# Breach of Personal Security through Applicative use of Online Social Networks

Bojan Nikolovski[1], Vasko Kokolanski [1], Jugoslav Achkoski[1] , Metodija Dojcinovski[1]

[1]*Military Academy "General Mihailo Apostolski", Vasko Karangeleski bb,1000 Skopje, Macedonia*

***Abstract*** **- Throughout this article there is an attempt to indicate the threats of potential to breach of personal security through applicative use of internet as well as applicative use of online social networks. In addition to many other ways of privacy protection applicative users of social network's sites must take into considerations the risk of distributing private data. Through a series of actions and settings users can customize the security settings with the ultimate goal of reducing the risk of attack on their privacy.**

***Keywords:*** **Security, Privacy, online social networks, Internet**

## 1. Introduction

The rapid growth of social network's sites, especially in combination with the use of portable digital devices such as mobile phones and tablet computers have led to an increased risk of invasion of privacy. A number of social services of almost all social networking sites are created by users to enhance their impact. For example, Facebook allows users to disseminate photographs, publish personal data as well as interact with the groups and companies or other users.

The main goal of this article is to indicate a way to protect personal safety and privacy through a series of measures and actions taken by the users.

This article is divided in eight sections. In each section an attempt is made to elaborate different online social networks as well as in couple of sections we make an argument of breaching of personal security. In the second section an argument is made that concerns breach of personal security by using of internet and online social networks in general. In the third section there is a basic elaboration or brief introduction to cyberspace. Generally, discussion in this section concerns applicative users of the internet. Section four is introduction to online social networks. In section five, six and seven an elaboration is made of adapting and updating the privacy settings for Facebook, Twitter and LinkedIn. And finally in section eight other security measures of protecting privacy for an applicative user of internet are discussed.

## 2. Related work

In research by Theodoros Semertzidis, Petros Daras and Isidro Laso Ballesteros named "*Social Networks Overview: Current Trends and Research Challenges*" [7] which is founded by FP7 program by EU main goals are the emergence and popularity of online social networks in recent years and how OSN has changed the Internet ecosystem with the end state which leads to a more collaborative environment., accordingly.

In the article "*Extraction and Analysis of Facebook-Friendship Relations*" by the authors Salvatore Catanese, Pasquale De Meo, Emilio Ferrara, Giacomo Fiumara, and Alessandro Provetti [16], question is made about social sciences, and the technique for analyzing social networks behavior.

In the article *"(Under) mining Privacy in Social Networks***"** by Monica Chew, Dirk Balfanz, Ben Laurie [9] the authors discussed distinct areas where the highly-interlinked world of social networking sites can compromise user privacy.

Accordingly throughout this article an attempt is made to indicate the threats of potential breaches of personal security through applicative use of internet as well as applicative use of online social networks.

## 3. Breach of personal security in the modern way of life

Generally, contemporary society increases the speed of life, and consequences are faster access to information. Information until a few decades ago was seen as personal data that was kept in private such as name, address, family members, address, phone number, photographs, family, friends, personal interests and preferences, etc. In the past few years, information is publicly available through online social networks.

Intelligence agencies adapt their ways of collecting information according to new technical developments.

The use of OSINT (collecting intelligence through open source) intelligence discipline is more

exploited than other intelligence disciplines in intelligence communities worldwide.

The Internet doesn't only become an important part of everyday life, but its widespread use has become necessary tool for societies, countries, and companies to work in an appropriate and convenient way.

As time passes and the dynamics of logging onto the global network has become an integral part of the work of individuals, businesses, governmental agencies, national and international profit and non-profit organizations. All of these mentioned above, regularly use the Internet's benefits that are based on information technology development.

Besides the benefit of information technology, usage of the same technology certainly has potential risks especially for applicative users of internet and online social networks as part of it.

## 4. Cyberspace

Rapid changes in technology have brought the world into the "information revolution." The benefits of this so-called "information revolution" were immediately absolved of society and individuals, but nobody took into account impossible threats. Potential threats in the new space (cyberspace) are developed in unconventional ways and they are unlimited.

This necessarily leads to the study of emerging threats in cyberspace and leveling them in terms of opportunities for the benefits of using the same space. Realizing this newly created space for the security breach and its detailed analysis, the threats that were unimaginable became part of everyday reality [4]. In the world global Internet networks are connected by more than two billion users [11].

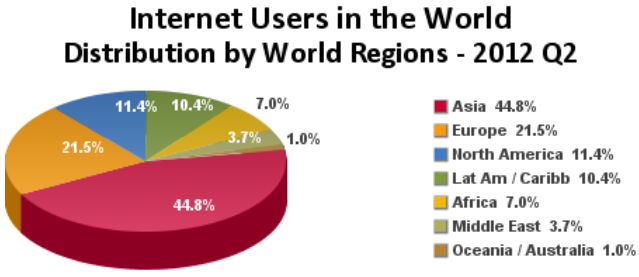


*Figure 1. Internet Users in World*

If only a small fraction of individuals, who are trained or have the skills and intentions to collect data from the Internet network, can lead to an increased risks of data leaks. Various organizations have recognized the importance of IT staffing and in order to actively recruit people who are highly IT literate. If you would combine following factors: vulnerability, increase in violence, information literacy and education of members of organizations can easily get to view the zone of overlap of real and cyberspace. Also the uses of the old tactics in intelligence disciplines to deal with unconventional threats are perceived that they are obsolete and generally out of use.

## 5. Online social networks

Social networking sites are defined as a network web-based service that allows individuals to create public or semi-public profiles within the web system. First, their allocation is to communicate and share data with parties using the same online social network. Second, social network sites provide monitoring of the activities of people that are online and the location of images made by them within online social networks.

The nature and nomenclature of these connections may vary from site to site. While we use the term "social networking sites" to describe this phenomenon, the term "social networking sites'' (They are both the same phrase) also appears in public discourse, and the two terms are often used interchangeably. We decide not use the term "networking" for the reason that the scope of the word "Networking" emphasizes initiation and communication, often between unknowns. Daily use of online social networks (OSN) like Facebook, LinkedIn, and Twitter has steadily increased in the number of its customers since 2005[1]. Social networking sites actually are major reflection of our everyday life, basically they depict user's everyday social interactions, theirs beliefs, likes and dislikes etc. This interaction certainly contains information beyond geographical boundaries.

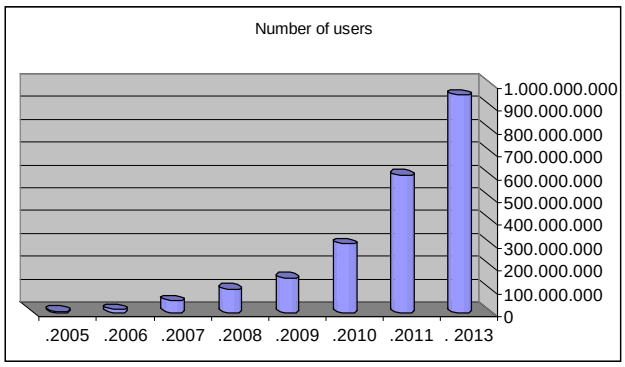


*Figure 2. Grow of Facebook online Social network users in World*

We as a user of social media can observe that social websites like Twitter and LinkedIn contain customer's data that overlap in the databases. While Facebook and Twitter tend to everyday social

interaction, LinkedIn is aimed for professional networking.

In research for the Internet concentrating on detecting trends in American life, by Amanda Lenhart, she shows that more than 50% of internet users of social networks have two or more online profiles. The study found that users have 80% profiles on various internet networks like Facebook, Twitter, and LinkedIn etc.

Using multiple social networks allow users to communicate with friends or to separate personal and professional contacts.

Social networking sites or Online Social Networks today are extremely popular and have a hundred million users [3].

The term "social network" was first used in the middle of the last century when the term social network was defined as a group of persons or organizations that are related to each other [4].

What makes social sites unique are not that they allow individuals to interact with strangers, but rather that they enable users to articulate and make visible the social networks.

In many of the major social networking sites the members are pushed to register new members, who are already part of their list of friends.

As a society in a new way of life, we can say that we depend on social networking sites, but use of social networking sites can be extremely dangerous to personal security if they are not careful when using them applicatively.

Logical question: Do you know what information to post regarding your work? Did you know that people can use social networking sites to gather information? Do you know that you can be at risk even if you do not use social networking sites?

Privacy and protection of personal data should have a major influence to bear in mind when using social networking sites. More details and elaboration of social networking sites are discussed in following sections of this article.

## 6. Adapting and updating the privacy settings on Facebook

Adapting and updating the privacy settings on Facebook is a "necessary evil" that is imposed on applicative users of Facebook. Namely these settings are needed whether it comes to data published in the News Feed, or it comes to people in photos.

The online social network Facebook, which is semi-private, opens opportunities for setting privacy. In addition Facebook is regularly adapting the basic privacy settings. When we are making a debate on the protection of privacy data, we must look at the facts for whom and to what extent users make announcements, to which they are available and the consequences of posting them.

The online social network Facebook is in constant conflict to establish a balance of options for customizing the privacy settings. Conflict is imposed by who has to control privacy, namely whether it the customers or the company that has the real capability to monitor all users.

If this is reformulated in an understandable way, Facebook wants to achieve information sharing between users, but as a normative framework company it should be responsible for handling within the scope of applicable laws and ethics.

Each new design, or changing of the privacy terms, Facebook changes something in the users' profile and the way we manage profiles. This can be depicted by the number of fields in users' profile of Facebook Based on the research conducted at Carnegie Melon University for a comparative review of personal data fields on Facebook profile in 2005 and 2012, the analysis shows a rapid growth of fields from 39 in 2005 to 126 in 2012 that contain personal information of the user. If we put this data in the graph, we would visually capture the above data with the following results.

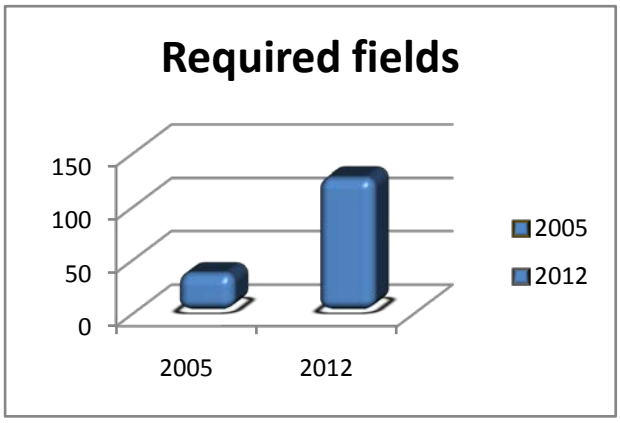


*Figure 3. Flowchart of the increase in the number of fields in Facebook profile*

## 7. Defining and differencing public and protected Tweets

Let's start this section with an elaboration of the differences between public and protected Tweets. Basically on opening an account or when a user is signing up for Twitter, there is an option to keep Tweets public (which is by the way the default account setting for Twitter) or to protect the Tweets.

To clarify for the accounts with protected Tweets, there is a mandatory to manual approval of each person who may view that account's Tweets.

Basically, public Tweets (as we already mentioned are the default setting) are visible to anyone, whether or not they have a Twitter account.

On the other hand, protected Tweets may be only visible for internet users if they have approval from Twitters' user.

In order to make this clearer we can introduce examples that in simple way can explain this adaptation. Basically if at one time anyone had public Tweets, those Tweets will always be public and searchable, even if there is a change of the settings to the "protected" mode. Only Tweets made after updating the settings will be protected. Also we must take into consideration that if anyone decides to unprotect the Tweets instantly that action will cause any previously protected Tweets to be made public.

## 8. Customizing and controlling privacy settings and managing social advertising on LinkedIn profile

LinkedIn upset their users when it altered its settings to show, by default, the names and photos of users within the third-party advertisements. This attempt of altering user privacy settings was so significant that the reaction to it forced LinkedIn to change back the settings a few days later.

Rather than to show user photos and names in third-party advertisements, LinkedIn now presents the number of users in your network who have recommended or followed the brand.

Now we will try to explain one of the ways to turn off the social advertising:

In the following paragraph there are presented steps for this activity which are visually presented in Figure 4. When users are on main page on their profile or LinkedIn homepage, couple of steps should be made. First users have to open menu "Settings" (number 1 on figure 4). On the top of this menu user have to click *user name* in the upper right corner of the home page. By doing this, the drop-down menu will appear, then selecting "Settings" then select "Account" (number 2 in figure 4) in the column next to "Account"(number 3 in figure 4), and finally click on "Manage Social Advertising"(number 4 in figure 4). By deselecting the box next to "LinkedIn may use my name, photo in social advertising" this adaptation is done. So that the LinkedIn does not have authorization to use users name in social advertising.

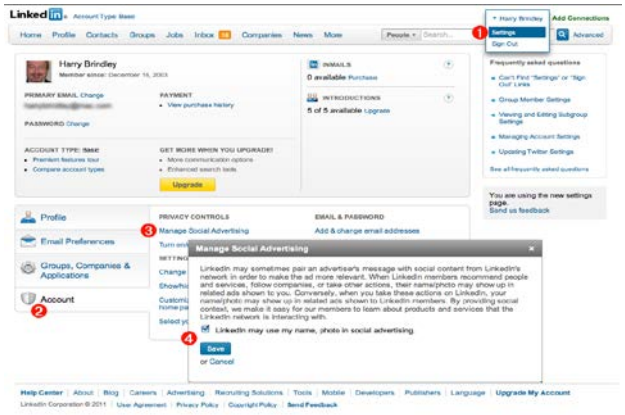


*Figure 4. Customizing and controlling privacy settings and managing social advertising on LinkedIn profile [10].*

On the other hand, these settings can be used for managing other settings like "who can email the user" and "manage visibility of information".

First, let's discuss how to protect users from third-party companies to store user information in their advertisements.

Starting on the LinkedIn homepage, click on *user name* in the upper right corner. On the drop-down menu, select "Settings". From the "Settings" page, select "E-Mail Preferences". In the column next to "E-Mail Preferences", click "Turn on/off partner InMail" .By deselecting the two boxes: LinkedIn does not have authorization to use users email in third party advertising. Second if users want to manage Who Can Save users Information a couple of steps should be taken by the user.

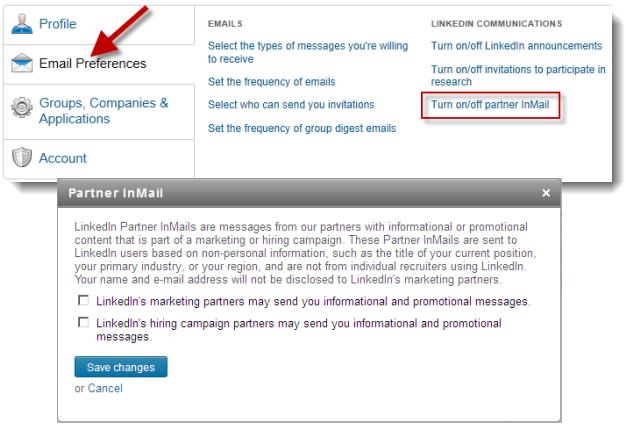


*Figure 5. Turn on/off partner InMail on LinkedIn profile*

Users have the option to be prevented from the unwanted information sharing.

It can be done by the customizing tab with label the "Turn on/off data sharing with 3rd party applications" in the Groups, Companies and Applications tab, listed just under E-mail Preferences. In that manner, users do not authorize the LinkedIn to use user information.

## 9. Other security measures

Contemporary solutions for additional data protection from the other applications are protocols where the use of HTTPS -protocol is widely broaden. In order to use these protocol users must make changes in their user's profiles on online social networks. This browsing is often referred to as Secure Browsing. By choosing the browsing on a secure connection (https) when it is possible, users achieve a higher level of security to their data.

It is possible to establish a dual authentication system in order to ensure that only you as a Facebook user can be logged on with one's own user data. On Facebook it is necessary to choose the Login Approvals and marking the option will be required to enter a login code from unauthorized devices in order to access a personal profile. Also, there is a possibility of getting notifications whenever a user logs into their own account from a device that has not been previously used.

## 10. Conclusion

Through elaboration of this paper, we can conclude that superiority of one country does not depend only from its people, its army and its values, but contemporary dominance depends from ICT (hardware, software) and financial infrastructure that support its economic development and prosperity.

The goal of modern intelligence organizations is to collect personal details of social network users which could be used to disrupt the economic stability of the country, and thus reduce the confidence of citizens in the institutions of the state.

Description of cyberspace was of great importance for this paper, because states nowadays are directly supported by this media and internet global networks link the computers that facilitate electronic transactions.

In order to explain the importance of the Internet in the process of gathering information through intelligence OSINT a disciplined look at the net in general is necessary. The scope of this process and the constant expansion of the Internet network leads to inability to implement the entire internet network system for, collecting, analyzing, targeting, and dissemination by the intelligence agencies.

To implement this part of the spectrum OSINT intelligence cycle, intelligence communities around the world have formed special units that would deal with this part of the spectrum of information.

The Internet is currently being used as an important source of information for many intelligence communities. Here we must bear in mind the dual role of the availability and expansion of the Internet.

The expansion of the Internet allows for greater availability of information, but on the other hand the expansion leads to opportunities for placement of misinformation, because it is an open system for anyone to publish data and information.

As the new system appeared online social networks in which intelligence communities pay special attention.

In conclusion applicative users of internet social networks must take into consideration the dangers of potential breaches of personal security and take all the necessary measures to prevent that.

## References


[1]. Amanda Lenhart, *Adults and social network websites*- Washington, DC: Pew Internet & American Life Project., 2009

[2]. Rathmell, A., *Cyber-terrorism: The shape of future conflict?* (accessed on 28.01.2013) http://www.informaworld.com/smpp/content~db=jour~content=a791623655~frm=titlelink

[3]. Ana V. Kovacevic, *Leaking information through Facebook,* Yearbook of the Faculty of Security annual, Belgrade University, pp 312, 2009.

[4]. Wasserman, Stanley; Faust, Katherine (1994). *"Social Network Analysis in the Social and Behavioral* Sciences". Social Network Analysis: Methods and Applications, Cambridge University Press. pp. 1–27.

[5]. Boyd, Danah. (2008). *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*. MacArthur Foundation Series on Digital Learning - Youth, Identity, and Digital Media Volume, Cambridge MIT Press, pp. 119-142.

[6]. Catanese, S., De Meo, P., Ferrara, E., and Fiumara, G. (2010). *Analyzing the Facebook Friendship Graph.* Proceedings of the 1st International Workshop on Mining the Future Internet, pp. 14-19.

[7]. Theodoros Semertzidis, Petros Daras and Isidro Laso Ballesteros named (2010) *Social Networks Overview: Current Trends and Research Challengesm*, nextMEDIA" CSA. ,Future Media Networks cluster., DG Information Society, Unit D2 Networked Media.

[8]. Counts, S., and Fisher, K. E. (2008). *Mobile Social Networking: An Information Grounds Perspective*, Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), pp. 153.

[9]. Chew, Monica, Balfanz, Dirk, and Laurie, Ben. (2008). (Under)mining Privacy in Social Networks.

[10]. Harry Brindley, *Ugh! Now LinkedIn is doing it too …*, slappHappe. August 11, 2011.

http://slapphappe.wordpress.com/2011/08/11/ugh-now-linkedin-is-doing-it-too/ (Accessed 18 November 2013).

[11]. Internet World Stats - Usage and Population Statistics. 2013. http://www.internetworldstats.com (Accessed 18 November 2013).

[12]. Grimmelmann, James. (2009). *Saving Facebook*, Iowa Law Review, pp 1137 - 1206.

[13]. Gross, Ralph, and Acquisti, Alessandro. (2005). *Information Revelation and Privacy in Online Social Networks*. Proceedings of WPES'05. Alexandria, VA: Association of Computing Machinery, pp. 71-80.

[14]. Guha, Saikat, Kevin Tang, and Paul Francis. "NOYB: Privacy in online social networks." *Proceedings of the first workshop on Online social networks*. ACM, 2008, pp. 49-54.

[15]. Han Lin, and Lin Qiu. (2012*). Sharing emotion on Facebook: network size, density, and individual motivation*. Extended abstracts on Human factors in computing systems, pp. 2573-2578.

[16]. Catanese, Salvatore, Pasquale De Meo, Emilio Ferrara, Giacomo Fiumara, and Alessandro Provetti, *Extraction and analysis of facebook friendship relations,Computational Social Networks*, pp. 291-324. Springer London, 2012.

*Corresponding author:* Bojan Nikolovski
*Institution:* Military Academy, Skopje, Macedonia

*E-mail:* bojannikolovski12@gmail.com