# Social Interaction Based Audience Segregation for Online Social Networks

Javed Ahmed[1], Guido Governatori[2], Leendart van der Torre[3] and Serena Villata[4]

[1] CIRSFID, University of Bologna, Italy
[2] NICTA QRL Brisbane, Australia
[3] University of Luxembourg, Luxembourg
[4] INRIA Sophia Antipolis, France

**Abstract.** Online social networking is the latest craze that has captured the attention of masses, people use these sites to communicate with their friends and family. These sites offer attractive means of social interactions and communications, but also raise privacy concerns. This paper examines user's abilities to control access to their personal information posted in online social networks. Online social networks lack common mechanism used by individuals in their real life to manage their privacy. The lack of such mechanism significantly affects the level of user control over their self presentation in online social networks. In this paper, we present social interaction based audience segregation model for online social networks. This model mimics real life interaction patterns and makes online social networks more privacy friendly. Our model uses type, frequency, and initiation factor of social interactions to calculate friendship strength. The main contribution of the model is that it considers set of all possible interactions among friends and assigns a numerical weight to each type of interaction in order to increase or decrease its contribution in calculation of friendship strength based on its importance in the development of relationship ties.

## 1 Introduction

Online social networks (OSNs) have experienced exponential growth in recent years. OSNs are the top most visited sites on the Internet.[5] According to Nielsen,[6] OSNs are the fourth most popular activity on the Internet nowadays. The key breakthrough brought by OSNs is that these sites promote the vision of a human-centric web, where network of people and their interests become the primary source of information, which resides entirely on social networking services [1]. Online social networks are one of the most popular fora for self representation and user interactions. Individuals join social networks to present themselves. In OSNs users can present themselves by constructing a profile. A profile is a digital

[5] Alexa http:/www.alexa.com/topsites
[6] Nielsen http://www.nielsen.com/

representation of an OSN user. A Profile contains huge amount of personal information about the user. Additionally, these users are engaged in various social interactions with other users. All these activities are recorded on these platforms which can be easily analyzed, manipulated, systematized, formalized, classified, and aggregated [2]. This poses a serious privacy threat to OSN users, and that is the main reason privacy is hotly debated topic in research literature [3] [4] [5] [6] [7] [8]. There are several dimensions of privacy threats in online social networks such as privacy threats related to OSNs users[9], third party applications [10], and OSN service providers [5]. In this paper, we are addressing the issue of privacy threats related to OSN users.

Tremendous growth of online social networks resulted in fundamental shift in status of end users. Individual end users become content managers instead of just being content consumers. Today, for every single piece of data shared on OSNs, the uploader must decide which of his friends should be able to access the data. In OSNs, term "friend" has become all-encompassing, it has become increasingly difficult for users to control which friends get to see what personal information. Several studies on Facebook usage have shown that the average number of friends per user is approximately 150. Anyone can make a request to join a user's friend circle–family members, colleagues, classmates, acquaintances, strangers etc. Current literature support the claim that users are willing to add strangers to their friend circle [9]. However, allowing strangers to join user's friend circle can lead to a number of privacy risks [11]. Most of the OSNs provide users with binary relational ties (e.g., friends or stranger) [12]. This binary indicator provides only a coarse indication of the nature of the relationship. In reality human relationships are much more complicated than a single binary relational tie. There is need for segregation of friends according to the strength of relational ties. Some of the social networking sites have begun providing friend-lists feature, in order to help users in organizing a large friend network into groups. Grouping several hundred friends into different lists, however, can be a laborious process; on what basis should users construct the friend-lists? And even if the user were to group friends into lists, are these lists meaningful for setting privacy policies? To alleviate the burden of constructing meaningful lists manually, we propose interaction based audience segregation model for online social networks. The estimation of friendship interaction intensity among OSN users and its classification based on different level of intensity can be quite useful for identifying privacy threat from individuals added as friends. The social web is kind of virtual society that exhibits many of the characteristics of real societies in term of forming relationships and how those relationships are utilized. In real societies, the relationship strength is a crucial factor for individuals while deciding the boundaries of their privacy. Moreover, this subjective feeling is quite efficiently utilized by humans to decide various other privacy related aspects such as what to reveal and whom to reveal.

The main question for this research is how interactions of users determine tie strength and implement privacy in online social networks. More specifically, we want to explore whether a users interaction with his friends can be used as

a basis for making data access decision for that users. To answer this question, we need to understand nature of privacy in online social networks and dynamics of interactions intensity for OSN users. We break main research question into three sub questions:

- How to measure privacy risk associated with social graph of OSN users?
- How to construct interaction graph by quantifying users interactions in OSN?
- How to segregate audience on the basis of interaction graph in OSN?

First research question help to quantify the privacy risk attributed to friend relationship in online social networks. We show that risky friends can reveal user personal information unintentionally in online social networks. For example, Javed and Serena are friends in online social network. Serena is very careful about the privacy. She adopts a policy that conceals all her friends from public. On the other hand, Javed, adopts a weaker policy that allows any users to view his friends. In this case, Serena's relationship with Javed can still be learned through Javed. We say that privacy conflict occurs as Serena's restrictive policy is violated by Javed's weaker privacy policy. This shows that the user can only control one direction of a an inherently bidirectional relationship. Second research question deals with user's interaction patterns in online social networks. We show that users tend to interact mostly with small subset of friends, often having no interactions with majority of their friends in online social networks. This cast doubts on the practice of extracting meaningful relationships from social graphs. We suggest interaction based model for validating user relationships in online social networks. Third research question deals with audience segregation. We consider social interactions as currency to estimate friendship strength and perform audience segregation. Providing users with audience segregation mechanism would improve the quality of interactions and self presentations. Rest of the paper is organized as follows. In section 2, we present characterization of privacy in OSNs. Impact analysis of various social interactions is presented in section 3. We discuss interaction based audience segregation and present model to compute the interaction intensity in section 4. Section 5 discuss the related literature. Finally, we conclude the paper with future research direction.

## 2 Privacy in Online Social Networks

With emergence of the Web 2.0, a new debate started about the meaning and value of privacy. According to some researchers privacy has been undermined by online social networks, even some of them claim that it no longer exist.[7] The concept of privacy is so intricate that there is no universal definition of it. One of the oldest definitions of privacy is "the right to be let alone". Warren and Brandeis were one of the first authors who recognize the multidimensionality of privacy concept [13]. Privacy on the web in general revolves mostly around

[7] Do Social Networks Brings the End of Privacy? http://www.scientificamerican.com/article/do-social-networks-bring/

information privacy. The information privacy is an individual's claim to control the terms under which personal information is acquired, disclosed or used [14]. With emergence of the social web, where users collaborate and share personal information, we need to define privacy in fine grained manner to address existing issues from multiparty perspectives. The definition of privacy should be able to address the privacy concerns related to OSN users, third party applications, and OSN service providers.

Palen et al. [15] defined privacy in very precise manner. This definition gives some idea of various realms in which privacy issue may occur. The authors classify three boundaries of privacy with which OSNs users are struggling.

**Disclosure Boundary** It deals with managing private and public scope of uploaded information.

**Identity Boundary** It deals with managing self representation with specific audience.

**Temporal Boundary** It deals with managing past actions with future expectations; user behavior may change over time.

The users have a scope in mind when they upload personal information in online social networks. This scope is defined by disclosure, identity, and temporal boundaries. The privacy is breached when information is moved beyond its intended scope either accidentally or maliciously. Simply a breach can occur when information is shared with a party for whom it was not intended, it can also happen when information is abused for different purpose than was intended, or when information is accessed after its intended lifetime.

Another very comprehensive concept of privacy is given by Patil et al. [16]. The authors present legal, social and technical perspectives from which the notion of privacy is commonly described and analyzed.

**Normative** from this perspective, privacy is an ethical concept. Privacy is viewed as right of individual and thus as a matter of freedom.

**Social** from this perspective, privacy has psychological and culture roots. Privacy is socially constructed based on the behavior and interactions of individuals as they conduct their day-to-day affairs.

**Technical** the technical perspective views privacy in terms of the functional characteristics of digital systems. Privacy is thus treated as the desire for selective and adequate control over data and information.

Note that three perspectives of privacy are not mutually exclusive but interdependent. Normative focuses on laws and policies aiming to protect the individual from cooperations, governments and other individuals. European data protection framework is an example which promotes informational self determination emphasizing an individual's right to control the collection and use of personal data. Technical dimension of privacy aims at translating norms and regulations into technical specifications. The Platform for Privacy Preferences Project (P3P) is one of the examples for enhancing the individual's ability to control information disclosure by technical means. Social dimension of privacy focuses on managing

social relationships and boundaries between public and private life. Privacy is breached if personal information is available outside its intended context.

Netter et al. [17] breaks the concept of privacy into a set of characteristics that aim at analyzing the OSN privacy from multiparty perspectives. The privacy risks associated with online social networks are mainly from OSNs users, third party applications, or OSNs service providers. Each characteristic address privacy risk related to one of these stakeholders.

**Audience Segregation** This characteristic describes that each individual performs multiple and possibly conflicting roles in everyday life and it needs to segregate the audience for each role, in way that people from one audience cannot witness a role performance that is intended for another audience. In current online social networks almost all friends are treated equally, As a result, privacy is threatened because a large audience might have access to personal information. This characteristic deals mainly with social web users.

**Data Sovereignty** It describes to what extent an individual is able to control the processing of its personal data. In case of online social networks personal data is available in structured manner. It can easily be copied, linked, aggregated, and transferred. This characteristic deals mainly with OSNs service providers and third party applications.

**Data Transience** This characteristic revolves around the loss of personal information over time. In computer mediated communication permanency of personal information poses great challenge to privacy, whereas data transience can be considered as typical characteristic of real world communication. This characteristic deals mainly with OSNs service providers and third party applications.

**Protection against profiling** It describes an individual's ability to prevent an adversary from collecting, aggregating and link personal data in order to create a digital dossier. The current landscape of online social networks poses this threat at large scale. This characteristic deals with OSNs service providers and third party applications.

**Privacy Awareness** It describes that an individual's awareness for privacy risks is a prerequisite for privacy preserving behavior. The characteristic deals with all stakeholders at social level.

**Transparency** It describes transparency of processing and dissemination practices. This characteristic deals mainly with OSNs service providers and third party applications.

**Enforcement** It describes an individual's means to bring privacy preference into force. This characteristic deals with OSNs service providers at legal level.

This paper focuses only on audience segregation characteristic to preserve three boundaries of privacy defined by Palen et al. The audience segregation is main characteristic that deals with OSNs users. A comprehensive solution to address the privacy risks associated with OSNs users can not be developed without taking into consideration importance of audience segregation. We consider social interactions as currency to estimate friendship strength and perform audience

segregation. In this paper, we develop a mathematical model for this purpose. The issues related to third party applications and OSNs service providers are not in the scope of this paper.

## 3 Social Interactions in Online Social Networks

Online social networks are popular for interaction, communication and collaboration between friends. The properties of social interactions have been studied by many researchers. Facebook data team recently showed that a typical Facebook user communicates with a small subset of their entire friends network, but maintains relationships with a group that is two times larger.[8] Wilson et al.[18] propose the interaction graph, a model for representing user relationships based on user interactions. The authors show that interaction activity on Facebook is significantly skewed towards a small portion of each user's social links. This finding casts doubt on the assumption that all social links imply equally meaningful friend relationships. Burke et al.[19] study the role of user interactions on Facebook. The authors quantify usage of visible actions (such as wall posts and comments) and also silent actions (such as profile visits). They show that, different from high levels of content consumption, high levels of direct communication among users is usually associated with greater feelings of emotional support from close friends. Jiang et al. [20] show that latent (or silent) interactions are much more prevalent and frequent than visible interactions. Gao et al. [21] attempt to characterize and detect malicious forms of interactions in online social networks.

In this section our main goal is to identify impact of various types of interactions provided by online social networks. OSNs provide a variety of social interactions. These interactions can play important role to estimate friend strength. There are several interaction factors that can be considered to identify their impact in developing relationship ties. These factors include type of interaction, frequency of interaction, and initiation of interaction. The type of interaction is quite important factor in order to estimate friendship strength. Online social networks provide numerous types of interactions such as messages, wall posting, comments, tagging, chatting etc, some of these interactions are real time and the others are non-real time. An individual chooses an interaction type on basis of relationship with target audience. Hence, the interaction type defines the intimacy, openness, sensitivity as well as strength of relationship between communicating parties. The interaction frequency refers to total occurrences of each type of interaction between an individual and his friends within certain period of time. This factor helps to understand that users are willing to interact with each other over a period of time. The interaction initiation factor is very important to understand strength of relationship. We further categorize this aspect in following manner.

**User Initiated Interactions** When the user initiate interaction with his friend it is termed as user initiated interactions. These interactions have more

[8] Maintained Relationships on Facebook http://overstated.net/2009/03/09/maintained-relationships-on-facebook

weight in developing relationship strength because the user is willing to communicate and collaborate with his friend.

**Friend Initiated Interactions** When an individual friend initiate interaction with the user it is termed as friend initiated interactions. These interactions have less weight in developing relationship strength because willingness of communication and collaboration is coming from the friend.

As discussed earlier, the selection of interaction type gives an indication of nature of relationship among users. Some the interaction types are preferred to communicate with close friends, whereas the others to interact with ordinary friends. Hence, all interaction types cannot be given similar weight in estimation of relationship strength. Each interaction type is given a numerical weight in order to increase or decrease its contribution in development relationship strength. We consider social interaction as a very strong indicator for friend segregation. Our model uses type, frequency, and interaction initiation factor to calculate interaction intensity that can be useful in audience segregation. The term audience segregation is explained in following section before presentation of our audience segregation model.

## 4 Audience Segregation in Online Social Networks

Social web users privacy issues can be addressed by providing users with tools that help them manage their personal content in more privacy friendly manner. In everyday life individuals have control over what kind of information is presented to different audiences. Mirroring or mimicking this real life strategy, we propose interaction based audience segregation model for online social networks. The term "audience segregation" was coined by Goffman [22] as part of a perspective on the ways in which identities are constructed and expressed in interactions between human beings in everyday context. According to Goffman, whenever individuals engage in interactions with others they perform roles, with which they hope to present a favorable image of themselves. One of the key elements of Goffman's perspective on identity is the fact that individuals attempt to present self-images that both are consistent and coherent. To accomplish this, performers engage in audience segregation. While Goffman's idea of audience segregation didn't originally relate directly to privacy, it is easy to see that audience segregation and privacy are, in fact, closely linked. Another quite similar conclusion is drawn by Nissenbaum [23] that is privacy revolves around contextual integrity. According to this view privacy revolves around person's ability to keep audience separate and to compartmentalize his social life.

Current online social networks don't provide users fine grained mechanism to separate and manage various audiences. Many social networks sites only provide their users the option to collect one list of contacts, called "friends". Some of the social networks offer functionality of creating separate lists which require user's time and efforts. Studies show that managing different lists is a burden to many users and rarely applied [24]. Given the fact that Facebook users, for instance, on average have 150 friends, this necessarily conflates different contexts.

Providing OSN users a mechanism which mimic real life interaction patterns to larger extent would improve self presentation, and reduce privacy risks. It will also enable users to avoid social convergence, and provide users opportunity to present different sides of themselves to different audiences.

### 4.1 Social Interaction Based Audience Segregation Model

In online social networks individuals are connected with diverse audience such as friends, family members, distant relatives, colleagues, old schoolmate etc. Some of them are intimately known to user, whereas others are distant, loose, or even unknown connections. This is main reason users want to make distinctions between the types of information they want to share with these different categories of connections, and give different connections access to different content. Social interaction based audience segregation can play vital role to achieve this objective.

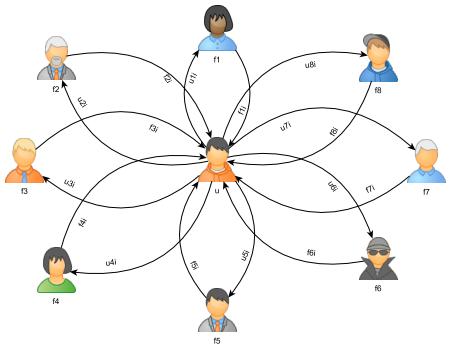


**Fig. 1.** An individual user's social cirlce in online social network

Social interaction based audience segregation model considers an individual user $u$ has $n$ number of friends, $f_1, f_2, f_3, \cdots, f_n$. The user and his friends can interact with each other by $k$ type of different interactions $[t_1, t_2, \cdots, t_k]$, either initiated by user or his/her friend. Each type of interaction $t_i$ is assigned a weight $w'_i$ on the basis of its importance in developing friendship strength. Following vector $w'$ represents the weights of all interactions:

$$w' = [w'_1, w'_2, w'_3, ..., w'_k]$$

and $w'$ is normalized as:

$$w = \frac{1}{K}[w'_1, w'_2, w'_3, ..., w'_k]$$

where $K = \sum_{i=0}^{k} w'_i$.

The frequency of all $k$ type interactions is also considered separately for user initiated and friend initiated interactions on basis of their repeated occurrences in communication. Let $a_i$ be the frequency of interaction $t_i$ and let $F_{u,j}$ be the vector representing the frequency of all $k$ type of interactions initiated by the user $u$ to user $j$ given as:

$$F_{u,j} = [a_1, a_2, a_3, ..., a_k]$$

where $1 \leq j \leq n$. Similarly, $F_{j,u}$ represents the frequency of all type of interactions between user $u$ and $j$ initiated by $j$. The interaction intensity is calculated by multiplication of each type of interactions frequency $a_i$ by its respective weight $w_i$ and accumulation of all such interaction types separately for user initiated interactions and friend initiated interactions. That is the interaction intensity of user $u$ with his friend $j$ is computed as:

$$I_{(u,j)} = \sum_{i=0}^{k} F_{u,j}(i) * w_i \tag{1}$$

where $F_{u,j}(i)$ is the interaction frequency of interaction type $t_i$ and $w_i$ is normalized weight as described above. Similarly, interaction intensity $I(j,u)$ of user $j$ with $u$ is computed.

$$I_{(j,u)} = \sum_{i=0}^{k} F_{j,u}(i) * w_i \tag{2}$$

Finally, user and friend initiated interactions are multiplied by their respective weights and accumulated to generate interaction intensity value of user $u$ with his friend $j$

$$T_j = \alpha * I_{(u,j)} + (1 - \alpha) * I_{(j,u)} \tag{3}$$

Where $0 \leq \alpha \leq 1$ and $\alpha, 1 - \alpha$ are respective weight for user and friend initiated interactions.

There are three main contributions of this model. First, it considers all possible of set interactions among friends. Secondly, the model considers the direction of interaction either from user to friend or vice versa. Finally, it assigns numerical weight to all interaction types based on their importance in the development of friendship strength.

## 5 Related Literature

One of the research studies closely related to our work is done by Lerone et al. [25]. The author has introduced interaction count based approach to determine relationship strength. The author simply takes into consideration three types of interactions and count them in order to calculate relationship strength. The interaction intensity model by Lerone et al. [25] do not differentiate interactions on the basis of initiative. Hence, it is possible that a malicious user intentionally spam interactions to get access to sensitive profile data. Our model takes into

consideration this issue and resolves it by assign more weight to interactions initiated by user himself. Our model has another advantage over [25] that it considers all interaction types offered by online social networks.

Waqar et al. [26] extended work of [25] by applying data mining model to calculate relationship strength, Whereas, the model is not validated on real OSNs data. The author also conducted online survey to analyze Facebook user's interaction behavior with their friends. Xiang et al. [12] proposed a model to infer relationship strength based on profile similarity and interaction activity. Lizi et al. [27] proposed interaction ranking based trustworthy friend recommendation model. Another interesting work by the author [28] proposed trust ranking based recommendation model for suggesting the most trustworthy community members. The author investigated four new interaction attributes that influence trust in virtual communities. A recent work related to friend recommendation is done by Zhao et al.[29]. The author proposed scalable and explainable friend recommendation model for social network systems.

The majority of online social networks offer second degree access which means a friend of a friend is able to access the user's personal information. According to Cuneyt et al. [11] friends can be source of privacy risk because this relationship always implies the release of some personal information not only to friends, but also to friends of a friend, which are strangers for the users. Another interesting fact demonstrated by Frank et al. [30] that more users are willing to divulge personal details to an adversary if there is a mutual friend connected to the adversary and the user. Christo et al. [18] shows that users tend to interact mostly with small subset of friends, often having no interactions with up to 50 percent of their friends. The author suggests a model for representing user relationships based on user interactions. These works supports our idea that all friends should not be give equal access to user personal information, but access to personal information should be administrated based on interaction frequency among users.

## 6 Conclusion and Future Work

In this paper, We proposed social interaction based audience segregation model which mimic real life interaction patterns to larger extent. We also identified the impact of various social interactions available to users in online social networks. There are three main contributions of our model. First of all, it consider all possible of set interactions among friends. Secondly, the model considers the direction of interaction either from user to friend or vice versa. Finally, all interaction types are assigned a numerical weight in order to increase or decrease its contribution in interaction intensity calculation based on its importance in the development of relationship ties. Our future plans include implementation of this model.

## References


1. George Pallis, Demetrios Zeinalipour-Yazti, and Marios D Dikaiakos. Online social networks: status and trends. In *New Directions in Web Data Management 1*, pages 213–234. Springer, 2011.
2. Bibi van den Berg, Stefanie Pötzsch, Ronald Leenes, Katrin Borcea-Pfitzmann, and Filipe Beato. Privacy in social software. In *Privacy and Identity Management for Life*, pages 33–60. Springer, 2011.
3. Justin Lee Becker and Hao Chen. *Measuring privacy risk in online social networks*. PhD thesis, University of California, Davis, 2009.
4. Catherine Dwyer, Starr Roxanne Hiltz, and Katia Passerini. Trust and privacy concern within social networking sites: A comparison of facebook and myspace. In *AMCIS*, page 339, 2007.
5. Ai Ho, Abdou Maiga, and Esma Aïmeur. Privacy protection issues in social networking sites. In *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on*, pages 271–278. IEEE, 2009.
6. Giles Hogben. Security issues and recommendations for online social networks. *ENISA position paper*, 2007.
7. Balachander Krishnamurthy and Craig E Wills. Characterizing privacy in online social networks. In *Proceedings of the first workshop on Online social networks*, pages 37–42. ACM, 2008.
8. Chi Zhang, Jinyuan Sun, Xiaoyan Zhu, and Yuguang Fang. Privacy and security for online social networks: challenges and opportunities. *Network, IEEE*, 24(4):13–18, 2010.
9. Ralph Gross and Alessandro Acquisti. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 71–80. ACM, 2005.
10. Javed Ahmed and Zubair Ahmed Shaikh. Privacy issues in social networking platforms: comparative study of facebook developers platform and opensocial. In *Computer Networks and Information Technology (ICCNIT), 2011 International Conference on*, pages 179–183. IEEE, 2011.
11. Cuneyt Gurcan Akcora, Barbara Carminati, and Elena Ferrari. Risks of friendships on social networks. *arXiv preprint arXiv:1210.3234*, 2012.
12. Rongjing Xiang, Jennifer Neville, and Monica Rogati. Modeling relationship strength in online social networks. In *Proceedings of the 19th international conference on World wide web*, pages 981–990. ACM, 2010.
13. Samuel D Warren and Louis D Brandeis. The right to privacy. *Harvard law review*, pages 193–220, 1890.
14. Jerry Kang. Information privacy in cyberspace transactions. *Stanford Law Review*, pages 1193–1294, 1998.
15. Leysia Palen and Paul Dourish. Unpacking privacy for a networked world. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 129–136. ACM, 2003.
16. Sameer Patil and Alfred Kobsa. Privacy considerations in awareness systems: designing with privacy in mind. In *Awareness Systems*, pages 187–206. Springer, 2009.
17. Michael Netter, Sebastian Herbst, and Günther Pernul. Analyzing privacy in social networks–an interdisciplinary approach. In *Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom)*, pages 1327–1334. IEEE, 2011.

18. Christo Wilson, Bryce Boe, Alessandra Sala, Krishna PN Puttaswamy, and Ben Y Zhao. User interactions in social networks and their implications. In *Proceedings of the 4th ACM European conference on Computer systems*, pages 205–218. Acm, 2009.
19. Moira Burke, Cameron Marlow, and Thomas Lento. Social network activity and social well-being. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1909–1912. ACM, 2010.
20. Jing Jiang, Christo Wilson, Xiao Wang, Wenpeng Sha, Peng Huang, Yafei Dai, and Ben Y Zhao. Understanding latent interactions in online social networks. *ACM Transactions on the Web (TWEB)*, 7(4):18, 2013.
21. Hongyu Gao, Jun Hu, Christo Wilson, Zhichun Li, Yan Chen, and Ben Y Zhao. Detecting and characterizing social spam campaigns. In *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, pages 35–47. ACM, 2010.
22. Erving Goffman. The presentation of self in everyday life. 1959.
23. Helen Nissenbaum. Privacy as contextual integrity. *Wash. L. Rev.*, 79:119, 2004.
24. Joan Morris DiMicco and David R Millen. Identity management: multiple presentations of self in facebook. In *Proceedings of the 2007 international ACM conference on Supporting group work*, pages 383–386. ACM, 2007.
25. Lerone Banks and Shyhtsun Felix Wu. All friends are not created equal: An interaction intensity based approach to privacy in online social networks. In *Computational Science and Engineering, 2009. CSE'09. International Conference on*, volume 4, pages 970–974. IEEE, 2009.
26. Waqar Ahmad, Asim Riaz, Henric Johnson, and Niklas Lavesson. Predicting friendship intensity in online social networks. In *21st International Tyrrhenian Workshop on Digital Communications*, 2010.
27. Lizi Zhang, Hui Fang, Wee Keong Ng, and Jie Zhang. Intrank: Interaction ranking-based trustworthy friend recommendation. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*, pages 266–273. IEEE, 2011.
28. Lizi Zhang, Cheun Pin Tan, Siyi Li, Hui Fang, Pramodh Rai, Yao Chen, Rohit Luthra, Wee Keong Ng, and Jie Zhang. The influence of interaction attributes on trust in virtual communities. In *Advances in User Modeling*, pages 268–279. Springer, 2012.
29. Zhao Du, Lantao Hu, Xiaolong Fu, and Yongqi Liu. Scalable and explainable friend recommendation in campus social network system. In *Frontier and Future Development of Information Technology in Medicine and Education*, pages 457–466. Springer, 2014.
30. Frank Nagle and Lisa Singh. Can friends be trusted? exploring privacy in online social networks. In *Social Network Analysis and Mining, 2009. ASONAM'09. International Conference on Advances in*, pages 312–315. IEEE, 2009.