Social Networks: Privacy Issues and Precautions

Mohamad Ibrahim Ladan
Computer Science Department
Haigazian University
Beirut – Lebanon
mladan@haigazian.edu.lb

Abstract—**Social networks, such as Facebook, Myspace, LinkedIn, Google+, and Twitter have experienced exponential growth and a remarkable adoption rate in recent years. These social networks are touching our lives at home and at work by providing attractive means of online social interactions and communications with family, friends and colleagues from around the corner or across the globe; however, this comes with a growing concern regarding the privacy and security risks that accompany the use of such networks. In this paper, we will investigate and discuss the different privacy issues pertaining to social networks, in addition, we will propose some precaution measures that should be applied to tackle these issues.**

Keywords: Social Networks privacy issues; online privacy; information revelation; Social Networks privacy precautions measures.

I. INTRODUCTION

The size, growth adoption rate, and popularity of social media networks, such as Facebook, Myspace, LinkedIn, and Google+, are phenomenal. Facebook has reached more than 700 million users and according to a brochure released by Websense, a company specializing in computer security software, Facebook has an annual growth rate of 41% and Twitter is growing at 85% year after year. In 2011 Google released its Google+ social networking offering, first by invitation only and then generally opening the site [1]. In 2014, the largest social network is Facebook and other popular networks include Twitter, Instagram, LinkedIn, and Pinterest. [22]. This fast growth is due in part to the latest advancements in the field information and communication technologies, tablets, mobile smart phones, and other similar mobile computing and communication devices that have become very popular and sometimes necessary home and individual type of appliances to both kids and adults. These types of networks are useful and have a lot of benefits to all kind of users. They were built upon the concept of traditional social networks where you are connected to new people through people you already know. Their goal could be purely social, allowing users to establish friendships or romantic relationships, while others may focus on establishing business connections. They can be used for professional networking and job searches, as a means to increase sales revenue, as a way to reconnect with current and old friends, as a way to make new friends, or as a way to share information and to socialize.

Social networks can be described as web applications that allow users to create their semi-public profile [13], i.e., a profile that some information is public and some is private, communicate with friends, and build an online community. It is based on social relationships among users. Most people join social networks to share their information and keep in contact with people they know. The main feature of social networks is a friend finder that allows social network users to search for people that they know and then build up their own online community. They have changed radically the way people interact with each other regardless of their physical location. They provides every person, regardless of its age, the ability to easily communicate and share data and information of all types, audio, video, or text on one-to-one basis, one-to-many, and many-to-many in a matter of fraction of seconds without any difficulties. These benefits are accompanied with a growing concerns regarding the privacy of the information exchanged or stored on the communication links and servers of those social networks. These information could be sensitive or critical, such as the identification, confidential conversation, personal, and private data, and credit and financial data. So every user of social networks should be concerned one way or the other about these types of privacy risks. Most people became more aware and more concerned about these risks when Facebook inadvertently exposed millions of users' phone numbers and e-mail addresses to unauthorized viewers over years that began in 2012. The major reason for causing such breaches in social network security and privacy emerges from the massive amount of information that these sites process every day, making it much easier to exploit even if there is a little fault in the system. Furthermore, social networking is now no longer restricted to just desktop and laptop computers, the technology is available on smartphones, tablets, and just about anything that is connected to the Internet [4]. This wide spread of smart mobile devices has opened new paths for malware transmission, bringing concerns about

 ISBN: 978-1-61208-381-0

information theft, and tracking user's location and preferences.

Despite the fact that most of the privacy risks in using social networks are related to the Information Communication Technology and the internet infrastructure that these social networks are operating on. However, most privacy risks come from the nature of the social network application itself and sometimes from their privacy policies and the way people use the networks. This paper is focused on what we call user-related part of these risks, i.e., risks that are stemmed from user's behavior, privacy policies, and the nature of the application and its default configuration. The application-related part tends to be more technical, i.e., data and communication security, protocols used, enforcing privacy setting, security measures, encryption and decryption will be addressed in another paper.

The rest of this paper is organized as follows: In Section II, the various social networks privacy issues and concerns are presented and discussed. In Section III, different precaution measures and guidelines to maintain an adequate level of privacy on social networks are proposed and presented. In Section IV, discussion of the need for security and privacy legislation and policies to tackle the privacy concerns are discussed. Finally, in Section V, a summary and conclusion of the paper is given.

II. SOCIAL NETWORKS PRIVACY ISSUES

"If you feel like someone is watching you, you're right. If you're worried about this, you have plenty of company. If you're not doing anything about this anxiety, you're just like almost everyone else." [15]

The increased pervasiveness and use of information communication technologies have changed many people's lives in terms of how they work, form, and maintain social relations. This rise in social networks or networked societies comes with a lot of concerns, mainly the privacy concern. Social networks usually share three common elements. They allow individuals to construct a public or semi-public profile within a confined system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system. While the concept of privacy is not new, modern technological advancements have meant that privacy concerns have evolved. New information communication technologies have transformed our ability to collect, aggregate, and share data. Modern technology has the ability and power to capture, store, aggregate, redistribute, and use data from individual users. The problem is that the owner of this information is often unaware of, or at least unconnected to, its storage and utilization, and that such ubiquitous data collection is harmful to personal privacy [23].

The "State of the Net" research and statistics from Consumer Reports suggest that there is an overall increase in certain digital problems, such as ID thefts, phishing schemes, and security breaches. The most surprising findings however, involve how much Facebook knows about more than 900 million members, and how much we, members, freely offer information that could be extracted by employers, insurers, some government offices, as well as identity thieves and other criminals [17].

Most if not all social network user's profiles contain real information about users. Sensitive information, such as user's full name, contact information, relationship status, date of birth, previous and current work, and education background attract hackers. In addition, most social network users share a large amount of their other private information in their social network space, and publish the information publicly without careful consideration. Hence, social networks have become a large pool of sensitive data. Moreover, social network users tend to have a high level of trust toward other social network users. They tend to accept friend requests easily, and trust items that friends send to them.

Most social networks ask users to agree to Terms of Use policy before they can use their services. However, these Terms of Use often contain phrases permitting social networks to store user's data on their servers and even share it with third parties. The levels of privacy presented for users in social networks vary from one network to the other. Some encourage users to provide real names and other personal information, such as age, family, education, interests, and even relationship status. Facebook has attracted attention over its policies regarding data storage, such as making it difficult to delete an account, holding onto data after an account is de-activated and being caught sharing personal data with third parties [12].

Privacy can be viewed from the perspective of control. Whether it is control over personal data, the choice to disclose data, the physical presence of others, the number of others present in disclosure, or choosing which person to discuss and share issues with, control is central to maintaining privacy. The main privacy issue in social networks is the abuse and the leakage of profile and personal information of the users. Several cases related to privacy issues have surfaced up lately. A report in the *Wall Street Journal* indicates that the Facebook, along with MySpace, and a handful of other social networks, have been sharing users' personal data with advertisers without users' knowledge or consent [6]. The data shared includes names, user IDs, and other information sufficient to enable ad companies, such as the Google-owned DoubleClick to identify distinct user profiles. Moreover, Facebook appears to have gone farther than the other networks when it comes to sharing data. When Facebook's users clicked on ads appearing on a profile page, the site would at times provide data, such as the username behind the click, as well as the

 ISBN: 978-1-61208-381-0

user whose profile page from which the click came. In addition, Twitter has admitted that they have scanned and imported their user's phone contacts onto the website database so that they can learn more about their users. Most users were unaware that Twitter is created this way for new users to search for their friends. More than 1,000 companies are waiting in line to get access to millions of tweets from users that are using the popular social networking website. Companies believe that by using data mining technologies they would be able to gather important information that can be used for marketing and advertising [11]. Twitter has stated that they will have their privacy guidelines illustrated more clearly in the future [10].

Although some users may have no problem in revealing their personal information to a large group of people and may not care about the privacy policies and setting of the network, others they care and try to make use of the available security features. However most social networks restore the relaxed default setting after each update. Facebook was criticized due to the perceived carelessness regarding privacy in the default setting for users [8].

Other main issue related to privacy is stemmed in the fact that many social networks provide an Application Programming Interface (API) for 3rd party developers to create applications for the network's platform. These 3rd party applications are very popular among social network users, and once installed, they are able to access user's data automatically, and are capable of posting on users' space or user's friend's space, or may access other user's information without user's knowledge. In addition, these 3rd party applications are able to track social network user's activities, or allows advertisement partner to access and collect social network user's data for commercial and advertising purposes [14].

On the other hand, posting and sharing, directly or indirectly, photos or videos may result in an individual's breach of privacy or to an organization's breach of confidentiality.

Another important issue related to privacy is that potential employers are looking up information about their potential employees using social networks. The information found is used to screen job applicants and may affect or hurt their chances of being employed. Employers may find out that an applicant made a political statement that conflicts with the company ideologies. Facebook and Twitter are being used a lot to screen job applicants. On Facebook and Twitter, we believe employers are trying to get a more personal view of a candidate, rather than the resume-like view they will see on LinkedIn. This means that is important for social networks users to keep in mind that some, if not most, employers use these networks to do some sort of pre-screening their job applicants [16].

Many social networks have responded to criticism and concerns over privacy. It is claimed that changes to default settings, the storage of data and sharing with third parties have all been updated and corrected in the light of criticism, and/or legal challenges. However, many critics remain unsatisfied, noting that fundamental changes to privacy settings in many social networking sites remain minor [9].

III. SOCIAL NETWORKS PRECAUTIONS

The popularity of social networks continues to increase, especially among teenagers and young adults, and the concerns related to privacy risks and issues continue to increase. Fig. 1 shows the worldwide number of active Facebook users from 2008 to 2014. As of the third quarter of 2014, Facebook had 1.35 billion monthly active users [24].

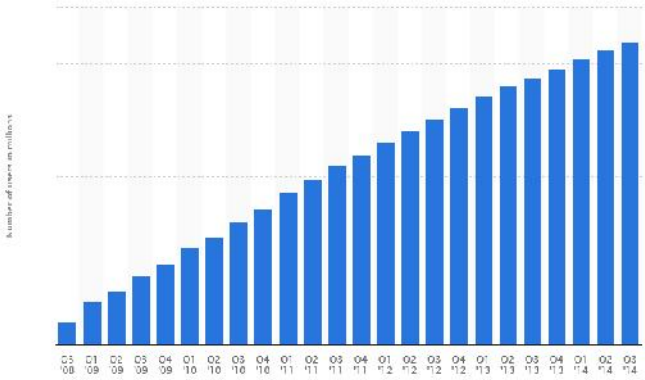

Figure 1: Number of monthly active Facebook users worldwide from 3rd quarter 2008 to 3rd quarter 2014 (in millions)

Therefore, privacy issues become more and more critical and some precautions should be taken to address these issues while using social networks. These precautions can be stated as a set of guidelines and helpful tips that social network users should follow to protect their private information while making use of the benefits of the networks. These guidelines and helpful tips include the following:

- Review the social network's privacy policy before signing up. If the privacy policy is not clear on how it protects the member's information, do not sign up or limit your use of such a network.
- Choose a strong password that cannot easily be guessed and different than other passwords you have on different systems or social networks.
- Check and configure the privacy settings. The default settings for some social networks may allow anyone to see your information, these setting

 ISBN: 978-1-61208-381-0

should be changed to allow only those people you trust to have access to the information you post.

- Remember that social networks are based on the internet which is a public resource.
- Keep in mind that once information is posted online, it can possibly be viewed by anyone and may not be withdrawn after that even if you delete the information from your account, cached or saved copies may still exist on other computers on the network. Therefore, confidential information should not be posted or shared. You should only post information you are comfortable revealing to a complete stranger.
- Limit the amount of personal information you post. Do not post information that would make you vulnerable, such as your address or information about your daily schedule or routine.
- Do not post information like your address, mobile phone number or any information that could be used for banking site security questions, such as your mother's maiden name, hometown, favorite car, school name etc. Identity thieves can find out a lot about you just by the information you may already have on your profile, and they can fill in the blanks.
- Do not tag your location and whereabouts, and do not announce that you are on vacation or away for an extended period of time. You don't want to compromise your feeling of safety and security if someone may know you're not home. It also opens up opportunities for cyber stalkers.
- Be careful about installing third-party applications. Some social networks provide the ability to install third party applications, such as games or other entertainment functionality, however some of these applications may be malicious and may have full access to your account and the data you share. In addition, some of these applications may modify your security and privacy settings. Hence, do not install applications unless they come from trusted, well-known sources.
- Don't believe everything you read online. People may post false or misleading information about their own identities. The internet makes it easy for people to misrepresent their identities and goals.
- Limit the people who are allowed to contact you on social networks. If you interact with people you do not know, be cautious about the amount of information you disclose.
- Think twice before clicking a link to another page or running an online application, even if it is from someone you know. Many applications require you to share your information when you use them. Attackers use these sites to distribute their malware.
- Be careful when adding new friends. A "Friend" is anyone on the Facebook network whom you permit to see your personal information, such as birth date, photos, job, comments and list of other Friends. Friends can also see Friends of Friends, which means that you have possibly added strange individuals whom you may never have met as your active%20users%202008individuals have access to your personal and private information.
- Limit the number of your friends. The more friends you have the more people who have access to your information and the more vulnerable your account is.
- Teach children about internet safety and be aware of their online habits. Children are more susceptible to the threats resulted from the use of social networks. Although many of these networks have age restrictions, children may misrepresent their ages so that they can join.
- If you are working in a company and you often communicate with your colleagues using social networks then talk to the manager to put a social Network Use Policy in place for your company to protect the privacy of information exchanged using these networks.

IV. DISCUSSION

Although more people and companies are finding new ways in using social networks, their successes have been faced by major concerns of privacy risks. The control of information or data is lost once it is posted to a social network. Despite the fact the posted info is meant to only go to selected friends may seem protected by the limited distribution to a restricted audience, nothing prevents one of those friends from forwarding that post to someone else outside of the original poster's group of friends [18]. The same can occur within a group of employees collaborating on a project, it only takes one person to become a leak and forward information to outside the group. And if privacy permissions on a social media site are not set correctly, the data may leak out and become public by default. This can easily happen with FaceBook's privacy policy that keeps changing from time to time. As a matter of fact, as the popularity of social networks continues to grow, the concerns over privacy risks and privacy protection becomes more important and more serious for the users. On the other hand, users are having more concerns about not being able to delete permanently their data they have on the social networks. As humans, we can forget. But the Internet never forgets. And once that data is released, there is no getting rid

 ISBN: 978-1-61208-381-0

of it [1]. Viviane Reding, the Vice President of the European Commission said: "God forgives and forgets, but the Internet never does" [2]. Privacy advocates are working to change this problem by introducing a "right to be forgotten". This is being proposed in a new draft of the European Data Protection Directive that "measures will be put in place to allow European citizens' to have their data deleted by private companies" [3].

Furthermore, as social networks continue to take advantage of mobile devices and location-based services, users will be exposed to even more privacy concerns. Although users will unquestionably enjoy using some of these services, they could possibly be making themselves exposed to more serious privacy risks. Hence, social networks that employ location-based services will have to focus on user privacy concerns to gain people trust.

As people increase the amount of information they share on social networks, some of these giant social networks will have and store a huge amount of personal information about their users. Hence, the need for more privacy controls increases. In addition, without good universal guidelines and overall legislation and privacy laws on how this information can be gathered and used, it could be misused, either intentionally or unintentionally. As a matter of fact, there has been quite a bit of controversy over how much data social networks, such as Facebook and Twitter collect. Facebook lately had a scandal where it used people's profile information to post ads on Facebook that appeared to be authorized by the person whose profile was pulled. It had their profile picture and text that stated that one should buy this product or use such and such a service. There was a lawsuit and millions of people received an e-mail informing them about this lawsuit and how they could take action and possibly receive a settlement of money. Facebook lost millions of dollars because of this blooper [19].

The privacy legislation process has already started developing in the USA and other part of the world, and it's likely to gain even more momentum in years to come and that there will be additional towards universal legislation on privacy regulations. An instance of the new privacy legislation process that is taking place in the USA is the Commercial Privacy Bill of Rights Act of 2011 ("CPBR"). It represents one approach to protecting consumer privacy, and it aims to establish a regulatory framework for comprehensive protection of personal data for individuals under the protection of the Federal Trade Commission. The CPBR would require companies that collect consumer data to adhere to certain security practices and would also require consumers to opt-in to the collection of sensitive information. Consumers could also access, correct, and control information that companies have stored. In addition, the bill would limit the data that a company could collect during any given transaction to only data that is necessary for the transaction's completion. For instance, an online clothes store could not require the consumer to provide personal information, such as his or her birthday if such information is peripheral to the consumer's purchase of snow suits [20, 21].

Without universal privacy regulation and legislation social networks have been setting their own privacy policies, and there is currently an enormous amount of variation between networks. As a result of that, users are often confused as to what privacy controls are available and how they should be used. Additionally, most people do not really understand how to recognize the potential for information misuse. People often share information innocently because they want to use a specific feature, or because they wish to qualify for a free product or service. When universal legislation is in place, social networks will have standard guidelines and policies to follow, thus creating a more secure, safe, private, and less confusing user experience [5].

V. SUMMARY AND CONCLUSION

With the constantly growing popularity of social networks, such as Facebook, Google+, MySpace, Twitter etc. in the personal scope, and others, such as LinkedIn in business circles, undesirable privacy risk issues have arisen as a result of this unexpected rapid rise and due to the availability of huge amount of sensitive information related to large number of users. Therefore, concerns related to privacy issues and breach of privacy in social networks that can put the individual or a company in a serious risk are increasing.

A privacy issue occurs, in its simplest form, when someone, who may be a hacker or not, gain access to private and confidential information about users who are not careful about what they expose on their Social network accounts. In addition, the potential damage to a user as a result of privacy breach depends on how much this user is actively participating or engaging in the social networks, as well as the amount of information he or she is posting. The more information in general, and private information in particular, is posted the higher the risk and harm.

Moreover, privacy issues in social networks, other than those rising from security issues, are more related to users behaviors and awareness of privacy policies and terms and conditions for using these networks. The more information a user posts, the more information becomes available for a potential misuse by malicious users/hackers. Users who provide private, sensitive, and confidential information about themselves and their friends will be more vulnerable, themselves and their friends, for being attacked or hacked. Information, such as a person's social security number, street address, phone number, financial information, or confidential business information should not be posted and shared online. A well-informed user will not only help to maintain privacy, but will also educate others on these issues. The best solution to social network privacy issues is to limit the amount of shared and posted information.

Social networks developers try to implement different mechanisms and measures to protect their users' information and data, but attackers will always find new methods to break through those measures. Therefore, social network users should be aware of all these threats, and be more careful when using such networks and to limit the amount of shared and posted information. In addition, until universal

 ISBN: 978-1-61208-381-0

privacy regulation and legislation are developed and enforced, social networks are setting their own privacy policies that sometime, intentionally or unintentionally, do not protect the privacy of users date and personal information.

This paper addressed, discussed and presented the different types of privacy issues and risks arising from the use of social networks. In addition, it summarized and presented different privacy precautions tips, measures, and helpful guidelines to be followed to protect the user's private information while making use of the benefits of social networks.

REFERENCES

[1] Shullich, R. Risk Assessment of Social Media: http://www.sans.org/reading-room/whitepapers/privacy/risk-assessment-social-media-33940. Dec. 5, 2011

[2] Berwaerts, P. The right to be Forgotten: http://www.business2community.com/government-politics/the-right-to-be-forgotten-0111815. Dec. 28, 2011

[3] Whittaker, Z. European data protection law proposals revealed: http://www.zdnet.com/blog/london/european-dat-protection-law-proposals-revealed/1365. Dec. 7, 2011

[4] V. Jain, InformationWeek, May 19, 2014

[5] Top Five Social Media Privacy Concerns 2014. http://www.reputation.com/reputationwatch/articles/top-five-social-media-privacy-concerns, 2014.

[6] E. Bangeman, http://arstechnica.com/tech-policy/news/2010/05/latest-facebook-blunder-secret-data-sharing-with-advertisers.ars, May 21 2010

[7] Staying Safe on Social Network Sites, http://www.us-cert.gov/ncas/tips/ST06-003, Feb. 06, 2013.

[8] Kelly, S. Identity 'at risk' on Facebook. BBC News. http://news.bbc.co.uk/1/hi/programmes/click_online/7375772.stm

[9] N. Saint, Facebook's Response to Privacy Concerns: "If you're not Comfortable Sharing, Don't". http://www.businessinsider.com/facebooks-response-to-privacy-concerns-if-youre-not-comfortable-sharing-dont-2010-5, 2010.

[10] Sky news, "Twitter admits peeking at address books, announces privacy improvements". Feb. 16, 2012.

[11] K. Gladdis, "Twitter secrets for sale: Privacy row as every tweet for last two years is bought up by data firm". London: daily mail. Feb. 28, 2012.

[12] Bangeman, E. Report: Facebook caught sharing secret data with advisers. http://arstechnica.com/tech-policy/news/2010/05/latest-facebook-blunder-secret-data-sharing-with-advertisers.ars, 2010.

[13] D. M. Boyd and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship," J. Computer-Mediated Communication, vol. 13, no. 1, pp. 210–30. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html, Oct. 2007.

[14] Online Social Networks," WOSN '08 Proceedings of the first workshop on Online social networks, pp. 37-42. http://www2.research.att.com/~bala/papers/posn.pdf, 2008

[15] Sullivan, B. Social Media Polarizes Our Privacy Concerns. Facebook And Its Competitors Are Challenging Long-Held Perceptions of Privacy. http://www.msnbc.msn.com/id/41995992/ns/technology_and_science/t/study-social-media-polarizes-our-privacy-concerns/#.UMEDzYNtjjU. October 3, 2011

[16] How Employers Use Social Media to Screen Applicants, INFOGRAPHIC.http://theundercoverrecruiter.com/infographic-how-recruiters-use-social-media-screen-applicants/

[17] Rosa Golijan, Consumer Reports: Facebook privacy problems are on the rise, NBC News, http://www.nbcnews.com/technology/technolog/consumer-reports-facebook-privacy-problems-are-rise-749990. 2012.

[18] Associate press, http://www.foxnews.com/us/2011/11/08/judge-rules-teacher-should-lose-job-after-facebook-post/, 2011.

[19] Smith, M.; Szongott, C.; Henne, B.; von Voigt, G.; , "Big data privacy issues in public social media," Digital Ecosystems Technologies (DEST), 2012 6th IEEE International Conference on ,vol., no., pp.1-6, 18-20 June 2012, doi: 10.1109/DEST.2012.6227909

[20] TO TRACK OR NOT TO TRACK: RECENT LEGISLATIVE PROPOSALS TO PROTECT CONSUMER PRIVACY, Harvard Journal on Legislation, Vol 49, 2012.

[21] Danah Boyd & Ezster Hargittai, Facebook Privacy Settings: Who Cares?, FIRST MONDAY. http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3086/2589. Aug. 2, 2010

[22] The U.S. Digital Consumer Report". Featured Insights, Global, Media + Entertainment. Nielsen. Retrieved 25 November 2014.

[23] D. J. Houghtona and A. N. Joinsona, Privacy, Social Network Sites, and Social Relations, Journal of Technology in Human Services, Volume 28, pages 74-94, Issue 1-2, 2010. DOI:10.1080/15228831003770775

[24] Statistica 2014, http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/, access date Dec., 22, 2014.

 ISBN: 978-1-61208-381-0