1. Introduction

The security of private information of users online is a critical topic, particularly since social networking applications became popular. According to Cutillo et al. [1], beyond the usual vulnerabilities that threaten any distributed application over the internet, online social networks raise specific privacy concerns due to their inherent handling of personal data.

The definition of social network site given in Boyd and Ellison [2] was a web based service that creates connections between users and their profiles in a bounded system. As Gross and Acquisti [3] proposed, social networking sites (SNS) can be separated into nine types: business, common interests, dating, face-to-face facilitation, friends, pets, and photos. According to this classification, social network sites include online shopping sites and e-government sites. Facebook spans several types: common interests, friends, and photos. Overall, it can be classified as a “friends”-oriented social network site. QQ, the number 1 ranking chat software in China, can be classified as “face-to-face facilitation”. Using QQ, people can communicate by typing, by audio and using video.

Most SNS ask users to create a profile so that contacts can be made for additional purposes. As some private information is used to create a profile, the security of private information on SNS has become an increasingly important topic.

The development of the internet saw changes to the definition of privacy. The definition of privacy by Warren and Brandeis [4], “the right to be let alone” was traditionally cited as a synonym for privacy until the rise of the online environment when its shortcomings became apparent. As a well accepted definition of privacy, Westin [5] held the opinion that privacy is the right to keep the disclosure of personal information safe from others.

The boom of the internet and the explosion of new technologies have brought with them new challenges and thus new connotations of privacy. Clearly, when people deal with e-government and e-business, they do not only need the right to be let alone, but also to be let in secret. Not only do they need freedom of movement, but also to be assured of the secrecy of their information. Solove [6] has critiqued traditional definitions of privacy and argued that they do not address privacy issues created by new online technologies. Austin [7] also asserts: “[w]e do need to sharpen and deepen our understanding of traditional concerns regarding privacy in order to respond to these new situations”.

The relationship between privacy and the use of SNS is subtle. Generally, people would like personal information to be known by a small circle of close friends and family, and not by total strangers. In some
instances, people choose to reveal particular personal information to strangers, but choose not to share it with people who know them well [8], [3]. In either case, users’ information disclosure can be helpful to other users, companies and third parties. Private information is particularly valuable when the information of many people in a group is gathered on SNS [9] and aggregated.

There are two main methods of information gathering: (i) an information leak based on privacy disclosure; and (ii) an information leak based on attack techniques. Privacy disclosure refers to those information users who voluntarily publish their personal information online. This data may be contained in profiles and information exchanged between one or more people. Attack techniques steal private information that users wish to keep secret. Figures 1 and 2 show the two categories of privacy invasion.

![Fig. 1. Means of privacy invasion on SNS](image1)

![Fig. 2. Basic instance of privacy invasion](image2)
2. Information leak caused by privacy disclosure

Privacy disclosure refers to any personal information a user may willingly provide to a website. Websites employ a variety of online collection techniques, including collecting e-mail addresses from list servers, chat rooms, and forming news groups to induce users to disclose personal information.

The topic of harvesting and selling user data has been debated since the establishment of business-to-consumer (B2C) bricks-and-click and click-only companies. Some companies have been criticized for using information collected from consumers in the online purchase industry for marketing purposes. Some of these companies include America Online for attempting to sell subscribers' telephone numbers and Intel for developing the new Pentium chip that identifies users [10].

Even more controversial is harvesting users' personal information requested on SNS which can be deemed highly sensitive given the nature of making online “friends”. According to Caudill and Murphy [10], personal information exposed online encompasses both public information such as a driver’s license, mortgage information and private information such as income. The demarcation between what is considered private information and what is considered public information is shifting. This has allowed some personal information to find its way onto the public domain. With development of the internet, the public portion of private information is growing and consumer information is being gathered and disseminated more easily.

2.1 Ways to acquire private information

- Collect registration information

Clients have to enter information to register for an online service. There are some optional field entries, but some fields are required. Though this data collection is commonly claimed to be for improving service delivery, often the data is used for other purposes [11].

- Trace user’s IP

According to TCP/IP protocol, data packets transferred between PCs contain an IP. By checking the IP, the host computer can infer a client’s position and denote whether they are online.

- Search track record in cookies

A cookie is a profile created in a Client PC by a Server, which conserves page views, the access time and network settings of clients. Searching clients’ information in cookies, hosts can explore internet use patterns of clients.

2.2 Improper use of disclosed privacy information

There are two main uses of user information: (i) business and (ii) marketing.

- Doing business with users’ information

Businesses profit from user information. A well-known example of doing business with users’ information is the alleged selling of email addresses by the network operating company Gratis Internet.

- Doing marketing with users’ information

Online merchants can also increase business by doing marketing research and advertising based on the availability of information about users [10]. If consumers disclose an email address or telephone number in their “public” profile, they will likely receive annoying commercial emails and phone calls. This invades the privacy of the consumer and causes unfair competition to sellers who do not abuse consumers’ personal information.

2.3 Achieving privacy protection against information leaks based on privacy disclosure
Most online service organizations ask for registration with some personal information, and users seemingly have no choice but to provide sensitive information. But users are not entirely helpless. Various ways do exist for users to safeguard their privacy from online organizations that insist on the collection of personal details for access to a given service.

Various approaches for protecting privacy are recommended, such as market regulation, self-regulation and mandatory government rules [12].

- **Market-regulation**

  According to Swire and Litan [12] media stories play an important role in broadcasting privacy practices of different companies. As users become more aware, they can affect privacy behavior. Sheehan and Hoy [13] point out that as “… privacy concern increased, respondents reported that they were more likely to provide incomplete information to web sites, to notify Internet Service Providers … about unsolicited e-mail, to request removal from mailing lists, and to send a flame to online entities sending unsolicited e-mail. Additionally, as privacy concern increased, respondents reported that they were less likely to register for web sites requesting information.”

  Companies who are serious about maintaining user privacy have begun to promote their practices as a means to encourage, attract and retain customers. Yet there are well-known companies that have questionable privacy practices who will experience sizeable loss of business.

- **Self-regulation**

  Self-regulation is based on the three traditional components of government - legislation, enforcement, and adjudication – but in self-regulation these functions are carried out by the private sector. Legislation refers to the question of defining the appropriate rules, enforcement refers to the initiation of an enforceable action when the rules are broken, and adjudication to whether or not a company has violated the privacy rules [14].

  Though self-regulation is showing great promise in the USA, the Federal Trade Commission found that though more than 85% of websites collect personal information from consumers, only 14% provide any notice with respect to their information practices, and approximately 2% provide notice by means of a comprehensive privacy policy [15].

- **Mandatory government rules**

  In the European Union, there is an emerging trend toward the use of legal action by government to keep organizations in check. Four features of the laws about privacy and data protection in the EU are discussed by Cate [16]. He said: “Typically they apply to both public and private sectors; they apply to a wide range of activities, including data collection, storage, use, and dissemination; they impose affirmative obligations (often including registration with national authorities) of anyone wishing to engage in any of these activities; and they have few, if any, sectoral limitations - they apply without regard to the subject of the data.” Data collection by companies in the EU must meet four constraints. According to Caudill and Murphy [10]:

  “[f]irst, a company should have a legitimate and clearly defined purpose to collect information. Second, that purpose must be disclosed to the person from whom the company is collecting information. Third, permission to use information is specific to the original purpose. Fourth, the company can keep the data only to satisfy that reason; if the company wants to use the information for another purpose, it needs to initiate a new information collection and use process.”

  Despite the success of some government regulations, some writers contend that government should not stand in the way of market regulation, and government intervention may disturb the invisible hand of market forces [12]. But every approach has advantages and disadvantages. Through market and self-regulation, companies can be selected naturally by users. But when it comes to monopolistic companies, such as Amazon and iTunes, users do not have much choice. These companies were first movers providing...
users with new online services, and maintain a high level of market share. They offer value to consumers which some consumers feel they cannot forgo, despite the obvious privacy risks.

Mandatory government rules are necessary given that in some instances neither market regulation nor self-regulation will work.

Fig. 3. Regulation mechanism of data transfers

3. Information leaks caused by attack techniques

It is not enough to rely on disclosure by information users to cause an information leak. Attack techniques can also be used to get information that may otherwise be considered private.

A particular advantage of the internet is its ability to collect real-time behavioral data which are easily accessed through the use of cookies. “Social network users don’t think of themselves as part of a group so much as individuals, so there is a persistent belief among users that none would bother attacking them”[9].

Security company iDefense tracks down those who attack these sites, to find out what they are after. “It is client information,” says Rick Howard, the company’s Director of Intelligence, “We’re seeing a lot of user ID and passwords for Facebook and other sites. They’re doing data mining on those credentials” [9].

To obtain an abundance of information for data mining, it is not enough to rely on users’ careless attitudes toward disclosing personal information, so various techniques employed to attack social network sites are developed to catch easy prey.

3.1 Data mining techniques used on SNS

Data mining is the process of extracting hidden patterns from data. Through the process of data mining, fragments of users’ information can be brought together and integrated. It is possible to build a complete personal file of a user, including their individual social security number or credit card numbers. The status of data mining in social networks has been addressed by scholars such as Chakrabarti [17] and Getoor [18]. There are also some improved data mining techniques that are an ideal fit in the social networking context [19]-[22]. Alist and Song [21] uncovered interaction patterns in business processes from event logs by combining concepts from workflow management and social network analysis. Mika [22] identified Flink (created by Flink Labs), which employs semantic technology for reasoning with personal information extracted from a number of electronic information sources including web pages, emails, publication archives and “friends of a friend” (FOAF) profiles.
It is meaningless to some extent to discuss whether or not it is legal to conduct data mining of personal information if a business has made customers aware of the collection of personal data in their disclosure statement. The illegality of attack techniques is much clearer.

3.2 Attack techniques

As Roy Hills, technical director at NTA Monitor said, "Attackers are creating websites in which they embed malicious code to track a visitor's searches, user names and passwords. The code can affect a visitor's PC without their knowledge and can quickly spread to other visitors' machines" [23]. Users of social network sites could be attacked in two ways: (i) an attack directly on the websites or PC systems of users, or (ii) certain malicious applications that users are deceived into downloading.

3.2.1 Direct attack techniques

The most common attack techniques referred to in the literature include a Distributed Denial of Service (DDOS) [24][25] and the Sybil Attack [26]. There are also articles about the feasibility of performing such attacks [27][28].

The DDOS attempts to make a web resource unavailable to other applicants by delivering huge amounts of application requests simultaneously.

The Sybil attack was widely used in peer-to-peer networks, making a node illegitimately claim multiple identities (the identity either completely fabricated or stolen). One of the purposes of performing a Sybil attack is to disarrange the reputation system in the SNS. By creating a large number of Sybil nodes that collude, the attacker artificially increases his rating.

3.2.2 Malicious applications

While direct attacks depend mainly on complicated techniques, malicious applications partly depend on the carelessness of users. Mansfield-Devine [9] cited a well-known infringement called the “Secret Crush” worm on Facebook, in which each victim received a message saying that someone online had a secret crush on them. In order to find out the alleged identity of the individual, the user needed to pass on the invitation to five of their friends and install an application-software named “Crush Calculator” which was in fact a Zango application, in this instance spyware.

Mostly, users are deceived into downloading malicious applications. The two best ways to achieve that are:

1. For the purpose of embodying public participation, social network sites allow, sometimes encourage, users to upload client-side JavaScript made by themselves [8][9]. Sometimes the JavaScript is a small game, sometimes it is a small test, and sometimes it is a virus.

2. The well-known deception of phishing online, where a phisher pretends to be some trusted organization which is familiar to the user [29]. SNS are the perfect organization that phishers want to pretend to be. The situation is worse when SNS increasingly provide tools and content so that the user cannot distinguish between a trusted application and one that is malicious. It is easy for applications made by phishers to be concealed within an SNS [9].

4. Defense mechanisms

4.1 Defense mechanisms against direct attack techniques

Chen et al. [30] proposed a classification of distributed denial of service defenses. They classified DDOS defense mechanisms into three categories: congestion-based, anomaly-based and source-based. Congestion-based defense mechanisms only react when congestion occurs. "False positives occur when the attack detection algorithm cannot single out the legitimate traffic that contributes to congestion and
false negatives occur when attack traffic does not result in congestion” [30]. Anomaly-based defense mechanisms work when an anomaly is detected. As the monitors are not responsive to all kinds of attacks, anomaly-based defense mechanisms mainly focus on resisting TCP (Transmission Control Protocol) and SYN (Synchronize) attacks. Source-based defense mechanisms are used to detect empty or false source addresses that send out IP packets.

Cheng and Friedman [31], Lai et al. [32] and Feldman et al. [33] proposed defenses against Sybil attacks in reputation systems. They aimed to prevent the Sybil nodes from boosting a malicious user’s rating, not to control the number or size of Sybil groups [34]. Yu et al. [34] present a novel protocol called SybilGuard to restrict Sybil attacks. Users can create lots of identities but not trust relationships. SybilGuard uses this to identify those suspect malicious identities and filter them.

### 4.2 Defense mechanisms against malicious applications

If the web site is not privacy friendly enough for the user, the user might turn away from it and not make any transactions there [12].

Objections include:

a) Privacy policies are too complex for most users to manipulate.

b) User privacy preferences which users should import are often too complex and nuanced, and thus using it would be more of a burden.

c) Users tend to have little experience articulating their privacy preferences.

d) Users are generally unfamiliar with much of the terminology used by privacy experts.

e) Users often do not understand the privacy-related consequences of their behaviors.

Clearly, privacy protection mechanisms need to be designed using human-computer principles with easy manipulation. This will undoubtedly be the most important aspect of developing privacy policies in the future.

Changing the structure of SNS can render ineffective the control malicious applications can otherwise gain. Cutillo et al.[1] build a model of social networking on a peer-to-peer architecture, to avoid scale effect on malicious applications. This acts to restrict the diffusion of malicious applications, although it should be noted that this is not helpful to those users who were initially deceived. But user diligence when using SNS is still the most effective way to escape online attacks.

### 5. Users’ behavior with respect to SNS and privacy

The rapid growth of contemporary SNS has coincided with an increasing concern over personal privacy [35]. These sites “allow individuals to present themselves, articulate their social networks, and establish or maintain connections with others” [36]. The more popular the internet, the more danger to privacy there could be.

Studies in behavioral theory summarize users’ behaviors when private information is at risk. Son and Kim [37] introduced the notion of information privacy-protective responses (IPPR), which is “a set of internet users’ behavioral responses to their perception of information privacy threats that result from companies’ information practices”. There are also studies on techniques and privacy policies [38][39].

### 5.1 Profile creation and information disclosure

Use of one’s real name is a practice strongly encouraged by most SNS, including Facebook.

“Most people don’t bother with different user names and passwords, so if they can figure out what your username and password are on Facebook, there’s a chance that at least a small percentage of those will
be the same for your banking login also” says Rick Howard, Director of Intelligence in iDefense. Even if some people think they have not been that naïve, just as Devine [9] indicated “the average user’s profile contains information like their pet’s name, where they went to school, family details – just the kind of information used for security or ‘lost password’ questions by banking services”.

This is exacerbated because people frequently try to add strangers to their pool of friends on social network sites, more often than not just to increase the number of friends in their profile [40]. Acquisti and Gross [41] found users’ privacy concerns are weak predictors of their membership of the network. Trusting their ability to control their private information, even those with high levels of privacy concern reveal great amounts of personal information on SNS, and, because of the lack of human-centric design, privacy protection techniques and policies are not well employed by users.

5.2 Use of privacy techniques and policies

Most social network sites have privacy setting capabilities and features. Various protections are suggested by scholars [42], [43], although most are not used sufficiently.

Three major problems reduce the use of privacy settings on SNS. First, privacy policy setting is too complicated for users who have no knowledge of which privacy policies to use. Second, it is difficult to design privacy policies for all possible cases. “Lastly, privacy policy setting without considering the privacy-related consequences may cause privacy violations” [38].

Lehikoinen et al. [39] found privacy settings that SNS provide are rarely used and that participants relied mainly on their own judgment in what information they shared and how that was achieved.

Overconfidence in one’s own knowledge and the prevailing disbelief that one could fall victim to attack, make users especially vulnerable in social networks, where they are facing various perils on social network sites. According to cost-benefit theory, there must be reasons good enough to convince users to disclose personal information.

5.3 Reasons for information disclosure on SNS

As there are so many risks perceived by transacting in social networks, some attention should be given to how to deliver private information on the internet. Forman et al. [44] believe that online self-disclosure is driven in part by:

a) The desire for identification with a community, and
b) The need for self-verifying feedback from other community members affirming that one is a member.

Scholars in this area trace this back to the theory of weak ties. Weak ties include friends of a friend, family of a colleague and so on. It refers to the association of two people who do not interact so much but are both familiar with the same brokerage with the relationship as friends or colleagues.

As demonstrated by Granovetter [45], [46] and Burt [47], weak ties are essential to the flow of information that integrates otherwise disconnected social clusters into a broader society. Considering the situation with respect to SNS interaction is a dyadic process and can be maintained if parties involved get more benefit than risk exposure when sharing information [48] [49]. As SNS have been one of the best ways for people to consolidate their old ties and work on new ones, there is an impetus to create a profile and to subsequently display social connections.

5.4 Factors affecting user behaviors

Paine et al. [50] reviewed numerous studies, and drew the conclusion that privacy concern was the most important factor affecting privacy disclosure [51], but Acquisti and Gross [41] found users’ privacy concerns
to be weak predictors of their membership of the network. Even some of those users with high levels of privacy concern enjoyed sharing personal information on social network sites.

Different groups behave differently in the face of potential risk. As Fogel and Nehmad [52] stated, different risk taking attitudes exist between genders of users with profiles on SNS: greater risk taking attitudes exist among men than women. In general, privacy concerns and identity information disclosure concerns are of greater importance to women than men. Greater percentages of men than women also display their phone numbers and home addresses on social networking websites. In addition, it was found that individuals with profiles on social networking websites have greater risk taking attitudes than those who do not.

There are also scholars who have studied the effect of differences in age with respect to behavior on SNS. Pfeil et al. [53] demonstrated that teenagers have larger networks of friends compared to older users of MySpace. The majority of teenage users’ friends are in their own age range, while older people’s networks of friends tend to have a more diverse age distribution. In addition, their results show that teenagers tend to make more use of different media within MySpace and use more self-referencing compared to older people.

There are still other factors influencing privacy data disclosures on SNS. Lehikoinen et al. [39] also found that culture of community and competence are significant factors affecting information disclosure in social online services.

6. Topical themes and issues

6.1 Privacy-preserving collaborative social network

Information sharing in or among social networks can be used as a helpful antiterrorist strategy [54], an intelligence sharing capability [55] and in project fulfillment procedures. Mutual benefit calls for collaborative social networks while everyone still cares about their private information. Yang [54], Blosser and Zhan [55] and Zhan et al. [56] discuss how to design social networks with better privacy controls.

According to Blosser and Zhan [55], three main hurdles exist in building a collaborative social network. “The first hurdle is how to actually combine the social network data of multiple, potentially competing providers into a single network. This must be done in a way to prevent a provider from acquiring the data of other providers and without the central server knowing the contents of the social network. The next hurdle is keeping the collaborative social network updated so edges that have been removed in sub-networks are removed in the collaboration.” The last hurdle is handling user interaction within the collaborative social network.

Both Yang [54] and Blosser and Zhan [55] have worked on the structures of privacy-preserving collaborative social networks. Blosser and Zhan [55] propose a client-server architecture as the technological base of a collaborative social networking environment, allowing the users and other social networks to be clients of a server that would keep the data and communications partitioned. They also determined which nodes within different social networks were the same by finding matching attributes (e.g. email addresses, names and so on), so the edges in both networks should be combined at that point. Yang [54] proposed publishing a combination of information in a generalized node depending on the intended degree of privacy, and he proposed new criteria to determine which information was to be shared in a generalized node: need to know, need to share, privacy and trust. According to experiments, the methodological approaches in both articles seem to be useful. Meanwhile they all believe a more complete network including the structure and information filtering system needs to be developed in the future.
6.2 Innovative business models for privacy protection

Despite more and more techniques being developed for privacy protection, a problem still remains: who should pay for those techniques and who should be held liable for damages when users’ privacy is infringed? Illegal encroachments on privacy should be punished by law, but there is a large grey area around specific liabilities and responsibilities between users and companies of SNS in different contexts. Inventors of most existing techniques address only a part of the problem taking a given stakeholder perspective: Langheinrich [57] provides a privacy policy on behalf of users while Karjoth and Schunter [58] take the view of companies. According to Caudill and Murphy [10], government rules tend to place the burden on companies, and Rosenblum [59] emphasized users’ self-limiting common sense to be important in reviewing other profiles and posting their information online as well.

O’Reilly [60] has created business models for the next generation of software. He believes that data control may be the chief source of competitive advantage for companies. Hoffman et al. [61] also believe that the “effective way for commercial web providers to develop profitable exchange relationships with online customers is to earn their trust”, which can be done by “allowing the balance of power to shift toward a more cooperative interaction between an online business and its customers”.

Though these are the main opinions that have been proposed by scholars, the concrete structure of the business model is rarely mentioned. An innovative business model taking into account privacy protection is desperately needed by both users and providers of SNS. The duty of companies, users and government in protecting users’ privacy should be made clear, and the model should be easy to implement.

6.3 Personalized services or privacy invasion?

Facebook introduced the beacon platform in 2007, which was aimed at tracking users’ online purchasing habits and publishing it to a friend. The purpose of this strategy was to bring about more customized advertising. But people felt their privacy had been breached. After user groups resisted the feature, the beacon platform was closed. On April 21, 2010 Mark Zuckerberg announced Facebook would bring out an “Open Graph” plan. This plan attempted to connect users of Facebook to the rest of the networked world according to their preference and behavior online. Within a few days of the announcement, privacy advocacy groups urged the Federal Trade Commission to investigate the plan.

According to Kevin Werbach, legal and business ethics professor at the Wharton School, University of Pennsylvania, “act now; apologize later” is one way that big companies are pushing forward with new services. It is only after the service is introduced that we learn whether a company ultimately will face a backlash from users and regulators.

7. Comparative analyses

Table 1 outlines the findings of this paper. Four main parts are presented: (i) information leaks based on privacy disclosure, (ii) information leaks based on attack techniques, (iii) users’ behaviors with respect to SNS and privacy and (iv) some other topical themes and issues which are presently receiving a great deal of attention. Important articles focusing on those areas are arranged and referenced in the last column.
<table>
<thead>
<tr>
<th>Main parts</th>
<th>Problem</th>
<th>Detail or solution</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information leaks based on privacy disclosure</td>
<td>Improper use of disclosed information</td>
<td>Doing business and marketing</td>
<td>DeCew (1997)[11] Caudill and Murphy (2000)[10]</td>
</tr>
<tr>
<td></td>
<td>Mandatory government rules</td>
<td>Cate (1997)[16] Caudill and Murphy (2000)[10]</td>
<td></td>
</tr>
<tr>
<td>Information leaks based on attack techniques</td>
<td>Data mining techniques</td>
<td>Probabilistic relational models; Bayesian logic programs; Relational probability trees etc</td>
<td>Chakrabarti (2000)[17] Getoor (2003) [18]</td>
</tr>
<tr>
<td></td>
<td>Factors affecting users</td>
<td>Levels of privacy concern, risk taking attitudes, age and gender</td>
<td>Fogel and Nehmad (2009)[52] Pfeil et al. (2009)[53] Lehikoinen et al. (2008)[39]</td>
</tr>
<tr>
<td></td>
<td>Use of profile protection</td>
<td>Rarely used because difficult and poorly designed</td>
<td>Bennett and Grant (1999)[42] Kleinberg (2007)[43] Ko et al. (2007) [38] Lehikoinen et al. (2008)[39]</td>
</tr>
</tbody>
</table>
8. Conclusions

Users' rights to privacy are in danger. Users' online behaviors are careless, threatening the safety of their property, reputation and sometimes even their lives. Dealing with information leaks depends on what users are willing to disclose, and it has to do with government laws and market regulation within a given jurisdiction. Self-regulation is an advanced form of market regulation.

Attack techniques include direct attack techniques and malicious applications. Protection from direct attacks relies on experts, but protection from malicious applications depends mostly on users' watchfulness.

Users can reduce their risk by increasing their own levels of safety awareness. Previous studies have shown that users' behaviors on SNS have placed individuals in dangerous situations. The theory of weak ties provides reasons why users disclose personal information in SNS. Future research should address privacy-preserving collaborative social networks, innovative business models ensuring privacy protection, and the question of personalized services or an invasion of privacy.

Acknowledgements

The work was supported in part by the National Natural Science Foundation of China under Grant No. 70901039 and 71171106, National Planning Office of Philosophy and Social Science under Grant No. 11&&ZD169, NCET-11-0220 project, Jiangsu Planning Office of Social Science under Grant No. 11TQC010, Jiangsu University Philosophy and Social Science key project under Grant No. 2012ZDIXM036 and Nanjing University Innovation Team Support Project.
References

25. E. Athanasopoulos et al., "Antisocial Networks: Turning a Social Network into a Botnet," in Proc of
43. J. Kleinberg, "Challenges in Mining Social Network Data: Processes, Privacy, and Paradoxes," in Proc of ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2007, pp. 4-5.