# Social Network Privacy: Issues and Measurement

Isabel Casas, Jose Hurtado[✉], and Xingquan Zhu

Department of Computer and Electrical Engineering and Computer Science,
Florida Atlantic University, Boca Raton, FL 33431, USA
{icasas1,jhurtad2,xzhu3}@fau.edu

**Abstract.** Social networks are becoming pervasive in todays world. Millions of people worldwide are involved in different form of online networking, with Facebook being one of the most popular sites. Online networks allow individuals to connect with friends and family, and share their private information. One of the reasons for the popularity of virtual communities is the perception of benefits received from the community. However, problems with privacy and security of the users information may also occur, especially when members are not aware of the risks of posting sensitive information on a social network. Members of social networking sites could become victims of identity theft, physical or online stalking and embarrassment as a consequence of malicious manipulation of their profiles data. Although networking sites often provide features for privacy settings, a high percentage of users neither know nor change their privacy preferences. This situation brings to consideration about many important aspects of social network privacy, such as what are the privacy issues in social networks? what are common privacy threats or risks in social networks? how privacy can be measured in a meaningful way? and how to empower users with knowledge to make correct decisions when selecting privacy settings? The goal of this paper is twofold. First, we discuss potential risks and attacks of social network site users privacy. Second, we present the measurement and quantification of the social privacy, along with solutions for privacy protection.

## 1 Introduction

With the arrival of the Internet, online social networking has transitioned from being used by selected user groups to mass adoption. While personal information is occasionally made available via the Internet, these sites further promote the sharing of personal related content. Boyd and Ellison presented in [21] a definition of online social networks: "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system". With their commercial success and rapid growth in participation, online networking has diversified its usage across a myriad of different websites. In [2], Acquisty

J. Wang et al. (Eds.): WISE 2015, Part II, LNCS 9419, pp. 488–502, 2015.
DOI: 10.1007/978-3-319-26187-4_44

and Gross presented a classification of sites as follows: common interests, dating, business, pets, photos, face-to-face facilitation and friends.

Even though each social network site has its own unique concept and themes, most of them require users to create a representation of themselves or profile with the purpose of interacting with other users. Because user profiles may contain private or sensitive information, such as home address, school, personal preference etc., the protection of private data has become increasingly important. Although the visibility of a profile can be fine-tuned by users, this feature varies from site to site, and information is often completely visible by default settings for many networks, such as Facebook. To aggravate the situation, online networking companies often have nontransparent ways of handling users data since they intend to maximize their revenue by targeted advertising or other channels.

The advancement of online social networking has brought changes and new perspectives to numerous already established concepts and ideas. In 1890, Warren and Brandeis [22] created what is considered the first United States publication advocating for the right of privacy, with privacy being simply defined as: “the right to be let alone”. On his book Privacy and Freedom [23], Westin defines privacy as the right “to control, edit, manage, and delete information about them[selves] and decide when, how, and to what extent information is communicated to others”. While these definitions have been accepted for many years as synonym of privacy, their limitations become clear when applied to cyberspace, particularly in online social networking environments.

Indeed, privacy has brought new challenges to the academic community and much research has been done in the subject [25–29]. Still, privacy understood in the online situation is a rather elusive term; users should have the right to be left alone but also, as presented in [30], should have the right to be “left in secret”. The link between the usage of social networks and privacy is not easy to understand. On one hand, some users would like to share their personal information only with friends or family members but not strangers [2,31]. On the other hand, some users are happy to publicize personal related content with total strangers. In [48], the author suggests to look at privacy from different perspectives, including governmental policies, citizen rights, and consumers protection. In the case of online social networks, its consumers have the right and must know, what information is being collected, by whom and how it will be used. In any case, when information is published, users expose themselves to threats that range from identity theft, embarrassment, stalking to hiring discrimination. Furthermore, personal data from numerous users from a social network can be profitable to other users and third parties.

Due to many concerns raised regarding privacy issues in social networks, research has been made in developing efficient ways of measuring and evaluating privacy. Some works have proposed brand new models to approach privacy in online social networks in order to address flaws of existing models [32]. Following a different approach, some researches propose smart ways of using the existent privacy settings from popular networking sites such as Facebook. Applications that analyze current privacy preferences and recommend more privacy-aware ones have also been developed [11,12]. The authors in [3,4] constructed a privacy index, where the calculation of the privacy index incorporates sensitivities and visibilities of known attributes in a users profile. In this paper, we examine two aspects of online privacy. First, we make an analysis on privacy issues in online social networks as well as attacks against users privacy. Next, we review the literature to find what has been studied in the subject of privacy measurement in online social networks. While our findings show that many works have been done regarding privacy issues in social networks, very few works, however, have addressed the measurement of the privacy, which leaves plenty of room for improvement.

A brief view of the social network entities, and their roles and relationships from data perspectives is shown in Fig. 1.

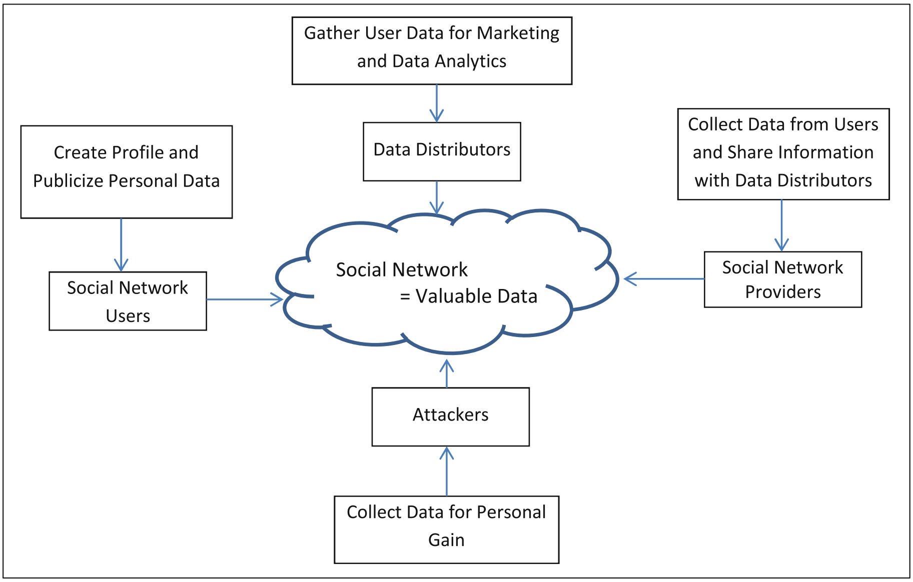
Gather User Data for Marketing and Data Analytics
Data Distributors
Create Profile and Publicize Personal Data
Collect Data from Users and Share Information with Data Distributors
Social Network Users
Social Network = Valuable Data
Social Network Providers
Attackers
Collect Data for Personal Gain

**Fig. 1.** Social network entities, and their roles and relationships from data perspectives

## 2 Privacy Issues in Social Networks

With the advancement of the internet, private information has been made available more than ever and online social networks have played a major role in this situation. Privacy implications are determined by how identifiable private information can be derived from provided data, its recipients and its uses [2]. Numerous discussions have been previously made on privacy in social networks [30,33–35].

Researchers have identified two main methods of private information gathering: data leakage due to privacy disclosure and data leakage based on attack techniques [30]. Yang *et al.*, [24] further separated these two main methods into four categories: (1) individual items (profile picture, home address etc.) are available to attackers, (2) aggregation of items of the same person collected though different social sites, (3) inference of hidden attributes from public attributes and, (4) de-anonymizing datasets. In [24], the authors modeled two types of attackers: tireless attacker and resourceful attacker. Resourceful attackers have enough means such as storage and knowledge to gather information from social networks and create his/her own database or digital dossier. Tireless attackers, although lack material means, are willing to dedicate plenty of time and energy. These types of attackers are usually knowledgeable in information retrieval techniques. Information can be collected by crawling the web to obtain personal data, particularly from social networks or mining datasets published by networking sites.

In the following, we will review privacy disclosure issues in social networks and major means of risks and attacks. A brief summary of the privacy disclosure issues, misusage, and common private information gathering methods is shown in Table 1.

### 2.1 Privacy Disclosure Issues

When creating a profile in a social network, especially the one like Facebook where users are encouraged to provide real data, personal information is at risk. As the study in [2] reveals, users are happy to share personal information: more than 90 % of users uploaded a clear and identifiable picture to their profile, more than 50 % had their current address and almost 40 % had their phone numbers. Users might want certain information to be seen by a close circle, but not by strangers or vice versa. They might also want people who know them well, being kept away from their information. Current privacy models in social networks have been criticized because there is a disconnection between users believed privacy settings and what is in fact happening to their data [32]. Researchers have also concluded that privacy policies and privacy settings are hard to understand for the general social networks members. As a consequence, privacy protection choices are oftentimes poorly selected.

Plenty of controversy has generated the fact that employers began requesting social network credentials from their applicants or current employees. Several states including California, Illinois, Maryland, Michigan, Missouri, New York, Minnesota, South Carolina and Washington have passed legislations protecting the rights of the employees to keep privacy on some parts of their online profile [47]. Some schools have also been involved in similar discussions for trying to control students social networks accounts. A simple joke from a friend posting and tagging an awkward picture could leave social media users exposed. Not only credentials have been requested by employers but also deletion of social media accounts and addition of human resources director as “friend” [43]. Even though social networking has radically changed the definition of privacy, with more personal information being made public, situations like this undermined social sites members privacy expectations.

### 2.2 Privacy Attack Issues

All this profusion of information could potentially be a target for privacy breach type of attacks. These attacks can come from three main sources: users' so called friends (other users within the network), third party applications, and service providers.

**Re-identification and De-anonymization.** Anonymization is one of the common techniques for user privacy protection. The idea of anonymizaiton is to strip the data from all attributes that might identify an individual. For example, demographic information, names or social security. This process of anonymization has often been considered a synonym of privacy and it is usually referred to as personally identifiable information removal [44].

When collected data can be linked to a person or an individual, it is called re-identification. To anonymize data, a social network is assumed to be a graph and transformations are applied to achieve privacy preservation. Assuming a social network to be a graph has many advantages but also has some disadvantages. For example, a graph behavior can be modeled by using analytical tools. Link prediction is one of the tools that can be used for modeling and prediction of graphs evolution over time. Combining link prediction with de-anonymization algorithms could be a channel to re-identification.

Anonymised information from social networks is being shared with advertisers and other businesses which expose users' data to re-identification. Several de-anonymization techniques have been recently discussed in the literature [44–46]. An attacker could create several accounts in a social network which share a link pattern among them and connect them to target users. It would be very easy for the attacker to identify his/her accounts and the target account after anonymization. A study presented in [46] showed that knowing someones group membership in a social network is enough to identify that person. Furthermore, the authors in [44] presented a class of de-anonymization algorithms that with minimum background information, an attacker is able to identify a persons record in an anonymized dataset with a high accuracy. These algorithms include three main parts: a scoring function to measure how well a record from a non-anonymized dataset (background knowledge from social network users) matches a record from the anonymized dataset; a matching criterion which is an algorithm to decide based on the results of the scoring function, if there is a match between records; and record selection that selects a "best guess" record if necessary [44].

**Phishing.** Phishing is a well-known form of social engineering. These attacks involve a perpetrator impersonating a trusted party with the goal of obtaining users private information such as passwords, credit card numbers, and social security numbers. These attacks have generalized ways of luring victims into accepting, for example, a request from a popular banking business, but generally almost no information is known about the receiver. However, when phishing is combined with elements of context, it reaches incredible high success; as it has been studied, it becomes four times more effective [40]. With the massive amounts of data available from social networks, context aware phishing can be dangerously increased. Users leave behind trails of information such as likes on Facebook, stories and videos posted and tweets. A smart fisher can exploit all these elements to increase the yield of an attack.

**Is My "friend" a Threat?** In social networks, communication between friends is facilitated. Unless a profile is completely open for everyone, only friends of the user have access to view his/her personal information. However, in [2], Acquisti and Gross noted how the word friend has a different meaning in the online and offline context. While offline relationships are extremely diverse in terms of how close a relation is perceived to be, we only have simplistic binary relations online: friends or not. As a consequence, a friend in a social network could perfectly be someone who we would not consider friends offline. Therefore, befriending users in online social networks could open a door for stealing information.

Privacy attacks coming from friends have been presented in [36]. The authors present what is called same-site and cross-site profile cloning. In a same-site profile cloning attack, the perpetrator creates a duplication of a users profile within the same network with the goal of befriending the victims friends. Because the request comes from a known person, the victims contacts are likely to accept and expose their personal information to the perpetrator. A more vicious attack is cross-site cloning because it raises less suspicion. The perpetrator knows a user and his friends from network A and creates a duplicate profile in network B where the user is not registered. Friendship requests are then sent to the users friends who also have a profile in network B. User awareness is crucial to avoid these attacks.

**Malicious Third Party Applications.** Third party applications provide online social network users with additional functionality, for example, games and horoscope. They are extremely popular and most users take advantage of them. While these applications are built using the social network API and oftentimes reside on the platform, a different company develops them thus; they are considered untrusted [39]. Careless and naive users are perfect victims for malicious third party applications; a well-known example is the Facebook worm "Secret Crush" [37]. Targeted users received a message saying that someone had a crush on them; to reveal the identity of the crush, users had to forward the invitation to five of their contacts and install an application called "Crush Calculator" that was in fact spyware. Meanwhile, there are applications that access users public and private attributes to perform their intended functionality; a restaurant recommender application must have users current location or a horoscope application must have users birth date. Oftentimes, users are unaware of the usage of their private information by third party applications.

In recent news [38], Facebook decided to take action on the way third-party apps published stories to the News Feed, without explicit action from the users.

According to the Facebook website: “Weve also heard that people often feel surprised or confused by stories that are shared without taking an explicit action”.

**Social Networking Service Providers.** When users upload their information to a social network, they are trusting the company (or service providers) to protect their privacy. However, it is known that online networking business profit from sharing their members information [30] therefore, there is a fine balance between securing members privacy and distributing their data to advertisers. Meanwhile, poor software engineering practices offer hackers the opportunity to access private data. As it was published in December 2011 [41], a bug on the “reporting flows” of Facebook caused Mark Zuckerbergs private pictures being leaked.

**Table 1.** Privacy disclosure and misusage (left column) and common private information gathering methods (right column).

| Privacy disclosure | Privacy attacks |
|---|---|
| Improper use of disclosed information | Re-identification and de-anonymization |
| Hiring discrimination | Context aware Phishing |
| School admittance discrimination | Information leakage from friends |
| | Malicious third-party applications |
| | Attacks to social network providers |

## 3 Privacy Evaluation and Measurement

With the popularity of online networking sites and the many concerns that have been discussed in regards to privacy issues, one fundamental challenge is *how to measure, evaluate and guarantee privacy and security in online social networks.*

A practical way for privacy evaluation is one of the steps to empower users to a better and robust information protection as well as a powerful method to make users attentive of how their privacy will be exposed, when certain data is posted online or when they make changes to their privacy choices. Two main approaches have been followed to pursue this goal. The first approach takes as the main component the existing privacy options already provided by the networking sites [6]. The second methodology aims to create an index that is in indication of good or bad privacy [3–5]. Both approaches have its advantages and disadvantages. A benefit of fine tuning existing privacy settings is that, since they are already part of the networking sites, with some assistance offered to users, they could become part of their everyday practice. However, it has been demonstrated that users tend to not change default settings [2,7]. In addition, recent surveys suggest that users often have no knowledge about these settings or have a strong perception of complexity that in many cases is justified. On the other hand, methods for privacy index creation go further than suggesting ways of better hiding information by taking into account relationships between actors and attributes as well as predictive power of combinations of attributes. However, several of the magnitudes used for calculations and formulations come from very subjective areas such as users perception of an attributes influence on privacy and are not very accessible to the general users population.

### 3.1 Privacy Setting Recommendation

Recommending well informed and carefully selected privacy settings for online social networks, has been proposed by researchers. For example, as of March 2013, Facebook reported 1.11 billion users whose profile information is set to be shareable/accessible with friends, friends of friends, and very often, the rest of the public. By default, privacy settings of users accounts on Facebook are open to everyone searches, inside and out of Facebook. Furthermore, research has demonstrated that not only users in general are more likely to leave default settings as is [7] but also, that a small number actually change default privacy preferences on Facebook [2].

One of the first known intents of aiding users with privacy choices was Reclaim.org. The company offered an open source application which worked as a scanner of Facebook members privacy settings [9]. After downloading the application, it would evaluate the accounts privacy selections showing what settings had been securely configured as well as what information was available to the public; it would also make recommendations to enhance privacy selections. The Green Safe is an application that was created to keep Facebook members data out of Facebooks control [10]. Users data is imported into the application, and subsequently, deleted from Facebook. Friends are still able to access the information but it will be hidden from third party applications and partner sites. The Green Safe mines users profiles for targeted advertising, yet the privacy policy ensures that the company will not “share, trade or sell your information with anyone”.

### 3.2 Machine Learning Techniques for Setting Recommendation

An interesting idea that has not been extensively researched is the usage of recommender systems. This type of systems would recommend privacy choices by establishing links between members that have been found to share similar privacy preferences.

Specifically, the work made in [6] uses machine learning as the basis for a recommender system. The authors in [6] created a training dataset which includes attributes from users profile (for example, name, work experience and time zone), interests (such as communities and groups), privacy settings on photo albums and privacy settings on posts.

Surveys conducted by Westin [13] have assisted researches in classifying online network members into three groups based on their privacy concerns: High and Fundamentalist, Medium and Pragmatic, Low and Unconcerned. Fundamentalists refer unwillingness to provide data on websites and go to extremes to avoid revealing any type of personal information. Pragmatics are described as willing to share personal information if they find it being beneficial. Unconcerned users have no problem revealing personal information upon request as well as not having concerns with their privacy. By analyzing users attitude towards sharing their photo albums and posts, a model can be trained to classify members as one of the above mentioned categories (Fundamentalist, Pragmatic, and Unconcerned). This categorization process creates another attribute called privacy_category which is the class label given to a user based on their privacy choices. A standard decision tree was used to infer the privacy_category of the users selected for the training dataset. When a new user joins a social network (Facebook was used as the platform for the study) a $k$-nearest neighbor classifier would determine the privacy_category for the user. Based on the characteristics of the predicted class, the application recommends which attributes should be disclosed and which ones should be hidden. An application with this type of feature would provide an improvement to privacy settings rather than leaving them completely open which is the default.

### 3.3 PrivAware and Privometer

In 2010, Facebook provided a software environment intended for third-party developers to create their own applications that access Facebook members information. Numerous applications have been developed using this platform, such as games, information sharing, social causes promotion and privacy protection. Two interesting examples of these applications designed for privacy protection are PrivAware [11] and Privometer [12].

PrivAware [11] was designed based on a basic principle that information should be protected from escaping its intended boundaries. Therefore, PrivAware assists users quantifying privacy risks associated to friend relationships in Facebook. Specifically, PrivAware deals with the attributes inference problem. It has been shown by studies [14–16] that even if a social network member is cautious towards privacy, certain attributes can be inferred based on the values of those of his/her friends; for example political view and affiliations.

PrivAware methodology to the inference reduction problem is: given a set of friends and a privacy requirement represented as the maximum acceptable number of predictable attributes, find the maximum set of friends that fulfills the privacy requirement. PrivAware applies a basic algorithm for attribute inference: given an attribute, the algorithm finds its most popular value among the users friends; this value is assigned to the user if the number of friends sharing this attribute surpasses a previously selected threshold. PrivAware then gives users the choice of either delete unsafe friends, partition friends into groups and apply access control (set risky group to invisible) to each group or "contaminate" his/her friends network with users who do not share common attributes with the target user. The second approach is more desirable since users are not likely to remove friends particularly those who are more similar to them or pollute their network and create confusion among desirable contacts. From the results of collecting data from PrivAware, the authors showed that 59.5 % of the time attributes were correctly inferred based on users social contacts. Also, their heuristic approach to friends removal or grouping for privacy preservation was 19 less than the baseline (removing contacts at random).

Following a similar principle as PrivAware, but with more extended functionality, Privometer [12] is presented as a privacy protection tool that measures the extent of information revelation in a user profile and suggests self-sanitation activities to control the amount of leakage. At the time Privometer was presented, it was the "first functional prototype of a privacy measuring tool to be implemented on a social network" [12]. It provides users with an insight on how a malicious application that could be installed in a contacts profile can access beyond public profile information. Privometer works under the assumption that a third-party application installed in a contacts profile runs an attribute inference algorithm using one of the most popular inference models. Privometer determines the amount of information leakage using some renowned inference models to identify the one that causes the most damage to users privacy. The final leakage value is derived from combine probability of inference. Users are then presented with a graphical measurement of their privacy, a ranking of friends based on their individual contributions to information revelation and actions for remediation. The actions suggested by Privometer are in addition to the privacy settings already provided by Facebook and range from requesting a contact to hide specific attributes to deleting a contact.

### 3.4 Privacy Index

Quantifying and measuring privacy can be very challenging, mainly because the definition of privacy is very subjective and each individual might have a different opinion about this concept. In 2013, Yong Wang *et al.*, [3–5] proposed to use privacy index (PIDX) to quantify privacy. For the authors, privacy can be assessed based on three metrics: known attributes, their sensitivities, and visibilities. Furthermore, they consider that a combination of attributes may also compromise users privacy; combinations of attributes are called virtual attributes. Based on these assumptions, three privacy measurement functions are discussed and evaluated: weighted privacy measurement function, maximum privacy measurement function, and composite privacy measurement function. Three privacy indexes were further created on the privacy measurement functions: weighted privacy index ($w$-PIDX), maximum privacy index ($m$-PIDX) and composite privacy index ($c$-PIDX).

To reflect the sensitivity of an attribute, a privacy impact factor is assigned to each of them. For full privacy disclosure the value of the impact factor is 1 and it is calculated as a ratio of its privacy impact to full privacy disclosure. A larger numbers indicate that the information is more sensitive. Probabilities are also used to describe attributes visibility. An unknown attribute would have visibility of 0, for a known attribute it is 1 and values between 0 and 1 represent partial disclosure.

Let $(L, S, V)$ represent the set of actors' complete attribute list, their privacy impact and visibilities, respectively.

$$L = (a_1, a_2, \ldots, a_n) \qquad S = (s_1, s_2, \ldots, s_n) \tag{1}$$

$$V = (p_1, p_2, \ldots, p_n) \tag{2}$$

For the purpose of this experiment, $p_i = 1$ $(1 \leq i \leq n)$

Let $(L_k, S_k, V_k)$ represent and actors complete attribute list, their privacy impact and visibilities.

$$L_k = (a'_1, a'_2, \ldots, a'_m) \qquad S_k = (s'_1, s'_2, \ldots, s'_m) \tag{3}$$

$$V_k = (p'_1, p'_2, \ldots, p'_m) \tag{4}$$

- Weighted Privacy Measurement Function and Weighted Privacy Index (w-PIDX)

$$f_w(L_k, S_k, V_k) = p'_1 + p'_2 + \ldots + p'_m = \sum_{i=1}^{m} p'_j s'_j \tag{5}$$

$$w - PIDX = \frac{f_w(L_k, S_k, V_k)}{f_w(L, S, V)} * 100 = \frac{\sum_{i=1}^{m} p'_j s'_j}{\sum_{i=1}^{n} s'_j} * 100 \tag{6}$$

- Maximum Privacy Measurement Function and Maximum Privacy Index (m-PIDX)

$$f_m(L, S, V) = max(p'_1 s'_1 + p'_2 s'_2 + \ldots + p'_m s'_m) = \sum_{i=1}^{m} p'_j s'_j \tag{7}$$

$$w - PIDX = f_m(L_k, S_k, V_k) * 100 = max(p'_1 s'_1 + p'_2 s'_2 + \ldots + p'_m s'_m) * 100 \tag{8}$$

- Composite Privacy Measurement Function and Composite Privacy Index ($c$-PIDX)

$$f_c(L, S, V) = f_m(L_k, S_k, V_k) + (1 - f_m(L_k, S_k, V_k)) = \frac{f_w(L_k, S_k, V_k)}{f_w(L, S, V)} \tag{9}$$

$$w - PIDX = f_c(L_k, S_k, V_k) * 100 \tag{10}$$

As shown, $w$-PIDX is a centrality measure useful for measuring attribute incremental changes, although it is not useful for privacy ranking. However, this is not the case with $m$-PIDX, which is good to measure privacy relative value but not incremental changes. Based on their experiments, the authors selected $c$-PIDX as the most accurate and complete measure of privacy for a social network actor.

Previous works in privacy indexes [17,18] are mainly based on the item response theory (IRT). Although IRT is a powerful tool, it is designed based on three assumptions: users are independent, items are independent, and users and items are independent. In reality, these assumptions do not apply very well to real-world social networks. The work in [18] goes to the extent of assuming independence between attributes without considering attributes underlined relationships. This represents a problem as it has been confirmed by [19,20] that combination of attributes may harm users privacy since it can lead to the inference of unknown attributes.

A brief summary of the privacy measurement and evaluation is shown in Table 2.

**Table 2.** Privacy measurement and evaluation

| Measurement or Evaluation | Detail |
|---|---|
| Privacy settings recommendation | PrivAware, Privometer |
| | Machine learning techniques to recommend attributes based on similar users height |
| Privacy index | Weighted Privacy Index ($w$-PIDX) |
| | Maximum Privacy Index ($m$-PIDX) |
| | composite privacy index ($c$-PIDX) |

## 4 Conclusion

In this paper, we discussed two important topics, privacy issues, and privacy measurement and evaluation, in online social networks. Large amounts of personal related content have become accessible over the internet via online social networks. While users enjoy connecting with friends and family, concerns over privacy are becoming an increasing important factor. Advances in information retrieval and data analytics provide adversaries with almost unlimited access to the plentiful personal information on the web. We have seen different types of attacks against users privacy, and how with a small portion of information, attackers are able to connect users online persona, to the real life individual. Due to all these concerns, security and privacy must be quantified and evaluated. This paper has shown studies aimed to measure privacy. Some applications have been built that can be integrated with networking sites such as Facebook with the goal of assisting users to evaluate their current privacy choices and recommend settings for maximum protection. An equally important question about the privacy concerns is the measurement and the quantification of the privacy, and we have discussed three privacy measurement in the paper. Our research shows that not much has been implemented and passed along to users. Although social networking companies offer some form of privacy settings, there is a great interest in sharing users data for profit. As a result, it becomes users' responsibility to be knowledgeable and be aware of every decision they make when networking online.

## References

1. Bilge, M., Strufe, T., Balzarotti, D., Kirda, E.: All your contacts are belong to us: automated identity theft attacks on social netorking. In: Proceedings of the 18th International World Wide Web Conference, Madrid, Spain. ACM (2009)
2. Gross, R., Acquisti, A.: Information revelation and privacy in online social networks. In: Proceedings of ACM Workshop on Privacy in the Electronic Society, pp. 71–80, November 2005
3. Kumar, R.N., Wang, Y.: SONET: a SOcial NETwork model for privacy monitoring and ranking. In: Proceedings of the 2nd International Workshop on Network Forensics, Security and Privacy (2013)
4. Wang, Y., Nepali, R.K.: Privacy measurement for social network actor model. In: Proceedings of the International Conference on Social Computing, pp. 659–664 (2013)
5. Wang, Y., Nepali, R.K., Nikolai, J.: Social network privacy measurement and simulation. In: Proceedings of the International Conference on Computing, Networking and Communications (ICNC) pp. 802–806 (2014). doi:10.1109/ICCNC.2014.6785440
6. Ghazinour, K., Matwin, S., Sokolova, M.: Monitoring and recommending privacy settings in social networks. In: Proceedings of the Joint EDBT/ICDT 2013 Workshops, pp. 164–168. ACM (2013)
7. Mackay, W.: Triggers and barriers to customizing software. In: Proceedings of CHI 1991, pp. 153–160. ACM Press (1991)
8. Duffany, J., Galban, O.: Hacking Facebook Privacy and Security. Polytechnic Univ. of Puerto Rico San Juan (2012)
9. Shimel, A.: Reclaim your privacy from facebook. PCWorld. Network World, 19 May 2010
10. Perez, S.: New App Helps Keep Facebook's Hands Off Your Data. Readwrite. N.p., 10 May 2010
11. Becker, J.L.: Measuring privacy risk in online social networks. ProQuest, UMI Dissertations Publishing (2009)
12. Talukder, N., Ouzzani, M., Elmagarmid, A., Elmeleegy, H., Yakout, M.: Privometer: privacy protection in social networks. In: 2010 IEEE 26th International Conference on Data Engineering Workshops (ICDEW), Long Beach, CA (2010)
13. Kumaraguru, P., Cranor, L.F.: Privacy indexes: a survey of westins studies. Technical report CMU-ISRI-5-138, Carnegie Mellon University, CMU, Pittsburgh, PA, USA, December 2005
14. Staddon, J., Golle, P., Zimny, B.: Web-based inference detection. In: SS 2007: Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium, pp. 1–16. USENIX Association, Berkeley (2007)
15. Macskassy, S.A., Provost, F.: Classification in networked data: a toolkit and a univariate case study. J. Mach. Learn. Res. **8**, 935–983 (2007)
16. Neville, J., Jensen, D.: Leveraging relational autocorrelation with latent group models. In: Proceedings of International Workshop on Multirelational Mining, pp. 49–55 (2005)
17. Maximilien, E.M., Grandison, T., Sun, T., Richardson, D., Guo, S., Liu, K.: Privacy-as-a-Service?: models, algorithms, and results on the facebook platform. In: Web 2.0 Security and Privacy Workshop (2009)
18. Liu, K.U.N.: A framework for computing the privacy scores of users in online social networks. ACM Trans. Knowl. Disc. **5**(1), 1–30 (2010)

19. Sweeney, L.: Uniqueness of simple demographics in the U. S. population. Data privacy Lab white paper series LIDAP-WP4 (2000)
20. Golle, P.: Revisiting the uniqueness of simple demographics in the US population. In: Proceedings of the 5th ACM Workshop on Privacy in Electronic Society. ACM (2006)
21. Boyd, D., Ellison, N.: Social network sites: definition, history, and scholarship. J. Comput. Med. Commun. **13**(1), 210–230 (2008)
22. Warren, S., Brandeis, L.: The right to privacy. Harvard Law Rev. **4**(5), 193–220 (1890)
23. Westin, A.: Privacy and Freedom. Athenaeum, New York (1967)
24. Yang, Y., Lutes, J., Li, F., Luo, B., Liu, P.: 26 Stalking online: On user privacy in social networks. Paper presented at the 37-48 (2012). doi:10.1145/2133601.2133607
25. Backstrom, L., Dwork, C., Kleinberg, J.: Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography. In: Proceedings of ACM International Conference on World Wide Web, pp. 181–190 (2007)
26. Hay, M., Miklau, G., Jensen, D., Towsley, D., Weis, P.: Resisting structural re-identification in anonymized social networks. Proc. of VLDB Endow. **1**(1), 102–114 (2008)
27. He, J., Chu, W.W.: Protecting private information in online social networks. In: Chen, H., Yang, C.C. (eds.) Intelligence and Security Informatics, vol. 135, pp. 249–273. Springer, Heidelberg (2008)
28. He, J., Chu, W.W., Liu, Z.V.: Inferring privacy information from social networks. In: Mehrotra, S., Zeng, D.D., Chen, H., Thuraisingham, B., Wang, F.-Y. (eds.) ISI 2006. LNCS, vol. 3975, pp. 154–165. Springer, Heidelberg (2006)
29. Liu, K., Terzi, E.: Towards identity anonymization on graphs. In: Proceedings of the 2008 ACM SIGMOD, pp. 93–106 (2008)
30. Chen, X., Michael, K.: Privacy issues and solutions in social network sites. IEEE Technol. Soc. Mag. **31**(4), 43–53 (2012). doi:10.1109/MTS.2012.2225674
31. Austin, L.: Privacy and the question of technology. Law Philos. **22**, 119–166 (2003)
32. Tierney, M., Subramanian, L.: Realizing privacy by definition in social networks. In: Proceedings of 5th Asia-Pacific Workshop on Systems (APSys 2014) (2014)
33. Chen, X., Shi, S.: A literature review of privacy research on social network sites. In: Proceedings of International Conference on Multimedia Information Networking and Security (MINES), vol. 1, pp. 93–97, November 2009
34. Joshi, P., Kuo, C.-C.: Security and privacy in online social networks: a survey. In: 2011 IEEE International Conference on Multimedia and Expo (ICME), pp. 1–6, July 2011
35. Zhang, C., Sun, J., Zhu, X., Fang, Y.: Privacy and security for online social networks: challenges and opportunities. IEEE Netw. **24**(4), 13–18 (2010)
36. Bilge, L., et al.: All your contacts are belong to us: automated identity theft attacks on social networks. In: Proceedings of the 18th International Conference World Wide Web (WWW 2009), pp. 551–560. ACM Press (2009)
37. Mansfield-Devine, S.: Anti-social networking: exploiting the trusting environment of Web 2.0. Netw. Secur. **11**, 4–7 (2008)
38. King, R.: Facebook dials back on third-party app shares, 27 May 2014. http://www.zdnet.com (retrieved)
39. Gao, H., Hu, J., Huang, T., Wang, J., Chen, Y.: Security issues in online social networks. IEEE Internet Comput. **15**(4), 56–63 (2011). doi:10.1109/MIC.2011.50
40. Jagatic, T.N., et al.: Social phishing. Commun. ACM **50**(10), 94–100 (2007)

41. Duell, M.: Mark Zuckerbergs private Facebook photos revealed: Security glitch allows web expert to access billionaires personal pictures. The Daily Mail (MailOnline), December 2011. http://www.dailymail.co.uk/news/article-2070749/Facebook-security-glitch-reveals-Mark-Zuckerbergs-private-photos.html
42. Valdes, M., McFarland, S.: Employers Ask Job Seekers for Facebook Passwords. Associated Press, 20 March, 2012
43. Vijayan, J.: New laws keep employers out of worker social media accounts. Computer World, 4 January 2013. http://www.computerworld.com/article/2505609/data-privacy/ill-bans-firms-from-asking-workers-job-seekers-for-social-media-info.html
44. Backstrom, L., Dwork, C., Kleinberg, J.: Wherefore Art Thou r3579x?: anonymized social networks, hidden patterns, and structural steganography. In: Proceedings of the 16th International Conference on World Wide Web (WWW 2007), pp. 181–190. ACM Press (2007)
45. Narayanan, A., Shmatikov, V.: De-anonymizing social networks. In: Proceedings of the 20th IEEE Symposium on Security and Privacy (SP 2009), pp. 173–187. IEEE CS Press (2009)
46. Wondracek, G., et al.: A practical attack to de-anonymize social network users. In: Proceedings of IEEE Symposium on Security and Privacy (SP 2010), pp. 223–238. IEEE CS Press (2010)
47. Vijayan, J.: Ill. Bans firms from asking workers, job seekers for social media info. PCWorld. ComputerWorld, 7 August 2012
48. Barnes, S.B.: A privacy paradox: social networking in the United States. First Monday, 4 September 2006. http://firstmonday.org