Perceived and Realized Privacy of Online Social Networks

1 Abstract

With the fast development of Online Social Networks (OSN), privacy issue has become a great concern. Among all the research attempts of social network privacy, quantification of OSN user risks is an important attempt to deal with this problem. But how to quantify the privacy risks faced by OSN users is a challenging problem. Past work on this topic has been done by Justin et al.[1], Tran Hong et al. [2] and Kun et al. [3]. Kun et al. proposed a model to calculate the privacy score of OSN users. The model uses two intuitive metrics, sensitivity and visibility, as the factors for privacy score calculation. Inspired by the work done by Kun et al., we propose a model to quantify the privacy risks of OSN users, our model assume that OSN users intent to enjoy the benefits of OSNs, but on the other hand, the disclosure of personal information also brings risks to the social network users which are potentially hidden.

The social benefits is determined by the number of users who can view an item. The more viewer, the higher social benefit. On the other hand, the implied privacy risks by disclosing an item is determined by how sensitive the item is as well as the potential users. The networked environment of OSN determines the potential audiences of a profile item.

And we argue that the privacy risk is also based on the probability that a certain profile item is visited by another OSN user. We model this probability as a random walk process over all the potential social network users.

In summary, by integrating social benefits and potential risks, our model tells the relative privacy risks of social network users for specific profile setting.

2 Introduction

In recent years, online social network sites are becoming more and more popular, it provides people a virtual world for social relations and entertainments. Millions of people are providing their personal information to enjoy the benefits of these social sites. While, on the other hand, the risks of privacy breach through social network becomes and urgent and a more and more of public concern.

And several social network accidents also tells the truth of privacy risks of online social networks. Years ago, facebook's Beacon[4], which correlate users' shopping activities on other websites with their Facebook profiles, had to be closed because of the protests of users' personal privacy violation. Google buzz[5], a social networking, microblogging and messaging tool from Google integrated into Gmail, was sued because of compromising users' privacy by sharing their email contacts to maximize influence of this service. These and other similar social network privacy breach incidents have educated people to have more concern on the privacy of their private information, for example, they may ask[6], what benefits and risks can I have if I disclose my personal information on the social network? And people are unwilling to risk losing control of their personal information.

In this paper, we are making attempt to answer this particular question, to quantify the benefits and risks of engaging in social networks. Without loss of generality, we use Facebook as our main target for analysis. Similar models can be extend to other social networks.

We argue that the main driving force for people to join in a social network is the benefit provided by such networks, and the disclosure of personal sensitive information to social networks poses privacy risks which is negative from a user's point of view. We try to integrate these two together and define privacy as combination of positive social network benefits as well as negative social network privacy risks.

We define privacy as a probablistic problem , which considers user as in a network and privacy risks happens when the user is visited by another user. We call this model realized privacy.

It has been shown that users of social network state that they are worried about their privacy, but put at the same time detailed personal information on their profiles[7]. We are trying to explain this privacy paradox in this paper. On one hand, we consider we consider social network privacy as both positive and negative parts, which are two intuitive concerns of using social networks; and on the other hand, we consider the probablistically realized privacy, which puts user in a social network and privacy can be realized when another user visits him. We use real data extracted from facebook to fit our model.

Organization of the paper is as follows. Part II introduces related with of social network privacy. Part III defines notations of our social network privacy model. Part IV presents our model and part V presents our data and experimental results. And part VI concludes the paper by pointing out our future work and related issues.

3 Related Work

In recent years, research community has been trying hard to deal with privacy issues of online social networks, related topics include spamming and phishing [8, 9, 10, 11, 12], attack analysis [13, 14, 15, 16, 17, 18, 19] etc., which are also directly related to traditional web privacy and security. Fang et al. [20] proposes a classification model to help social network users automate the privacy related settings. Social network privacy control is also considered an access control problem. Carminati et al. [21, 22] propose client-based semi-decentralized access control model, access is granted based on the attestation of access authorization by the access requestor. Mohd et al. [23] proposes a reflective policy assessmenst method based on visualization to help user understand the implications of access control policies. Another research branch related to social network privacy is related to the social network platform, which targets privacy risks by third party application and social network providers. Adrienne et al. [24] addresses the privacy risks associated with social network APIs through proxy. Singh et al. [25] propose an information flow model to control what untrusted applications can do with the information they receive.

Attempts to quantify social network risks have also been tried. Justin et al. [1] propose a model to quantify privacy risks of a social network user by infering from his/her friends. Kun et al. [3] proposed a framework to estimate the privacy score for a social network user. They calculate the potential privacy risks by considering two factors, one is sensitivity, which is a measure of private level of an profile item and another is visibility, which measures how many people will view the profile item.

Our work is most related to the work done by Kun et al.. However, our work provides novel contribution to the research of this field. First, we consider the social network privacy as well as social network benefits. So, our privacy model composes of two controdicting concerns from the point view of social network users. And this considerations are pratical in reality. Second, we propose realized privacy, which considers the fact that privacy risk happens when another user visits this private information. And we make attempt to use real data from facebook to fit our model.

4 Modeling Social Network

We model social network as a graph $\mathcal{G}$, which consists of N nodes. Every node $u_i, 1 \leq i \leq N$ corresponds to a user in the social network. Nodes in graph $\mathcal{G}$ are connected through links, which correspondes to friendships in social networks. And for simplicity purposes, we consider friendships as a directed link denoted as $f_{ij} : u_i \rightarrow u_j, i, j \in \{1, 2, \ldots, N\}$.

In a social network, user u_i has N_i friends, and these friends form a micro-community denoted as $\mathcal{C}_F = \{u_j | \exists u_i \rightarrow u_j, 1 \leq j \leq N_i\}$, and friends of these friends form a even larger micro-community denoted as $\mathcal{C}_{FOF} = \{u_k | \exists u_i \rightarrow u_j \rightarrow u_k, 1 \leq j \leq N_i \text{ and } 1 \leq k \leq \sum_{m=1}^{N_i} N_m\}$, and the extreme larger community consists of all users in the given social network, and we denote it as $\mathcal{C}_{ALL} = \{u_i | u_i \in \mathcal{G}\}$. And for comparison, we also denote the smallest micro-community, the user him/her-self, for user u_i as $\mathcal{C}_{USER} = u_i$. The community is illustrated in Figure 1.

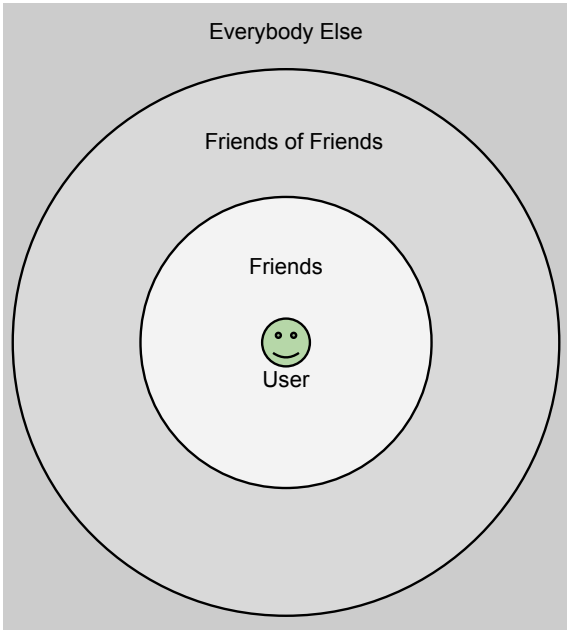

Figure 1: User Centric Social Network Communities.

Every node u_i in social network $\mathcal{G}$ has P_i number of features $F_i = \{f_{ij} | 1 \leq j \leq P_i\}$. These features, in social network, corresponds to the profile items of a user, e.g. name, date of birth, address, education etc., which are the identities of user u_i in the social network. Profile items are basic information for social interaction and can also be used by social network providers to provide personalized services such as friends recommendation, search and targetted advertising.

Usually, social networks require a minimum number of items upon registration, for example, sex, birthday etc.. And other optional items can be updated later. Because profile items are carriers of personal private information, social network sites provide configuration options for user to change their targetted audience for each item. For a user u_i, we denote the setting of social network profile item f_{ij} as s_{ij}. For example, Facebook provides settings that include only me, friends only, friends of friends and everybody from the most conservative to the most open. So for the case of facebook, we have $s_{ij} \in \{S_{me}, S_f, S_{fof}, S_{all}\}$. And we will use these levels of settings in our privacy model. Although Facebook also provide finer grained privacy setting by specifying specific users to view a certain profile item, in our model we ignore this situation and will leave it for future work. The meaning and corresponding audiences of each privacy settings are listed in Table 1.

Access Setting	**Audiences**
Only Me(S_{me})	$\mathcal{C}_{USER}$
Friends (S_f)	$\mathcal{C}_F$
Friends of Friends (S_{fof})	$\mathcal{C}_{FOF}$
Everybody (S_{all})	$\mathcal{C}_{ALL}$

Table 1: Profile Item Access Setting and Corresponding Audiences.

Online Social network is a complex system, and there are many factors that can cause privacy breach, for example, malicious users who aim to obtain your personal information for advertising etc. On the other hand, social interactions between friends also have many forms, one such obvious factor is the importance of friendship, which corresponds to the weight of links in our social graph model $\mathcal{G}$; another example is the weighted importance of social interactions, which are the way

how social benefits are realized in practice. In order to make the problem simple and manageable, we make the following assumption in our social network model, (a) all friends of user u_i which is in $\mathcal{C}_F$ have equal importance to user u_i; (b) user u_i has equal probability to visit his/her friends $\mathcal{C}_F$ and friends of friends $\mathcal{C}_{FOF}$.

5 The Social Network Privacy Model

5.1 Social Benefits

Definition 1. Benefits of social network is the positive gain by using social networks, such as keeping contact between friends.

5.2 A Review of Social Networks Risks

Risks of social network is about the potential privacy damage cause by using social networks. Such as the lost of private information e.g. SSN. Usually, malicious users use various social attacks to achieve this goal. In this section, we will review attacks of social networks.

Spammers and content polluters are threatening privacy of OSN users. Studies on the features of social spam and measures to effectively filter out these spams has been studied by Kyumin Lee et al. [26], Stringhini et al. [27], Gao, Hongyu et al. [28] and Huber, Markus et al. [9]. They find that the identified spam data contains contents that are strongly correlated with observable profile features. This finding tells us that spammers are trying to improve their spamming success rate by gleaning user profile information using various ways, and then do context based spamming. Once successful, users' OSN account can be compromised and more sensitive or even private information might be stolen.

Phishing is a form of social engineering in which attackers attempts to fraudulently acquire sensitive information by impersonating a trustworthy third party. Phishing messages with malicious URL links or attachments can be send to social network users. When users clicked the malicious URL or download/execute the attachment, malicious programs or websites, they can steal users' personal information or do harm to users' computer. Tom Jagatic et al. [29] studied phishing attacks by using the publicly available personal information from social networks. They find that the phishing attack was easy and effective with a success rate of 72%.

Identity Threft Attacks

Bilge, Leyla et al.[17] studied identity theft attacks. They proposed that existing users of OSN can be compromised, and their identity can be used to request friendship with other cloned victims. And they prove that this attack can be done on five most popular social networking sites by means of automated profile cloning and cross-site profile cloning. And further experiments results on real social network users confirm that this type of attack can achieve a high success rate.

Social network providers hosts large amount of sensitive data from OSNs users. The sensitive data providers a good source both for the research and for the business, so there is a require that data be analyzed by social network providers itself or unknown third parties. Past work on privacy preserving data publishing [30] have proposed several methods to deal with this issue. But for concern of simplicity, current data publishing of social network data usually use the anonymization method to shield sensitive information. But research by Lars Backstrom et al. [16] and Gilbert Wondracek et al. [15] who that anonymization methods can cause breach of user privacy.

Lars Backstrom et al. [16] show that adversaries can use anonymized social data to infer links between social network users. Both passive and active attack are shown to be effective to do this de-anonymization attack. With prior knowledge of the the social network and the de-anonymized links, attackers can identify a specific user.

Also, the de-anonymization of social links brings privacy threats to social network users. [31] proposes the use of interaction graph to impart meaning of social links by quantifying user interactions, and showed that interaction graph can be used as a better representation of user interactions of social network users. Similarly, [13] dicusses neighborhood attacks. The identity of a specific

user can be identified by obtaining some knowledge about the neighbors of a targeted victim and the relationship among these neighbors.

Lian Liu et al.[32] have studied privacy issue of sensitive edge weights of social networks and proposes methods based on randomization and purtabation for privacy preservation.

Sybil Attack

In large scale peer-to-peer systems, redundancy can be used to combat scurity threats from malious remote systems, but John et al. [18] show that the identity of these systems can be forged to undermine this redundancy, which is called Sybil attack. And they also show that Sybil attacks can always be possible for a system without a trustable centralized authority.

Auxilliary Data Attacks

Often times, social network activity can be linked to real life scenario. Minimum information is need for such kind of real life linkage attack if a lot of personal information is known about the victim. [33] compares online social network and real life social network and points out the domain feature of the real life social network and influences of online social network to the real life social network. This paper also proposes that different types of relationships of real life social network is a good implication of the design of online social networks for privacy purposes. It also proposes that causual relationships of both online and real life social network is common and further confirms that the interaction among social network users, which is also proposed in [31] are better implication of privacy concerns for online social network users.

Third Party Attacks

Third parties can pose serious threats to the privacy of OSN users. They can use various attacks[34], such as spamming and phishing attacks, infrastructure attacks, malware attacks, identity theft attack, neighbor attacks and other social attack methods to get users' private information. In this subsection, we will discuss spamming, phishing, identity theft and neighbor attacks in detail.

5.3 Perceived Social Network Risks

Risks and attacks of online social network reflect the potential damage to social network users. And users are learning, they start to make careful decisions about what information to put online under which circumstances, at the same time, more and more people are changing to a more restrictive privacy setting [35]. Usually, social network users will have risk considerations in mind when disclosing their private information on the social network. And it has been shown [36] that stronger privacy concerns resulted in more restrictive profile settings.

Definition 1. *Perceived risk is the direct reflection of user's opinion on how sensitive a specific profile item is to him/her-self. And this opinion will guide user make privacy settings on social network.*

5.4 Realized Social Network Privacy

Definition 2. *The social benefits and/or social risks of user u_i are realized when user $u_j, j \neq i$ visits the profile item f_{ij} of u_i, and we call the the social network privacy of u_i is realized upon event $e_{u_j \to u_i}$.*

We define the probability that the profile item f_{im} of user u_i is visited by user u_j as p_{jim}.

Use b_{jim} to denote benefit of u_j access profile item f_{im} of u_i.

The realized benefit of user u_i is defined as:

$$\mathcal{B}_i = \alpha_i \sum_{m \in \{1,2,\ldots,N_i\}} \sum_{j \in \mathcal{C}} b_{jim} \times p_{jim}$$

where α_i is parameter specific to each user, N is the number of items that user u_i has, and $\mathcal{C} \in \{\mathcal{C}_{USER}, \mathcal{C}_F, \mathcal{C}_{FOF}$ and $\mathcal{C}_{ALL}\}$ is the community of friendship.

The realized risk of user u_i is defined as:

$$\mathcal{R}_i = \beta_i \sum_{m \in \{1,2,\ldots,N_i\}} \sum_{j \in \mathcal{C}} r_{jim} \times p_{jim}$$

where β_i is the risk factor for user u_i, r_{jim} is the risk when u_j visits profile item f_{im} of user u_i, and p_{jim} is the probability of user u_j visits profile item f_{im} of user u_i.

For every friend $u_j, j \in \{1, \ldots, N_i\}$ of user u_i, the probability that u_j visits u_i is determined by the number of friends u_j has. And by assuming the simplest equal probability model we have $p_{ji} = \frac{1}{N_j}$, where N_j is the number of friends that u_j has.

For every friend of friend $u_j, j \in \{1, \ldots, N_i\}$ of user u_i, the probability that u_j visits u_i is determined by the number of friends of friends u_j has. And by assuming the simplest equal probability model we have $p_{ji} = \frac{1}{\sum_{k=1}^{N_j} N_k}$, where N_k is the number of friends of u_j's friend u_k has.

5.5 Deriving Benefit b_{jim} From Perceived Benefit

Social network benefit should be a perception of u_i about the benefit he can get by setting a certain privacy level. So, it is user specific. So, $b_{jim} = o_{jim}$, where o_{jim} is the observed benefit when u_j visits profile item f_{im} of u_i, which is actually the specific setting of privacy level for profile item f_{im} of user u_i.

5.6 Deriving Risk r_{jim} From Perceived Risk

Social network risk r_{jim}, is a natural property of a profile item f_m, it is the nature of the profile item, for example, some profile items are more risky than others in nature. Example, *phone number* is more risky than *education*. So, by this defnition, we can rewrite r_{jim} as r_m. We say that profile item f_m is more *risky* when more people set this item to be a more restrictive privacy level.

By using linear model, assign integer values to each privacy level $\mathcal{S} \in \{\mathcal{S}_{me} = 1, \mathcal{S}_f = 2, \mathcal{S}_{fof} = 3, \mathcal{S}_{all} = 4\}$, we can define r_m as mean value of aggregated privacy level settings.

$$r_m = \frac{1}{N} \sum_{i=1}^{N} o_{im}$$

where o_{im} is observed privacy setting of profile item f_{im} of u_i.

5.7 Item Response Theory (IRT) model

We use the two parametric logistic model to fit our privacy framework.

$$P_{ij}(\theta) = \frac{e^{\alpha_i(\theta - \beta_j)}}{1 + e^{\alpha_i(\theta - \beta_j)}}$$

$P_{ij}(\theta)$ is the probability that the privacy setting for profile item f_{ij} of user u_i can satisfy his/her expectation of using social network, α_i is the social network benefit expectation factor, which can be seen as a factor of openness of user u_i and/or benefit expectation of using the social network; β_j is the risk level for profile item f_j. And θ is the observed privacy level setting for f_j.

We expect that, when fixed risk levels β_j, the higher α_i, the harder to get satisfied; and when fixed α_i, less risky profile items can be easily satisfied. Figure 2 and Figure 3 have better illustration of these expectations.

And we can use optimization techniques to estimate parameters of benefit expectation factor α_i and risk β_j.

5.7.1 Estimating Benefit Expectation Factor.

5.7.2 Estimating Risk Vector.

References

[1] Justin Becker and Hao Chen. Measuring Privacy Risk in Online Social Networks. In *Proceedings of the Web 2.0 Security and Privacy 2009 Workshop (W2SP)*, May 2009.

[2] Tran Hong Ngoc, I. Echizen, K. Komei, and H. Yoshiura. New approach to quantification of privacy on social network sites. In *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, pages 556 –564, April 2010.

[3] Kun Liu and Evimaria Terzi. A framework for computing the privacy scores of users in online social networks. *ACM Trans. Knowl. Discov. Data*, 5:6:1–6:30, December 2010.

[4] B.Schiffman. Facebook ceo apologizes, lets users turn off beacon, 2007.

[5] Wikipedia. Google buzz, 2011.

[6] Elena Zheleva and Lise Getoor. To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In *WWW '09: Proceedings of the 18th international conference on World wide web*, pages 531–540, New York, NY, USA, 2009. ACM.

[7] Susan B. Barnes. A privacy paradox: Social networking in the United States. *First Monday*, 11(9), September 2006.

[8] Chris Grier, Kurt Thomas, Vern Paxson, and Michael Zhang. @spam: the underground on 140 characters or less. In *Proceedings of the 17th ACM conference on Computer and communications security*, CCS '10, pages 27–37, New York, NY, USA, 2010. ACM.

[9] Markus Huber, Martin Mulazzani, Edgar Weippl, Gerhard Kitzler, and Sigrun Goluch. Exploiting social networking sites for spam. In *Proceedings of the 17th ACM conference on Computer and communications security*, CCS '10, pages 693–695, New York, NY, USA, 2010. ACM.

[10] Markus Huber, Martin Mulazzani, Sebastian Schrittwieser, and Edgar Weippl. Cheap and automated socio-technical attacks based on social networking sites. In *Proceedings of the 3rd ACM workshop on Artificial intelligence and security*, AISec '10, pages 61–64, New York, NY, USA, 2010. ACM.

[11] Benjamin Markines, Ciro Cattuto, and Filippo Menczer. Social spam detection. In *Proceedings of the 5th International Workshop on Adversarial Information Retrieval on the Web*, AIRWeb '09, pages 41–48, New York, NY, USA, 2009. ACM.

[12] Fabricio Benevenuto, Tiago Rodrigues, Virgilio Almeida, Jussara Almeida, Chao Zhang, and Keith Ross. Identifying video spammers in online social networks. In *Proceedings of the 4th international workshop on Adversarial information retrieval on the web*, AIRWeb '08, pages 45–52, New York, NY, USA, 2008. ACM.

[13] Bin Zhou and Jian Pei. Preserving privacy in social networks against neighborhood attacks. In *ICDE '08: Proceedings of the 2008 IEEE 24th International Conference on Data Engineering*, pages 506–515, Washington, DC, USA, 2008. IEEE Computer Society.

[14] Krishna P.N. Puttaswamy, Alessandra Sala, and Ben Y. Zhao. Starclique: guaranteeing user privacy in social networks against intersection attacks. In *CoNEXT '09: Proceedings of the 5th international conference on Emerging networking experiments and technologies*, pages 157–168, New York, NY, USA, 2009. ACM.

[15] Gilbert Wondracek, Thorsten Holz, Engin Kirda, and Christopher Kruegel. A practical attack to de-anonymize social network users. *Security and Privacy, IEEE Symposium on*, 0:223–238, 2010.

[16] Lars Backstrom, Cynthia Dwork, and Jon Kleinberg. Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography. In *WWW '07: Proceedings of the 16th international conference on World Wide Web*, pages 181–190, New York, NY, USA, 2007. ACM.

[17] Leyla Bilge, Thorsten Strufe, Davide Balzarotti, and Engin Kirda. All your contacts are belong to us: automated identity theft attacks on social networks. In *WWW '09: Proceedings of the 18th international conference on World wide web*, pages 551–560, New York, NY, USA, 2009. ACM.

[18] John R. Douceur. The sybil attack. In *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, IPTPS '01, pages 251–260, London, UK, 2002. Springer-Verlag.

[19] Arvind Narayanan and Vitaly Shmatikov. De-anonymizing social networks. In *SP '09: Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, pages 173–187, Washington, DC, USA, 2009. IEEE Computer Society.

[20] Lujun Fang and Kristen LeFevre. Privacy wizards for social networking sites. In *WWW '10: Proceedings of the 19th international conference on World wide web*, pages 351–360, New York, NY, USA, 2010. ACM.

[21] Barbara Carminati and Elena Ferrari. Privacy-aware collaborative access control in web-based social networks. In Vijay Atluri, editor, *Data and Applications Security XXII*, volume 5094 of *Lecture Notes in Computer Science*, pages 81–96. Springer Berlin / Heidelberg, 2008.

[22] Barbara Carminati, Elena Ferrari, and Andrea Perego. Rule-based access control for social networks. In Robert Meersman, Zahir Tari, and Pilar Herrero, editors, *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*, volume 4278 of *Lecture Notes in Computer Science*, pages 1734–1744. Springer Berlin / Heidelberg, 2006.

[23] Mohd Anwar, Philip W. L. Fong, Xue dong Yang, and Howard Hamilton. Visualizing privacy implications of access control policies in social network systems.

[24] Adrienne Felt and David Evans. Privacy protection for social networking apis, 2008.

[25] Kapil Singh, Sumeer Bhola, and Wenke Lee. xbook: redesigning privacy control in social networking platforms. In *Proceedings of the 18th conference on USENIX security symposium*, SSYM'09, pages 249–266, Berkeley, CA, USA, 2009. USENIX Association.

[26] Kyumin Lee, James Caverlee, and Steve Webb. Uncovering social spammers: social honeypots + machine learning. In *Proceeding of the 33rd international ACM SIGIR conference on Research and development in information retrieval*, SIGIR '10, pages 435–442, New York, NY, USA, 2010. ACM.

[27] Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna. Detecting spammers on social networks. In *Proceedings of the 26th Annual Computer Security Applications Conference*, ACSAC '10, pages 1–9, New York, NY, USA, 2010. ACM.

[28] 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 annual conference on Internet measurement*, IMC '10, pages 35–47, New York, NY, USA, 2010. ACM.

[29] Tom N. Jagatic, Nathaniel A. Johnson, Markus Jakobsson, and Filippo Menczer. Social phishing. *Commun. ACM*, 50(10):94–100, 2007.

[30] Benjamin C. M. Fung, Ke Wang, Rui Chen, and Philip S. Yu. Privacy-preserving data publishing: A survey of recent developments. *ACM Comput. Surv.*, 42:14:1–14:53, June 2010.

[31] Christo Wilson, Bryce Boe, Alessandra Sala, Krishna P.N. Puttaswamy, and Ben Y. Zhao. User interactions in social networks and their implications. In *Proceedings of the 4th ACM European conference on Computer systems*, EuroSys '09, pages 205–218, New York, NY, USA, 2009. ACM.

[32] Lian Liu, Jie Wang, Jinze Liu, and Jun Zhang. Privacy preservation in social networks with sensitive edge weights. In *SDM*, pages 954–965, 2009.

[33] Paul Adams. The real life social network. 2010.

[34] Carl Timm and Richard Perez. *Seven Deadliest Social Network Attacks*. Syngress Publishing, 2010.

[35] Amanda Lenhart. Adults and social network websites, January 2009.

[36] Nicole Krmer Sonja Utz. The privacy paradox on social network sites revisited: The role of individual characteristics and group norms, 2009.

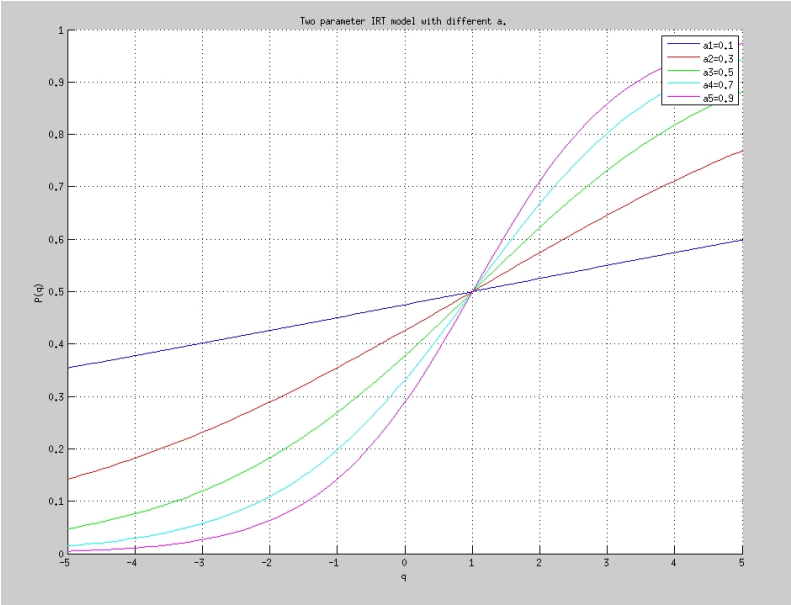

Figure 2: Satisfaction With different perception level.

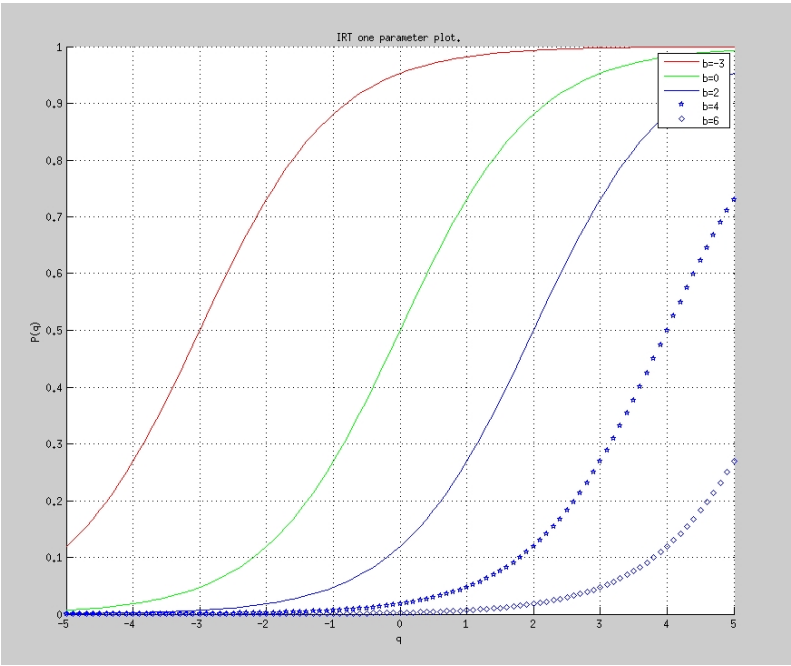

Figure 3: Satisfaction With different profile risk level.