2014

PRIVACY ISSUES IN ONLINE SOCIAL NETWORKS: USER BEHAVIORS AND THIRD-PARTY APPLICATIONS

Daniel W.K Tse  
*City University of Hong Kong, iswktse@cityu.edu.hk*

X. Xu  
*Department of Information Systems, City University of Hong Kong, xiaoxixu2-c@my.cityu.edu.hk*

M. Bai  
*Department of Information Systems, City University of Hong Kong, miaobai3-c@my.cityu.edu.hk*

Z. Chen  
*Department of Information Systems, City University of Hong Kong, zitaochen2-c@my.cityu.edu.hk*

X. Meng  
*Department of Information Systems, City University of Hong Kong, xinpemeng2-c@my.cityu.edu.hk*

*See next page for additional authors*

Follow this and additional works at: [http://aisel.aisnet.org/pacis2014](http://aisel.aisnet.org/pacis2014)

Recommended Citation

[http://aisel.aisnet.org/pacis2014/42](http://aisel.aisnet.org/pacis2014/42)

This material is brought to you by the Pacific Asia Conference on Information Systems (PACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in PACIS 2014 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Abstract

In contemporary society, social networking websites has developed dramatically and became an indispensable component in our daily life. Since it can help create a more feature-rich online social community, third-party service has been widely adopted in online social networks (OSNs). Integrating these third-party sites and applications has not only extended business of both social network server and third party and but also promises to break down the garden walls of social-networking sites. While at the same time it dramatically raises concerns on privacy leakage. This article mainly focuses on the privacy disclosure issues caused by user's behavior and third-party applications and websites. On the one hand, because of the diversity of usage behaviors, the revelation of personal information varies significantly. A survey is conducted to present empirical and quantitative result. On the other hand, the access mechanism between OSN and third party is not perfect enough. Besides, it could be a potential source of privacy leak that third-party services sometimes act as advertisers and information aggregators of a user's traversals. The relevant reasons and internal and external threats are presented. Finally, possible solutions to reduce the increasing information disclosure are provided. Actions should be taken along three fronts: the government, the users themselves as well as the third parties.

Keywords: online social networks; privacy issues; users’ behaviors pattern; third-party issues
1 INTRODUCTION

In recent years, online social networks (OSNs) have evolved into a social phenomenon. Individuals utilize such networks to communicate and bond with friends, relatives and acquaintances or even develop new relationships with complete strangers. Indeed, OSNs have already become an indispensable component in people’s daily life. However, online social networks are confronted with the same problem: the leakage of user information.

It is universally acknowledged that social networks usually require intensive user involvement, which makes it inevitable for the users to share personal information with acquaintances they barely known or even with strangers (Gross & Acquisti 2005). Thus, the article would summarize the user behaviors that are likely to lead to privacy revelation, identify potential risks related to as well as validate the observed patterns of user behaviors by a well-designed questionnaire.

In the meantime, to provide richer functionality, popular OSN have launched open platforms for enable third-party developers to offer applications with additional functionality and services which OSNs do not have through the use of APIs (application programming interfaces). It is obvious that the emerging third-party applications (TPAs) also poses severe privacy risks to users. To thoroughly look up the development, categories and access mechanism of TPAs would contribute to analysis of hide risks and prevention solutions.

2 RESEARCH METHOD

This article adopts both quantitative and qualitative analysis method to develop an understanding of the origins and possible disclosure ways of information relevance.

2.1 Methodology framework

The quantitative method is used mainly in the field of user behavior while the qualitative method is used primarily in terms of third-party part. In the first place, qualitative method is used to get a whole view of privacy issues followed by questionnaire analysis which presents quantitative method.

As shown in Figure 1, method of each part has been specified. The user behavior pattern is analyzed both theoretically and experimentally. Potential risks and corresponding solutions are defined qualitatively.

2.2 Statement of the questionnaire

The primary part of questionnaire is designed concentrated on user behavior. The rest questions about third party are added to see user’s perception and attention about disclosure due to TPAs.

There are five aspects of questions from the user’ perspectives including demographic factors, user’s decision on disclosing information, user’s privacy setting, user’s trust and privacy concern about OSNs and user’s privacy reflection.

The questionnaire uses five degrees including ‘Strongly Agree’, ‘Agree’, ‘Neutral’, ‘Disagree’, and ‘Strongly Disagree’ as the options to reveal the attitude of the interviewees. If interviewee chooses ‘Strongly Agree’ or ‘Agree’, this option should be considered as ‘Approve’. The research allocates those 5 options a certain score range from negative 1 point to positive 1 point while neutrality is appointed as 0 point. Multiplying the score of

<table>
<thead>
<tr>
<th>Description</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly agree</td>
<td>2</td>
</tr>
<tr>
<td>Agree</td>
<td>1</td>
</tr>
<tr>
<td>Neutrality</td>
<td>0</td>
</tr>
<tr>
<td>Disagree</td>
<td>-1</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>-2</td>
</tr>
</tbody>
</table>

Table 1: Final score of questions
each option by the percent of each option, the final score of the specific question can be got. The final score is ranged from negative 2 point to positive 2 point as shown in Table 1.

The objectives of this investigation majorly are undergraduates and postgraduates in universities in mainland China. 200 copies of this questionnaire are distributed.

3 LITERATURE REVIEW

3.1 Various Threats

As OSNs are highly developing, it has raised a lot of security concerns. Generally speaking, two types of threats are identified, traditional attacks and specific threats (Fire, et al 2014). Traditional attacks refer to classical threats such as Trojans, Malware, URL shortening etc. Specific threats refer to some unique attacks that OSNs have. They can be further divided into three categories, namely, identity related threats, private threats and social threats (Binsaleh 2013).

Threats appear inside the vendor of third-party applications (TPAs). On one hand, it is doubtful that TPAs vendors are trustful. In 2010, a piece of news shocked many users in OSNs. It was said that top 10 apps in Facebook were more or less aggregate and sell user data to advertising company (清雨 2012). On the other hand, TPAs are provided by coders with all kinds of professionalism and different levels. Very few coders are likely to have any secure software skills and awareness. There is a constant situation of new vulnerabilities simply stemming from poor coding. It is possible for malicious entities to exploit the badly written code to extract personal data (Mansfield-Devine 2008).

Since TPAs do not originate from by the OSN server, the details of the TPA code are unknown for OSN server. Thus, the trust of OSN server will not be inherited to TPAs. The OSN server may have certain degree of specific policies which have so many external variables difficult to police.

3.2 Existing Solutions

OSNs providers, researchers as well as security firms are searching for solutions to handle with the increasing threats. OSNs operators have launched several kinds of security protections. Basic one is privacy setting function such as coarse-grained access control (Fire, et al 2014). Authentication mechanisms and encryption are also widely used (Beye, et al 2010). For instance, part of OSN profile can be encrypted by public key cryptography (Lucas & Borisov 2008). One type of internal authentication is alert from OSN vendors. A specific case from QQ is that when a user account login in different place in very short time slot, the system will send the user a notification about identity theft threat. Special solutions are issued by some researchers. A multi-user taint tracker which enables TPAs be compliant with access regulations of OSNs vendors has been designed (Shakimov & Landon 2013). Additionally, securities firms, e.g. AVG, McAfree, provide Internet surfing security for users and companies such as Norton offer specific OSN applications for Facebook users (View 2011).

4 A STUDY OF USER BEHAVIORS

With the dramatic growth of the number of the users of OSNs, the information disclosed on the internet has increased at the same time.

4.1 User Behavior Patterns

In the previous studies, certain patterns of user behaviors that are likely to lead to privacy revelation have been observed.

4.1.1 User’s Decision on Disclosing Information

Basically, personal information related to OSNs can be divided into 5 categories: thumbnail profile (brief profile with photo), greater profile (additional information, address or relationships, etc), list of friends, user generated contents and comments (Krishnamurthy & Wills 2008).

According to the users, the appropriate information to be disclosed should be safe, socially acceptable and normal. In other words, the information should not be able to lead them to be stalked as well as has appeared in other users’ profiles (Strater & Lipford 2008). Among all the information fields, most users consider the contact information to be the most sensitive and chose not to release them (Strater
Also, the users might provide personal information based on their motivations. For example, they may disclose their class schedule to find classmates (Strater & Lipford 2008).

Interestingly, a strange social norm has been observed: When releasing personal information, the users tend to use an all-or-nothing approach. This means their personal information either is restricted to “only friend” or remains completely open to the public. (Strater & Lipford 2008).

### 4.1.2 User’s Privacy Settings

Although privacy settings are slightly different through different OSNs, the default privacy ones encourage their users to share personal information. Mostly, the personal information is automatically set to be viewed by all users. Some campus-oriented OSNs, like Facebook, focus their default privacy settings on regional networks. However, these social networks have one certain thing in common: despite the absolute majorities of privacy settings are allowed to be modified there is no way to limit the visibility of thumbnail profile (Krishnamurthy & Wills 2008).

Similarly, as disclosing information mentioned before, users also apply an all-or-nothing approach when setting up their privacy strategies. Usually, privacy options are set either none or all (“only friends” / completely open) (Krishnamurthy & Wills 2008). In addition, they either fill in more information fields or leave them blank as well (Krishnamurthy & Wills 2008).

Moreover, for most users, establishing privacy settings is also a one-time event (Strater & Lipford 2008). Their privacy disclosure decisions are made in creation of profile and did not think of them carefully. They might generate new contents once a while, but they rarely revisited them or revising the privacy settings.

Still, most users chose not to change the default settings (Williams, et al. 2009). They think the privacy setting interface is complex and lacks of usability. Even worse, the outcomes of their modifications cannot appear in their own pages.

### 4.1.3 User’s trust and privacy concerns about online social networks

There lies a fascinating paradox about OSNs: Although the users have certain degree of privacy concern, actually such concerns would not be converted into any actions (Dwyer, et al. 2007). Honestly, they usually do not have a clear awareness of who can access their personal information (Dwyer, et al. 2007).

Meanwhile, there is also a phenomenon called “shrinking audience”: The perceived audience would be shrunk over time (Strater & Lipford 2008). To be specific, the perceived audience transform from the public to people on their friend lists, with whom they have actual and regular interactions. Thus, they even have not realized that they disclose some sensitive information which they originally decide not to.

What’s more, online relations with complete strangers can be built where perceived trust and privacy safeguard are weak (Strater & Lipford 2008). Such relations sometimes can be extended beyond the boundaries of OSNs. For instances: exchanging e-mails, making phone calls or even face to face encounters.

Beside, users’ password management has two features according to researches (Hasan & Hussin 2010) and (Vorakulpipat, et al. 2011). In one side, lots of users would share password with their friends and relatives based on trust. Another phenomenon is that 83% of the total participants use the same password for several accounts (Hasan & Hussin 2010). Furthermore, 44.5% of this survey’s respondents indicated that they even use the same password for email and social networks accounts. Commonly, a user uses one email account to register for various networks for the convenience of receiving updates and resetting password. Combining the sharing action, the potential risk of this OSNs account will double or triple. Once the confidential data of a social network is leaked, which is easily to happen, the hackers will directly know users password of original email. Later, the hacker even can directly know other accounts information of this particular user under the help of email account.
4.1.4 Demographic and geographic factors

This part mainly identifies influences of demographic factors to users’ security attitudes as well as behavior, specifically, age, gender, education background and geographic location. All these factors have impact on users’ security behaviors. Referring to related conduction surveys, several hypotheses are mainly divided into two parts. Generally, the first hypothesis reveals the relationship between demographic factors, including gender, age and education level. Moreover, the second hypothesis put emphasis on geographic factors as well as developing or developed countries.

A) Demographic factors

By referring and analyzing the survey conducted by various researches, we identify demographic factors into three parts comprising age, gender and education background. All the differences among these three factors have significant impact on social network security behaviors.

Firstly, the influence of gender does concern. Males tend to expose more information in their profiles compared with females. According to previous surveys, many male users would even illustrate whether they are single or not in the OSNs profiles which is not given by many female users. Besides, in terms of accepting adding requests of a complete stranger, males are more willing to accept others’ requests than females, which can be calculated from the survey from (Williams, et al. 2009). At the same time, males are more likely to accept strangers’ invitation with 33% when compared with females with 28%, which might because female users’ accounts are more private and they are more sensitive to potential security risks.

Moreover, demographic factors also include age. Generally, younger people are less concerned about the information posted on their profiles. To be more specific, 15-24 years-old users post most personal information. But, in our reference research, gender is combined with age in the demographic survey and not used to analyze how it affects users’ privacy behaviors in the following part. Therefore, we would separate these two factors in the following questionnaire and analysis.

Another important factor is education level, which will also be involved when designing our survey. To be more detailed, postgraduate and graduates are two main focuses to be distributed questionnaires. Furthermore, we generate the hypothesis that a positive relationship exists between education level and users behaviors.

B) Geographic factors

In the previous survey conducted (Krishnamurthy & Wills 2008), when studying the percentage of the visibility of profile and friend list in different area, the authors demonstrate that they figure out a negative correlation between regional network size and the percentage of the use of privacy settings. In other words, users in smaller networks are less concerned. Similar conclusion is figured out in research (Vorakulpipat, et al. 2011). OSN users in developing countries, of which related OSNs policies, legal, ethics and awareness do not accord with this high speed development. Users are not sensitive with potential risks and it is much easier to trigger information security problems when comparing with developed areas. Consequently, we would take geographic factor into consideration.

4.1.5 User’s Privacy Reflection

Many researches, such as (Strater & Lipford 2008) and (Lang, et al. 2009), illustrate users’ reflection after participating in the distributed surveys. Usually, users’ privacy reflections can be promoted when they feel their privacy has been intruded. The most common ones are being contacted by a stranger or the Newsfeed feature. Newsfeed, or Minifeed, is a list of any recent activity on the profile. This new feature makes most users feel intrusive. In addition, participating in similar studies or attending related lectures can prompt users’ privacy reflections as well. Many of the interviewees report that they will alter their privacy settings and remove some information. Thus, the hypothesis is: user’s privacy utilization may increase as the improvement with their experience over time.

4.2 Potential risks triggered by user behavior and attitude

Lots of users’ behaviors could contribute to security risks especially in developing countries as mentioned above, where users do not that concerned and behaviors are not so standard. Worse still,
further potential loss of finance can be generated. However, article (Vorakulpipat, et al. 2011) reveals that, 75% of the respondents cannot identify basic security threats including “phishing” and “identity theft” in terms of users’ security awareness. Among all the risks, two consequences are most common.

In the first place, data re-identification is very typical. The adversary can conduct demographics re-identification (generates from the combination of gender, date of birth, and ZIP code), face re-identification (as the users “generously” provide high quality images and do not change profile pictures among different websites) and worse still, social security numbers (OSNs) and identity theft. With the help of powerful processors, various links would be generated based on the analysis of various OSNs accounts concerning one specific user. Giving demographics re-identification as an example, further analysis is even not needed due to the fact that many users directly post their real location on OSNs. It is not uncommon for the kind of crimes conducted to children based on the location which are posted by their parents. In other words, it is users themselves who provide valuable information to hackers. Also, the adversary can build a digital dossier of the user for continuously monitoring.

Furthermore, the user might be stalked by a potential adversary, including both cyber-stalking and cyber harassment. Hackers can collect all the related data of one user because users tend to use the same name for various OSNs. Cyber stalking usually involves relentlessly pursing while cyber harassment can lead to further offline attacks. Although the two terms always considered as interchangeable, they can be distinguished from the perpetrator’s originally motivations.

5 A STUDY OF THIRD PARTIES

5.1 Introduction of third-party applications

With the introduction of third party applications (TPAs), social networks have become a kind of platform on which mini-games and applets can be utilized to attract more users and enhance their profiles. Other than the traditional functions such as making friends and sharing photos, these applications are created by third party developers and have been widely adopted by adding additional values to users.

Utilizing TPAs seems to be a quite effective strategy to increase user stickiness and implement commercial values when faced with a rapid spread of OSNs. In this case, majority of leading social network sites have developed their own open platform. Based on it, diverse applications are created and adopted to keep positive user interactions. For instance, considering Facebook, one of the most popular OSNs around the world, there are more than 500,000 applications created by millions of developers. In addition, a very high adoption rate is also reported that 70% of Facebook’s users use at least one application every month (Facebook Statistics 2009). When looking into the Chinese marketing, data also show a beneficial tendency. For SinaWeibo, more than 15 million users are using over one thousand applications through its open platform. The number accounts for around 30% of its entire users and still increasing dramatically. Besides, there are about 2 million users per day using TPAs on SinaWeibo (王明功 2010). All the statistic data above can be regarded as powerful evidence of the popularity of TPAs. According to different functions and targeting users, existing TPAs can be divided into several types including basic, rich media, life style, business, social games and developer tools.

5.2 User behavior in TPAs

In this section, we shall discuss the user behaviors coming to TPAs. Firstly it is foremost to understand that why people have especially keen to use TPAs. A generally acceptable reason concluded from the past investigations reveal that a large proportion of users expect to have additional interaction with others through TPAs, such as sharing new photos or playing online games with their friends (Besmer & Lipford 2010). What's more, certain applications with specific functions can also arouse user's interest. A typical example is online games. From the perspective of the entertainment features of the Internet, online games are more susceptible to the users. Although a variety of reasons have contributed to the users adding of TPAs, all roads lead to the same destination that more and more applications are adopted by users.
Given the reasons mentioned above, it seems that users may primarily focus on the availability of TPAs rather than the security. Consequently, private information might be disclosed that result from a very weak consciousness of the security. On one hand, users need to sign a Privacy Agreement while installing and start using the TPAs which indicate consent to it for obtaining confidential information. However, most users rarely read this access message, ignore it and quickly click on the allow button. Once access to those applications, most of user's profile data as well as part of friends' profile data, is available for the application to query and use. Generally speaking, users' lacking control over their information and their difficulty in understanding the implications of application use are the crucial factors resulting in private information disclosure. On the other hand, OSNs provide people with a convenient communication platform, on which users can interact not only with families and friends but also with people from different countries and different backgrounds. For this purpose, some users are proactive to reveal their personal information as much as possible on social networks. Even in some cases, people may be more inclined to interact with strangers rather than their closest connections through TPAs. All of these subjective behaviors also can lead to security issues. As a consequence, researches on psychology and behavior of users are necessary and quite significant.

5.3 The OAuth protocol

To better understand the threats brought by TPAs in OSNs, it is essential to be clear about the access mechanism of TPAs. Nowadays, OSNs, like Facebook, Twitter, Sina, QQ etc., use Open Authorization (OAuth) protocol to protect user information. OAuth is an open protocol which allows secure authorization for web, mobile and desktop applications in a simple and standard manner (OAUTH).

The four main elements in OAuth protocol are as follows:

- **Service provider**: In our scenario, it refers to the OSN open platform which offers sign-on service and data storage. That is to say, the OSN server takes charge of login certification as well as user privacy protection. It is better to highlight that without the username and password, which are used to confirm the identity of the user, it is not legitimate to view and modify user content.

- **User**: The one who have username and password to login service provider which stores user information and service information. Generally speaking, user is unwilling to make personal data publicly but it is necessary to share part of user information with third-party apps and websites.

- **Consumer**: An application is required to be authorized and authenticated in order to gain access to user information. It can be web app, desk app or mobile app.

- **Protected resources**: It refers to the user information kept in service provider database.

The steps including are (Youku 優酷) (Hardt 2012):

1. **The user requires a third-party service via a TPA.** That is to say, user needs to share some information with the TPA.
2. **The consumer (third party) asks the OSN server for authorization from the user (resource owner).** The authorization can be made directly by the service provider or indirectly by an authorization center.
3. **The OSN server asks the user for authorization.**
4. **The user enters username and password to pass the OSN server authentication.** The OSN server authenticates the user and validates the authorization grant, and if valid, issues an access token.
5. **The consumer requests the authenticated information, like credential representing the user authorization, access token for example.**
6. **The consumer can serve the user after requesting the protected resource from the resource server and authenticated by presenting the access token.**

(微博 開放平台) (新浪微博) (Baidu 文庫) (ITeye) Firstly, the TPA should use Consumer_key and Consumer_secret along with signature and timestamp to require the Request_token. Then the OSN
server will generate the temporary Request_token. Notice that this token cannot be used to enter the OSN database to gain user information. After gaining the Request_token, the TPA will direct user to OSN server to get user’s authorization. If the user does not grant, the whole process is over. Or, if the user has granted, the TPA can raise a new request to exchange the Request_token for an Access_token. Finally, after getting the Access_token and other related authorized information, the TPA can access user data without obtaining username and password.

As presented above, the OAuth authorization framework puts the user in control of delegating access and grants a TPA limited access to an HTTP service (OAUTH). This allows third party service to integrate with OSN service on behalf of that user. Such delegated authorization mechanism offers authorization control based on privacy policies, to prevent providing username and password when a user responds to a requesting third party.

5.4 Threats brought by TPAs

In social media era, OSNs may bring users unexpected added value. That’s why social network accounts become increasingly significant. Besides, user data with great potential commercial value in exponential growth has attracted vast amounts of malicious entities. The main threats brought by third-party apps and websites are various from different aspects.

- Information source diversity. It is impressive that diverse and more user data start to be generated during using TPAs. For example, since jing.fm/# is bond with SinaWeibo, your friends in SinaWeibo will know what you have listened to this third-party website after you used jing.fm/# to listen music online.

- Drawbacks of the OAuth protocol. The OAuth protocol can offer authorization without providing username and password as mentioned in last paragraph but actually what third parties can access is much more sensitive than expectation. That is because many OSNs only provide an all-or-nothing policy without assigning which information TPAs can access. In other words, user can decide whether or not to authorize the TPAs. However, user cannot specify a granted access control when it comes to application-to-user interactions in the meanwhile (Cheng 2013).

- Powerful APIs. Mainstream OSNs have released web APIs to allow third-party developers to process and implement their own services. In fact, current APIs are designed without taking access control into consideration. The result is that after gaining authorization, APIs enable third-party apps or sites to establish new data or utilize and aggregate existing user information and activities without obstruction.

- Lack of concern about TPAs disclosure. OSN server may pay more attention about their own business than user privacy. In 2011, SinaWeibo closed many APIs because TPAs share information in Sina with other OSNs only, rather than user privacy disclosure (上海热线 2011).

- “Useless” information collection. Often, TPAs get information which is not useful for the apps service providing but may have some commercial value. A more serious concern is that some TPAs would require not only your data but also data of friends in your social graph. This is some degree resulting from the promotion requirement of the TPAs. What’s more, this kind of collection is usually without individuals’ precise knowledge or even awareness.

- Disclosure across websites. People often have multiple OSN accounts. Since the integrating of TPAs help break down the garden walls of social-networking sites, the data mining attack will be more efficient.

- Endlessly emerging attacks. There are many CSRF leakages in OSNs (WooYun). In 2012, it was repaired that

<table>
<thead>
<tr>
<th>Profile</th>
<th>Of Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall</td>
<td>Male 91 46.4%</td>
</tr>
<tr>
<td></td>
<td>Female 105 53.6%</td>
</tr>
<tr>
<td>Undergraduate</td>
<td>Male 55 54.5%</td>
</tr>
<tr>
<td></td>
<td>Female 46 45.5%</td>
</tr>
<tr>
<td>Postgraduate</td>
<td>Male 32 37.2%</td>
</tr>
<tr>
<td></td>
<td>Female 54 62.3%</td>
</tr>
<tr>
<td>Others</td>
<td>9</td>
</tr>
</tbody>
</table>

Table 2: Demographic of questionnaire
one leakage in Renn which could be used to skip the user certification step in OAuth authorization (WooYun 2012).

6 RESULTS ANALYSIS

Based on the study mentioned above on the OSNs, a survey is conducted which mainly focuses on revealing of the user behavior. 200 questionnaires are distributed to OSNs users while only 196 questionnaires are valid. Within the 196 valid questionnaires which are completed by the person whose age ranges from 18 to 27 years old, about 46.4% questionnaires came by male and the remained 53.6% came by female, as shown in Table 2. About 51.5% questionnaires are from undergraduate, 43.8% questionnaires are from postgraduate and only 2.0% are from PhD. In addition, there are 2.6% questionnaires are completed by the user who is exclusive the three types of objects. The interviewees use 4 OSNs on average.

6.1 Users’ perspective

In the field of sharing the personal information, female and male show the same preference. Besides, the difference for undergraduate and postgraduate are not significant except that the willingness of sharing user generated content. About 17% more undergraduate users prefer to share their content than postgraduate user, as shown in the Figure 2.

Considering the information disclosed by the user, almost all the interviewees think that information should be protected but only 35.2% of interviewees think the information they issued should be accepted by public while 37.24% are neutral. Moreover, the percent of female is almost a half larger than the percent of male, as shown in the Figures 3 and 4.

It is found that contact number and address are the two most sensitive among all related information and the OSNs users usually are not willing to disclose, as shown in Figure 5. According to the data of the survey, people would use OSNs with some certain purposes, as shown in Figure 6.

The research finds that most users restrict their profile only to friends or publicize them to all of others with the all-or-nothing approach, as shown in Figure 7. From the data collected, users tend to set their privacy options to either fill or leave them blank, as shown in Figure 8.
Analyzing to the user habit about the privacy setting, it is found that over one thirds of users tend to change the default privacy setting and less than one thirds users change that setting after using for a while, as shown in Figures 9 and 10. Interestingly, the percent of changing the default setting in after the establishment of the account of mail is 14% higher than female while there are 22% female are likely change the default privacy setting in the process of using more than male.

This user behavior which is correlated with privacy setting does not reveal any distinction between undergraduates and postgraduates. The research reveals the phenomenon that the number of users who consider the interface of privacy setting is not complex is almost double that the number of who think that is complex, as shown in Figure 11.

More than 50% of users admit that they cannot remember the detail about the privacy setting, only less than 25 percent tell us they can remember those setting, as shown in Figure 12. Beside, there are 20% more female consider the privacy setting interface less complex than male and almost 10% more female can remember the privacy setting than male. One possible reason is that the design of OSNs is
based on the user behavior of female. Another possible answer would be the frequency of using OSNs: Female uses more than male so that it seems easier for female to understand and remember the privacy setting.

It also illustrates that over 80% users have a relatively high privacy concern. Meanwhile, more than 70% users think that their privacy cannot be protected perfectly, shown in Figure 13 and 14 respectively.

However, those concerns do not trigger any actions. Specifically, over one third interviewees are not aware of who can access to their privacy information, shown in Figure 15. Over one third users, shown in Figure 16, even accept the completely unfamiliar one to be their friend and create extended relationships such as exchanging phone numbers. There is a gender difference that male would be more likely to make friend with strangers.

Different from the attitude of accepting friends, users are vigilant about OSNs password. About 52% users, shown in Figure 17, have different passwords of registering e-mail and OSNs account and keep confidential to their friends. This phenomenon is severer within the female, shown in Figure 18.

When they are aware that there are threats to their OSNs privacy information, almost everyone will remove their information and change the privacy setting and female is more likely to do so, as shown in Figures 19 and 20. The conclusion can be easily obtained that female act more cautiously than male when using the OSNs. There is a remarkable difference that only 57% of postgraduate would remove
their information when the thread is perceived which is much less than the percent of undergraduate
which is 91%.

6.2 Third-party perspective

According to the survey, the cognition of third party application is very limited. Specifically, about
57% of interviewees would neglect the declaration of authorization when installing the third party
application, as illustrated in Figure 21. Besides, nearly 47% of interviewees claim that they do not
know what they authorized when installing third party application and they have no idea about which
part of authorization is necessary, as shown in Figure 22.

7 PRIVACY DISCLOSURE & PREVENTION

7.1 Users’ perspective

To be honest, the most basic solution to user information leakage should be enforced by the
government. Indeed, it is OSNs’ obligation to enhance the existing mechanism to defend against
user’s privacy as well as restrict external applications. However, relying merely on OSNs to conduct
such enhancement voluntarily seems to be unrealistic. The majority of OSNs encourages users to
share personal information: the default privacy settings are permissive; not to mention that they might
even corporate with a large number of third-party applications. Thus, the enforcement from
government becomes indispensable.

Certain compulsory improvements are listed as following:

- The OSNs should provide the new users with immediate protection for the sensitive and risky
  information as they are more likely not to gain a basic understanding about privacy protection and
  make their decisions in haste.

- The interface should be improved to reduce its complexity and enhance its usability. Allocating
certain personal information setting on a separate page should not be allowed in any case.

- Risk assessment programs to educate users the potential dangers of posting sensitive information
  are highly suggested and it would be more effective if they were designed to cultivate user’s
  awareness in regular activities with OSNs.
In addition, there are several tips for users to acquire safety: Remembering the Internet is a public resource, the friends that the users constantly interacted with are by no means the only audiences; being wary of strangers, always consider their possible intentions for a second time; being skeptical with third-party applications, take user authorization seriously; lastly, scrutinizing and altering privacy settings as they are the instruments which can be used to defend privacy currently.

7.2 Third-party perspective

This part, in allusion to the problems existing in the utilization of TPAs, put forward the countermeasure and suggestion. Firstly, consider that user's profile data may be disclosed by TPAs deliberately or unconsciously, a kind of controlling mechanism is suggested to relieve the severity (胡启平 & 陈震 2010). On the premise of ensuring existing functions of TPAs, it should monitor the information flow strictly by controlling what kind of information the application could obtain and which external websites or programs can they exchange the information. In addition, each application needs to inform the control center which profile data are required and where are to be sent. These detailed lists ultimately display to users to determine whether the application is secure enough to be used or not. Such specific, transparent and strict information flow control is obviously more secure than the original access agreement that force users agreed to hand over all information to TPAs.

Furthermore, given that the TPAs is developed based on the open platform of different OSNs and can bring more benefit to them, these social network sites must take responsibility to avoid the disclosure of user's profile data. OSNs is required to provide more detailed privacy options for users that help to determine whether allowing TPAs acquire profile data and its updates. Meanwhile, application that wants to read user's private messages also needs a revaluation of its permission obtained before. Besides, rules of user information security protection must be launched to restrict the access of TPAs. All in all, social network should not escape from its responsibility, by contrast, also should play a successful role of monitoring and controlling. Last but not least, the increase of user's security awareness is a pivotal factor to avoid the disclosure of personal information (罗力 2012). To begin with, specific regulations should be suggested to limit information sharing on public social platform which can prevent confidential data and documents from revealing. What's more, a wide and deep-going education for users must be launched to enhance the sense of security and responsibility. In the end, it is crucial for individuals that guaranteeing their computer or mobile device equipped with comprehensive safety precaution.

8 CONCLUSION

This article is intended to raise concern about OSNs privacy issues among the youth. In this article, it is provided that both theoretical and experimental analysis of the vulnerabilities in OSNs due to user behavior preference and usage of TPAs. It is shown that certain user behavior patterns will lead to various privacy revelations. The usage of TPAs makes the situation worse. What's more, leakage in TPAs is hard to be aware by users. As it is analyzed, some disclosures are inevitable since the inherent leakages are due to the original design purpose of online social network. For example, Renn encourages users use real name and other personal information for easily finding schoolmates but actually it does not provide any real world identity authentication. In this situation, information of user who has lower privacy concern may be public to malicious entities who pretend to be a legitimate user.

However, it is noticed that in spite of various types of threats caused by user behaviors referred above, few persons change the default fragile privacy protection configuration provided by OSNs after maximizing the visibility of profiles. This happens due to the lack of basic security knowledge and neglect of perspective perceptible threats.

To sum up, three aspects of protections measurement related to user, OSN server and government should be taken and cooperated to decline the information disclosure.
REFERENCES


OAUTH, The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service. [Online]. Available: http://oauth.net/


