedrzejczyk, A. K. Bandara et al, From Spaces to Places: Emerging Contexts in Mobile Privacy, In Proceedings of the 11th International Conference on Ubiquitous Computing. ACM: Orlando, FL, USA ,2009.

13. V. Bellotti and A. Sellen, Design for privacy in ubiquitous computing environments, In Proceedings of the 3rd European Conference on Computer Supported Cooperative Work, (ECSCW 93), G. de Michelis, C. Simone and K. Schmidt, eds, Kluwer, 1993.

14. G. Demiris, O. D. Parker, J. Giger, M. Skubic, and M. Rantz, Olderadults' privacy considerations for vision based recognition methods ofeldercare applications, Technology and Health Care, vol. 17, 2009.

15. G. Lugano, Understanding Mobile Relationships, In Human-Centered Technology Workshop, 2006.

16. Flora S. Tsai, Wenchou Han. JunweiXu, and Hock Chuan. Chua, Design and development of a mobile peer-to-peer social networking application, In Expert Syst, 2009.

17. A. Tomlinson, P. Yau, and J. A. MacDonald, Privacy threats ina mobile enterprise social network, Information Security TechnicalReport, vol. 15, no. 2, 2010.

18. L. Barkhuus, B. Brown, M. Bell, M. Hall, S. Sherwood, M. Chalmers, From awareness to repartee: sharing location within social groups, In: CHI 2008, pp. 497–506.Barnes, S.B., 2006. A privacy paradox: social networking in the United States. 2008.

19. R. Ajami, N. Ramadan, N. Mohamed, and J. Al-Jaroodi, Security Challenges and Approaches in OnlineSocial Networks: A Survey, IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.8, August 2011