A Semantic Model for Friend Segregation in Online Social Networks

Javed Ahmed[1,2(✉)]

[1] CIRSFID, University of Bologna, Bologna, Italy
[2] CSC, University of Luxembourg, Luxembourg City, Luxembourg
shahanijaved@gmail.com

Abstract. Online Social Networks exhibit many of the characteristics of human societies in terms of forming relationships and sharing personal information. However, the major online social networks lack an effective mechanism to represent diverse social relationships of the users. This leads to undesirable consequences of disclosing personal information of the users with unintended audiences. We propose a semantic model for friend segregation in online social networks. The relationship strength and social context of the users play vital role in friend segregation. The model infers relationship strength and social context from interaction pattern and profile similarity attributes of the users. We also conducted a research study with online social networks users. The study gives insight on user's information sharing behaviour and interaction pattern in online social networks. The findings reveal that personal information disclosure depends on relationship strength among the users.

Keywords: Online social networks · Privacy · Self presentation · Tie strength · Audience segregation

1 Introduction

Online social networks (OSNs) experienced exponential growth and attracted vast majority of the Internet users in recent years. OSNs offer the Internet users new and interesting means to communicate, interact and socialize with their family and friends. The users spend an unprecedented amount of time using online social networks and upload large quantities of personal information. In online social networks the uploader of the data must decide which of his friends should be able to access the data. This resulted in fundamental shift in status of an end user. An individual end-user becomes content manager instead of just being content consumer. The responsibility of managing appropriate privacy settings for every single piece of data shared on OSNs put a cognitive burden on the user and hence most of the users end up using default privacy settings. The

J. Ahmed—Author is doctoral candidate in Erasmus Mundus Joint International Doctoral (Ph.D.) program in Law, Science and Technology. Professor Leendert van der Torre, Guido Governatori, and Serena Villata supervise the author.

A. Bozzon et al. (Eds.): ICWE 2016, LNCS 9671, pp. 495–500, 2016.
DOI: 10.1007/978-3-319-38791-8_36

default privacy settings are very permissive in nature and lead to undesirable consequences of user's personal information disclosure with unintended audience and this poses serious privacy threat to the end-users. It is main reason privacy has received significant attention in the research community.

The current online social networks provide multitude of privacy settings to manage access to uploaded content. However, privacy-setting interface is too complicated to most of the normal users. The current interface has limited visual feedback, and promotes a poor mental model of how the settings affect the profile visibility [1]. Even after modifying settings, users can experience difficulty in ensuring that their settings match the actual desired outcome. Madejski [2] shows that privacy settings for uploaded content are often incorrect, failing to match user's expectations. Some of the online social networks provide features of lists and circles. These mechanisms help users in partitioning their contacts and then use these partitions to selectively share their content with an appropriate audience according to their preferences. The relationships in real life evolve with time and these features do not offer any mechanism to the user to deal with this evolution. The responsibility of maintaining the appropriateness of these lists lies solely on the user. As a result, it is unsurprising that many users do not use these features. We conclude that there is disparity between desired and actual privacy controls. The main reason for this disparity is social aspects of privacy that are ignored by existing technical solutions.

2 Problem Statement

Despite of the multitude of privacy controls, current online social networks fail to provide an effective mechanism to manage access to uploaded content of the users [2]. The main reason for this failure is shortcoming of the online social networks to represent diverse social relationships. Online social networks carry problematic assumptions in their implicit design of representing social relationships. All friends are created equal that means they have access to same identity, and same social context of the user. In real life people play diverse roles and disclose their personal information according to the role. Each individual has several role-based identities to preserve the contextual integrity of the information, which is being disclosed. The notion of privacy as contextual integrity is compromised by online social networks. For example, one may self-present in significantly different ways when in a business meeting versus when on a date. OSNs place employers and romantic partners on the same communication plane, make it more difficult for users to segment audiences and present varied versions of the self. Difficulty in disclosing information selectively to various life facets can lead to "context collapse" [3]. The collapsing of social contexts has emerged as an important problem with the rise of online social networks.

Most online social networks employ "friendship" as the only type of bidirectional relationship. The friendship is binary, static, and symmetric relationship of equal value between all the directly connected users, which provide only a coarse indication of the nature of the relationship. In reality social relationships are of

varying tie strength (how close two individual are to one another), dynamic (change over time), and asymmetric in nature (one person pays attention to another, it does not mean the latter will reciprocate). It is challenging task to model dynamism, asymmetry, and relational strength in user relationships in contemporary online social networks. This is the motivation for our research work.

The main question for this research is how to represent diverse social relationships of the users in online social networks. More specifically, we want to explore whether a user's interaction pattern with his friends can be used as a basis for inferring relationship strength among users. We also examine link between profile similarity attributes and relationship context of the users. The strength and context of relationship are key factors to perform friend segregation. Friend segregation can play vital role to control personal information disclosure in online social networks. We break main research question into sub questions:

1. How interaction pattern and profile similarity attributes reveals strength and context of relationship among OSNs users?
2. How to develop a semantic model for friend segregation depending on strength and context of relationship among OSNs users?
3. How to evaluate the model for friend segregation in online social networks?

In human societies, the strength and context of relationship are crucial factors for individuals while deciding the boundaries of their privacy. We conducted a research study with OSNs users to examine their attitude towards online privacy and relationship forming. The main contributions of this research work are given below:

1. We conducted a user study to examine information sharing and relationship forming behaviour of OSNs users.
2. We developed a model for friend segregation in online social networks.
3. The evaluation of the model using set of predefined criteria and requirements.

3 Methodology

The methodology employed in this work is combination of mixed methods approach such as reviewing scientific literature to redefine privacy that suits needs of social web users, conducting a user study to establish link between interaction pattern and relationship strength among OSNs users, and iterative development of a semantic model for friend segregation in online social networks. The complicated nature of the problem is rationale for choosing such a methodology. In the first phase, we redefine privacy from social and technical perspective. This privacy definition is inspired from work of Pfitzmann et al. [4]. We customized this concept to suit needs of online social networks. This privacy definition includes three aspects that are contextual integrity, disclosure minimization and user control. The contextual integrity gives users ability to keep audiences separate and to compartmentalize their social life [5]. The notion of privacy as contextual

integrity can be useful in addressing the problem of context collapse. The relationship strength plays vital role in disclosure minimization. Granovetter coined the term tie strength [6]. Tie strength is a quantifiable social network concept that measures the quality of relationships. Current online social networks provide simple access control mechanisms allowing users to govern access to information contained in their own spaces. Unfortunately, users have no control over data residing outside their spaces. Irwin Altman addresses this problem by enhancing user control to deal with both individual and collaborative boundary regulation [7]. We conducted a user study in the second phase to identify relationship between personal information disclosure and tie strength. The research survey was designed to examine interaction patterns of user with their diverse friend network in OSNs. The 323 participants took part in the study out of which 245 are males and 81 females, which leads to male bias. The results of survey are presented in following section. Finally, we developed a semantic model for friend segregation in online social networks. The model takes into consideration the three aspects of privacy described above.

4 Results

In this section, initially we present results of user study. According to the results 65 % of the participants added more than 200 people in their friend network, and 26 % of the participants reveal that they also added strangers to their friend network. Whereas, only 3 % of the participants are interested to share their personal information with strangers added in their friend network. The results show that vast majority of participants interact with friends and family on daily basis, and their interaction with colleagues and classmates is on weekly basis, whereas their interaction pattern with acquaintances and stranger is rarely or never. The preferred interaction type with strong ties is messaging, posting, commenting, and chatting. The participant's preferred interaction type with weak ties is either liking or not applicable. The most frequently used interaction types are messaging, liking, chatting, wishing, and posting, whereas, the least frequently used interaction types playing games and tagging. The results reveal that personal information disclosure depends on relationship strength among the users; the frequency of interaction is higher among the users with strong relational ties as compared to users with weak relational ties. The results also demonstrate that choice of interaction type for communication depends on relationship strength among the users.

An ontological model is developed using OWL as our modeling language. The ontology design methodology used is Methontology. The pool of competency questions is developed in the specification phase. In conceptualization phase, we identified entities and their relationships from competency questions. The model integrates some concepts from FOAF and PRO ontologies. The implementation of the model is done using Protege. Apart from checking consistency using various reasoners, the evaluation of the model is performed at assertional level by translating competency question into SPARQL queries and retrieving data. Figure 1 presents detail diagram of the model.

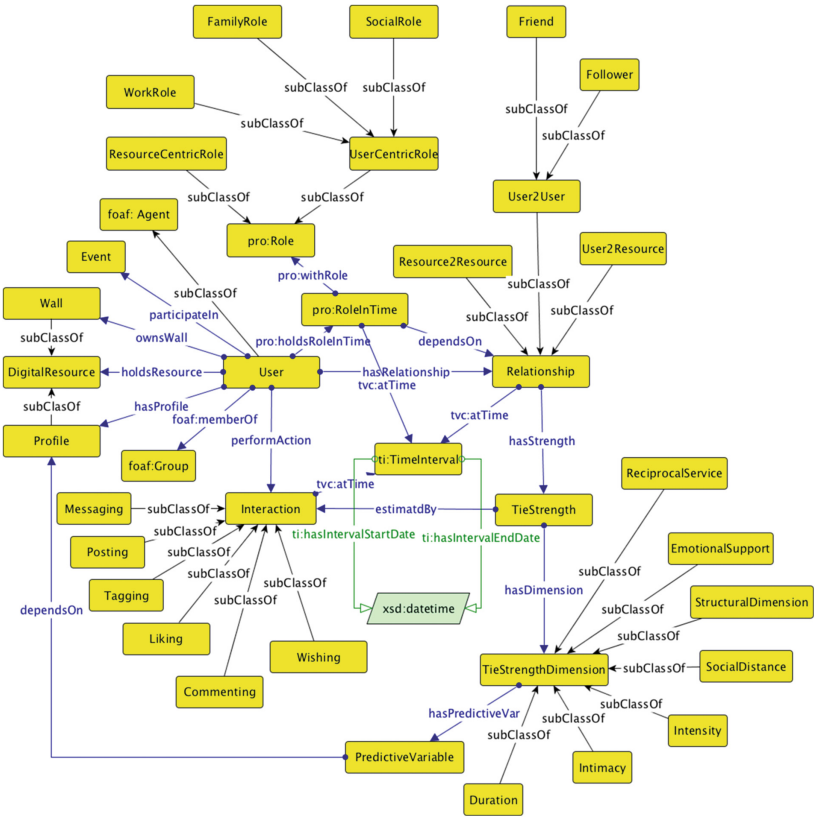

Fig. 1. Model for friend segregation

5 Related Work

The area of ontology based online social networks modeling is still in its early stages. One of the early solutions was proposed by Carminati et al. [8]. The authors propose online social network model based on semantic web technologies. The model considers the following five important elements of an online social network: (i) profiles, (ii) types of relationships among users (iii) resources, (iv) relationships between users and resources and (v) actions. The use of semantic web technologies allows the model to infer about the relationships among users and resources. Although the authors outline an access control framework, lack of formal descriptions and implementation leaves behind many ambiguities. A similar work is done by Masoumzadeh and Joshi [9,10], the authors propose ontology based access control model for online social networks. This model takes into account intricate semantic relationships among different users, data objects, and between users and data objects. The model enables expressing much more fine-grained access control policies on a social network knowledge base than

already discussed by Carminati et al. Both approaches don't take into consideration social context and relationship strength among users. The novelty of our approach is social perspective of privacy that ignored by these approaches.

6 Conclusion and Future Work

We presented a semantic model for friend segregation in online social networks. The model addresses three main issues faced by contemporary online social networks. First, the issue of context collapse is addressed by preserving contextual integrity of the user. Second, the issue of personal information disclosure to unintended audiences is addressed by disclosure minimization on the basis relationship quality. Finally, the issue of interdependent privacy is addressed by collaborative interpersonal privacy management. The model is inspired from work of well-known sociologists such as Goffman, Irwin Altman, and Granovetter. The model takes into consideration social aspects of privacy that are ignored by existing solutions to larger extent. The model is first step towards developing privacy friendly online social networks. In future, we plan to develop a third party social application for online social networks as a proof of concepts prototype to demonstrate the applicability of our model.

References

1. Akcora, C.G., Ferrari, E.: Graphical user interfaces for privacy settings. In: Alhajj, R., Rokne, J. (eds.) Encyclopedia of Social Network Analysis and Mining, pp. 648–660. Springer, New York (2014)
2. Madejski, M., Johnson, M.L, Bellovin, S.M.: The failure of online social network privacy settings, Department of Computer Science, Columbia University, Technical report CUCS-010-11, February 2011. http://mice.cs.columbia.edu/getTechreport.php?techreportID=1459
3. Vitak, J.: The impact of context collapse and privacy on social network site disclosures. J. Broadcast. Electron. Media **56**(4), 451–470 (2012)
4. Borcea-Pfitzmann, K., Pfitzmann, A., Berg, M.: Privacy 3.0: = data minimization+ user control+ contextual integrity. IT-Information Technology Methoden und Innovative Anwendungen der Informatik und Informationstechnik **53**(1), 34–40 (2011)
5. Goffman, E.: The presentation of self in everyday life. In: Contemporary Sociological Theory, pp. 46–61 (2012)
6. Granovetter, M.S.: The strength of weak ties. Am. J. Sociol. **78**(6), 1360–1380 (1973)
7. Altman, I.: The Environment, Social Behavior: Privacy, Personal Space, Territory, and Crowding. Brooks/Cole, Monterey (1975)
8. Carminati, B., Ferrari, E., Heatherly, R., Kantarcioglu, M., Thuraisingham, B.: Semantic web-based social network access control. Comput. Secur. **30**(2), 108–115 (2011)
9. Masoumzadeh, A., Joshi, J.: OSNAC: an ontology-based access control model for social networking systems. In: IEEE Second International Conference on Social Computing (SocialCom), pp. 751–759. IEEE (2010)
10. Masoumzadeh, A., Joshi, J.: Ontology-based access control for social network systems. Int. J. Inf. Priv. Secur. Integrity **1**(1), 59–78 (2011)