Journal of Yasar University 2011 22(6) 3693-3698

PRIVACY PROTECTION PROBLEMS IN SOCIAL NETWORKS

Mehmet Cudi OKUR[a]

ABSTRACT

Protecting privacy has become a major concern for most social network users because of increased difficulties of controlling the online data. This article presents an assessment of the common privacy related risks of social networking sites. Open and hidden privacy risks of active and passive online profiles are examined and increasing share of social networking in these phenomena is discussed. Inadequacy of available legal and institutional protection is demonstrated and the effectiveness of precautionary measures for protecting sensitive data is evaluated.

Key Words: *Social Network, online profile, privacy, virtual profile, privacy policy*

[a] Department of Computer Engineering Yasar University, İzmir, Türkiye. mehmet.okur@yasar.edu.tr

1. INTRODUCTION

Nowadays it is impossible to imagine a world without the Internet and many other advances that computers and the digital revolution have brought into daily life. Social networking is one of these current revolutionary developments that emerged and rapidly expanded in the last decade. As a result of this rapid expansion, social networking continues to increase in popularity, and is an important medium of communication for many of its participants. Social Networking Sites(SNS) including Facebook, Twitter, LinkedIn, MySpace etc. have introduced increasingly larger numbers of people to new and "virtual" worlds. SNS are websites that allow their users to upload information in various forms to a public profile, create a list of online friends, communicate with them and browse the profiles of other users. In many cases, the creation of an online profile is the first step for active membership in a SNS. Membership generally requires a certain amount of personal information to be submitted to the site. Each website has its own set of membership rules and standards. After subsription, the users of SNS share identity-related information by opening their profiles to others. This information may be directly referring to a person, or describing some of his/her sensitive attributes. In fact, SNS give great power to their members for manipulating information. Because, Information spreads much faster through these networks than through a real-life network. Reasons include the following facts: Digital information can be disclosed to a group of people very quickly, easy to copy and transmit, can be stored indefinitely and is searchable very quickly, Naturally these developments have also created various forms of risks and threats to the individuals and society. Among these, privacy related risks and threats keep growing despite considerable legal and technical counter efforts. The main reason is that, people are sharing more and more online information in SNS about themselves and others, which is difficult to control once broadcasted.

This paper provides an overall evaluation of privacy related risks in social networking and their possible impacts on members and other individuals. A discussion of the methods for privacy protection and their effectiveness is also presented.

2. ACTIVE AND PASSIVE PROFILES IN SOCIAL NETWORKS

The subscribers of SNS usually create their virtual profiles themselves, using the facilities provided by the social networking site. As such, the contents of a profile are based on individual preferences: Joining a particular service, what information to provide or hide, the language and tools used in providing that information and so on. To some extent, the virtual profile is a medium of creative self-expression, allowing an individual to shape his profile in order to reflect the specific ways in which he would like to present himself online.It is not surprising to observe that, parts of the information in most cases are far from being accurate. The extreme case is creating and displaying a totally false and overly exagerated profile.

Although many individuals may not join a SNS and create an intentional virtual profile, they are quite likely to have an unintentional or passive virtual profile. An individual's unintentional virtual profile is the complete trace of personal information about that individual which can be found online. This profile would usually contain a lot of uncontrolled and false information about the individual, creating an inaccurate virtual identity. In many cases, the information may have been accumulated online and posted again without the involvement of the individual concerned. Some possible sources of such information include: A name added to a public or private list, contact information for subscribing to commercial or public sites, online directory services, comments posted as reaction to a news story or to a blog, a name included on a list of people for a certain cause, group photos, video clips published on Internet media and so on. It must be noted that, the pieces of information are not obtained directly from the individuals concerned i.e. the entire process is totally unintentional. In some cases, the amount of unintential information can be considerable. It should be expected that, passive virtual profiles could contribute negatively to one's identity and even worse, create serious privacy risks for the real identity. Another source of concern is that, passive information will usually go for online dissemination without the approval or prior knowledge of the individual. As a result of huge caching and storage capacities provided by technology, the length of time getting longer and longer in which active or passive profiles remain online. Even information that has been deleted by the owner can remain accessible online and be retrieved by search engines long after deletion. In most cases deleting unwanted content is very difficult if not impossible. This indicates that a broad range of accumulated personal information would be available online for any individual that has had an active or passive existence in the virtual world. A rich source

of passive profile data is the trace of search activities and websites visited by an individual. As can be guessed, pieces of this kind of personal information that may seem to be harmless, could be damaging when taken together and processed for specific tasks.

3. MARKET VALUE OF SOCIAL NETWORKING DATA

As more and more people joining social networks , companies are also using those sites for marketing and collecting customer data. There are many social media analytics software and business intelligence tools available for extracting valuable information from active and passive profiles of people. On the other hand, Social network operators including Google, Facebook, Twitter , LinkedIn, Foursquares and others are businesses that make money essentially from advertisers. The social Network user Ids are becoming more valuable not only for commercial advertisements but also for direct marketing, e-commerce, social and political campaigns, human resources departments and insurance companies(Madden and Smith,2010).The market for active and private information is ever increasing. The reason is simple: An E-mail address and a user ID can open ways to a treasure of private information about not only the person involved but also about his or her contacts, friends etc. For example, a user ID provides direct access to name and profile photo, independent of the privacy settings of the site. Facebook's recommended privacy settings could reveal even more: location, hometown, list of friends, photos, and many of their "likes," such as activities, interests and groups. An individual's interests, tastes, likes and dislikes, preferences are contained both by the information that has been posted on the Internet and by the choices they make while online. All of these are reflected back them in advertisements. These advertisements are designed to be more effective using active and passive profiles of the targeted individuals.

Social networking sites have also financial incentives to generate revenues from the information the users upload. The usage of most of these websites is free, and SNS have to make up for their costs by generating revenues from using the identity-related information of their users. The most common way to achieve this is to create marketing profiles of users and serve them with targeted advertisements. As SNS and their marketing partners obtain excessive information about their users, an unbalanced situation arises. Because on one hand, the SNS have valuable sensitive information about their users but, on the other hand the users are not in a position to bargain about the terms at which they would disclose their information. This inequality leaves individuals vulnerable to various forms of harmful consequences, financial or otherwise.

4. INVASION OF PRIVACY

Protecting privacy and sensitive information in Internet are becoming common concerns for people or organizations. Because most Internet users do not realize how much information they are giving up, for example just by browsing the Web. Several marketers use people's Web-browsing histories and online identities to compile profiles that can be sold to advertisers without any permission or consent from the individuals. Actually, any information posted online to some list, group or network can become public in an instant. As many social networkers have friend lists of hundreds, information from profile updates, photos, tweets and wall posts is immediately and indiscriminately broadcast to all of their 'friends'. Given the amount of sensitive information fragments available online, it is not wrong to to assume that accumulated information can also be used for purposes other than marketing. In reality, once personal information is out, it's impossible to know who will have a copy of it, for how long and for what purposes.

There are many possibilities and methods for extracting private information from social networks(He, Chu and Liu,2006).For example, Anybody could take easily a screen grab of a private Facebook message and post it on a public site. Private Twitter feeds, supposedly viewable only by people who the author approves, can be "retweeted," or re-posted, onto the public internet. This kind of small pieces of information, which are insignificant on their own, when placed together, can amount to something which is sensitive and harmful. Another point is that; as people share more and more information about themselves online, a facts pool is formed for any user which contains his/her political views, thoughts on public matters, contacts, travels, locations and trajectories, social activities, memories etc. in very big data warehouses. Software tools that can extract information from data warehouses becoming more and more intelligent to combine and process seemingly unrelated and fragmented pieces of data.

Because of the great amount of online identity-related information, which disseminates easily and immediately through SNS, ill-intentioned people or organizations could easily exploit possibilities for damaging purposes. Identity stalkers, scammers and likes use the attributive information on SNS to identify their victim and use the referential data to contact them. The profiles of users combined with the ease of contacting a user, make SNS a useful platform for wrongdoers. The information on the websites can also be used easily to damage someone's reputation. With the large amount of attributive data on SNS, it is not difficult to reverse engineer information needed to steal someone's identity. Although there is no proof that these possibilities are affecting all users of SNS, experts agree that they affect a significant amount of users and can cause great damage (Gross, Acquisti and Heinz, 2005). Various forms of illegal activity may be based on the unauthorized collection, use and dissemination of personal information available online. As a worst case example, consider a situation in which an individual's virtual profiles may be used to accumulate sufficient information so that an identity thief could target that individual for the purpose of deceitful intentions. Even if the directly accessible profile is inadequate for this purpose, identity thieves can supplement the profile by other means , including hacker techniques for acquaring additional information from the individuals themselves.

5. LIMITED USER CONTROL ON PRIVACY

SNS interpret the consent that users supply when signing up for their services as a broad and informed consent. They implicitly assume that, all the available information about a user can be subjected to secondary usage. In reality, most users of SNS have only a minimal level of awareness and no control over secondary uses of their information. Apart from marketing, sensitive data may be posted to unwanted groups and destinations where information may be used for defaming or incriminating the individual. Another control problem arises when others can post information about an individual to a site, which can only be deleted after the harm has been done, if possible at all.

Usually, a statement on a web site describes what information about the user is collected by the site, and how it is used. The policy statement is posted fairly visibly and offers options about the uses of personal information. These options are called " opt-in" and "opt-out". An opt-in choice indicates that the web site won't use the supplied information without permission. Opt-out choice on the other hand, means the web site can use the information unless the user specifically disapproves. The main concern here is that a big majority of the site users are not aware of the options, their meanings or simply they don't care.

Another major issue is the increased complexity of privacy settings on SNS. The procedures and options have become so confusing that most users are not able to follow and feel they've lost control of the privacy settings. For example, Facebook's privacy policy is now 5,830 words long, there are 50 settings and 170 options to choose from (Facebook,2010).Obviously, the whole process is very difficult to grasp fully and apply for an average user. Facebook's terms of service prohibit anyone from accessing the site or collecting user information using automated means such as software robots. Facebook's and MySpace's privacy policies both contain options, such as allowing users to choose who can view their profile, find them in a search, or see other special data.

Choosing right options may help to limit privacy risksHowever, it is a well known practice that, third-party applications take information from application users, against the networking site's rules, and sell that data to advertisers. Although most SNS have technical protection intended to prevent business intelligence tools form using subscriber data,the invaders are still able to beat site's defenses and get in for processing extremely rich data sources. Some third party tools match supplied e-mail addresses with SNS profiles to collect targeted information. Although most laws and regulations restrict access to private information, attributive information is not properly protected. Conventional laws and regulations do not cover most of the privacy related issues involving SNS. Because, the boundaries of what is public and what is private are not clear in social networking. In most cases, it is hard to decide whether some facts are private or not when a user willingly posts them on a social networking site profile. In most cases the extent of moral and monetary damage is difficult to measure to be subjected to legal action. However, Social Network Sites violate many of the "Fair Information Practices" as set by the OECD and accepted by many countries (OECD,1980). Practical consequences of SNS activities also violate many other national and international rules and guidelines(European Union,1995). Another problem is that, the usage of information is not limited to the specified purposes covered by laws and regulations. Because, the processing possibilities and real intentions

are too broad and unpredictable in the case of information that is available through SNS . For these and similar reasons, most of the legal and institutional efforts for privacy protection do not have the right channels and instruments to refrain SNS and the other actors from violating basic privacy rights of individuals.

6. CONCLUSION

As a result of ever increasing and diversifying online involvement of people, controling and fully protecting one's virtual identity is a very difficult, if not impossible task. The attitudes of SNS have an important share on this situation. On the other hand, positive aspects of SNS and their inevitability for most people cannot be overlooked. Therefore, a compromise is needed between the benefits and potential harms of SNS. There are simple precautionary measures that individuals can take to protect and manage their online identity. Following these and several similar guidelines may help to protect the user's sensitive data to some extent. The privacy control mechanisms developed by social networking platforms are too complicated and far from being effective .Therefore, users themselves need to be aware of privacy risks and must always be watchful on what they post; including photos, content, links and who they should allow to see them. Despite all their complexities, trying to keep up to date with privacy policies and settings of SNS is also a good practice. Most SNS privacy policies now allow applications, groups, etc. to be blocked and/or reported. Use of these options to deny access and any other requests from the unwanted applications or groups may help to limit potential damages that might be caused by online information.

REFERENCES

The European Union, (1995) :Directive on the Protection of Personal Data.

J. He, W. Chu, and V. Liu (2006) :Inferring privacy information from social networks. In Proceedings of Intelligence and Security Informatics,volume LNCS 3975.

Madden,M.,Smith Aaron (2010) :Reputation Management and Social Media. http://pewinternet.org/Reports/2010/Reputation-Management.aspx.

R. Gross, A. Acquisti, and I. H. John Heinz. Information revelation and privacy in online Social networks.In WPES '05: Proceedings of the 2005 ACM workshopon Privacy in the electronic society, pages 71–80, New York.

Facebook Privacy Policy, available online at http://www.facebook.com/policy.php

OECD (1980): Guidelines on the Protection of Privacy and Transborder Flows of Personal Data