Social Networks Privacy Issues That Affect Young Societies

Alireza Azimi and Abouzar Abbaspour Ghomi

Abstract—Youth rush through their PCs, laptops and mobile phone to participate in social networks in developing countries is one thing that you cannot ignore these days. Social networking sites allow millions of individuals to create online profiles and share personal information with vast network of friends and often unknown number of strangers. Social network is somewhere that some think it might work as the leader of revolutions even in political aspects and user’s privacy and information shared by the user is the first target for that appeal. In this article we discuss some privacy issues that can have effect on young societies and also the possible ways of adopting social networks and consequences of it and steps that can be taken to help protecting one's privacy.

Keywords—Privacy, social networking sites, Information revelation, online privacy.

I. INTRODUCTION

In recent years, online social networks has become very popular, many web sites have sprung up where one can meet their offline friends in virtual world of the internet. Services like Facebook, Orkut, and MySpace etc allow people to host their online social networks, people create their profiles in such social networks and share this information with their friends and a vast amount of strangers on these social sites.

And the concern about users’ privacy that can be used for different purposes such as identity theft, or for advertisement markets and other negative intentions and the threat is more likely to be for those developing countries that have a young society and can be the main target for these concerns.

II. EVOLUTION OF SOCIAL NETWORKS

In recent years online social networking has moved from niche phenomenon to mass adoption. Although the concept dates back to the 1960s (with University of Illinois Plato computer-based education tool, see [16]), viral growth and commercial interest only arose well after the advent of the Internet.1 The rapid increase in participation in very recent years has been accompanied by a progressive diversification and sophistication of purposes and usage patterns across a multitude of different sites. The Social Software Weblog2 now groups hundreds of social networking sites in nine categories, including business, common interests, dating, face-to-face facilitation, friends, pets, and photos.

While boundaries are blurred, most online networking sites share a core of features: through the site an individual offers a “profile” - a representation of their selves] (and, often, of their own social networks) - to others to peruse, with the intention of contacting or being contacted by others, to meet new friends or dates (Friendster,3 Orkut4), find new jobs (LinkedIn5), receive or provide recommendations (Tribe6), and much more .It is not unusual for successful social networking sites to experience periods of viral growth with participation expanding at rates topping 20% a month. Liu and Maes estimate in [18] that “well over a million self-descriptive personal profiles are available across different web-based social networks” in the United States, and Leonard, already in 2004, reported in [16] that world-wide “[s]even million people have accounts on Friendster. [...] Two million are registered to MySpace. A whopping 16 million are supposed to have registered on Tickle for a chance to take a personality test.” The success of these sites has attracted the attention of the media (e.g., [23], [3], [16], [4], [26]) and researchers. The latter have often built upon the existing literature on social network theory (e.g., [20], [21], [11], [12]) to discuss its online incarnations. In particular, [7] discusses issues of trust and intimacy in online networking; [9] and [8] focus on participants’ strategic representation of their selves to others; and [18] focus on harvesting online social network profiles to obtain a distributed recommender system.

In this paper, we focus on patterns of personal information revelation and privacy implications associated with online networking. Not only are the participation rates to online social networking staggering among certain demographics; so, also, are the amount and type of information participants freely reveal. Category-based representations of a person’s broad interests are a recurrent feature across most networking sites [18]. Such categories may include indications of a person’s literary or entertainment interests, as well as political and sexual ones. In addition, personally identified or identifiable data (as well as contact information) are often provided, together with intimate portraits of a person’s social or inner life.

III. INFORMATION REVELATION AND ONLINE SOCIAL NETWORKING

While social networking sites share the basic purpose of
online interaction and communication, specific goals and patterns of usage vary significantly across different services. The most common model is based on the presentation of the participant’s profile and the visualization of her network of relations to others - such is the case of Friendster. This model can stretch towards different directions. In matchmaking sites, like Match.com⁸ or Nerve⁹ and Salon¹⁰ Personal, the profile is critical and the network of relations is absent. In diary/online journal sites like LiveJournal,¹¹ profiles become secondary, networks may or may not be visible, while participants’ online journal entries take a central role. Online social networking thus can morph into online classified in one direction and blogging in another.

Patterns of personal information revelation are, therefore, quite variable. First, the pretense of identifiability changes across different types of sites. The use of real names to (re)present an account profile to the rest of the online community may be encouraged (through technical specifications, registration requirements, or social norms) in college websites like the Facebook, that aspire to connect participants’ profiles to their public identities. The use of real names may be tolerated but filtered in dating/connecting sites like Friendster, that create a thin shield of weak pseudonymity between the public identity of a person and her online persona by making only the first name of a participant visible to others, and not her last name. Or, the use of real names and personal contact information could be openly discouraged, as in pseudonymous-based dating websites like Match.com, that attempt to protect the public identity of a person by making its linkage to the online persona more difficult. However, not with standing the different approaches to identifiability, most sites encourage the publication of personal and identifiable personal photos (such as clear shots of a person’s face).

Second, the type of information revealed or elicited often orbits around hobbies and interests, but can stride from there in different directions. These include: semi-public information such as current and previous schools and employers (as in Friendster); private information such as drinking and drug habits and sexual preferences and orientation (as in Nerve Personal); and open-ended entries (as in LiveJournal).

Third, visibility of information is highly variable. In certain sites (especially the ostensibly pseudonymous ones) any member may view any other member’s profile. On weaker pseudonym sites, access to personal information may be limited to participants that are part of the direct or extended network of the profile owner. Such visibility tuning controls become even more refined on sites which make no pretense of pseudonymity, like the Facebook. And yet, across different sites, anecdotal evidence suggests that participants are happy to disclose as much information as possible to as many people as possible. It is not unusual to find profiles on sites like Friendster or Salon Personal that list their owners’ personal email addresses (or link to their personal websites), in violation of the recommendation or requirements of the hosting service itself.

A. Privacy window in developing countries

There is another thing that can affect the way of looking at privacy and that’s is nothing but the believes and traditions of a society, a society in the third world countries generally are conservative about anything related to their privacy and that could origin from the beliefs and disbeliefs, however the new generation of people aren’t that enthusiastic about the traditions or beliefs of the past that could be result of things that are not discussed in this article, and these are the young people that know and live with the new technologies. These groups of people are less sociable and they are connected to an enormous stream of information everywhere they go and of course the social networking sites and they tend to care less about the privacy threats and that would be because of a cycle that is not complete, this cycle include the tool and how to use that tool, there is different kinds of social network each one for different kinds of purposes and how to use each one of them differentiates and having the knowledge to use each one of them matters, because of being the youngest society as consequence being one of the most impressive societies in the world. there is another pattern of behavior that is similar all over the world, the youth prefer social network that is more likely to be the society of their university or office or where they live, and they tend to like social networks that more peoples are familiar. The social network is a large society that the vast majority of whom login to the social networking sites, are waiting to read something new about someone or something and react upon that, this makes it a great set of services that can target the ideological part of someone’s life. To prevent or at least increase the amount of this kind of actions that can be used as a media to lead thousands of dissatisfied people to revolt against their own people and unstable most parts of a normal society, we can localize the social network websites by building up the features of an standard social network that obey a comprehensive set of rules and let the user to protect her own privacy in a doss that is usually lawless in the undeveloped countries, and sometime the regime itself has the double standards on this cases and there are a lot of stories about how personality identification works as a tool to find the suspicious ones by some organizations.

B. Building a digital dossier

When young users build their online profiles, they generally are not concerned about their privacy and publish more personal and sensitive information. Given that the storage costs are declining, it is possible for governments to continuously harvest information and store, later on when these young people enter the professional life which may have sensitive and delicate situations, such information then might become important and can be used in situations where it can be harmful for their public image or relations [3][7][8].

C. Manipulating users

Social engineering methods can also be used in online social networks, it can be used to retrieve more information.
about a user's profile, just by simply asking them, according to [6] by using an automated script about off 250,000 users who were asked to accept a friend request from a Facebook user using the script 75,000 users accepted the request and exposed their full profiles, thus it was deduced that 30 of all Facebook users may be willing to share their private information with a complete stranger.

D. Sharing personal Information

When people share their personal information over a social network, it is not clear who can read the information, can every one read that information? Or only the people from the friend list of the user see that information? But also and more importantly how does this affect the privacy of the user.

Social networking websites are now coming up with new innovative ideas for the users of the sites, Facebook for example now lets users to install applications in their profiles, these applications range from calendars to movie recommendation and review applications, dating, games and so on. Orkut is another example, Orkut is a social networking service owned by Google and thus combines the other services offered by Google, for example users can share their YouTube videos, their Picasa Photo albums, and blogs among other things on their profiles.

With profiles in such social networking web sites users are already sharing so much information, but when a social network combines the resources from other web sites, the privacy of the users can be exposed in a whole new manner.

E. Risks in sharing information

Thus in online social networks privacy can become a serious concern, when people share more information than just their name or age, information like their home address, their pictures and other sensitive information they can expose themselves to various risks. What can be those risks how exposing certain information can lead to those risks, and what can be the steps that can be taken to safeguard against such risks.

IV. Privacy Revelation

Social networking sites share the basic purpose of online interaction and communication, but the specific goals and usage patterns change across different services. The most common scenario is based on the use of the participants profile and the presentation of her/his network of friends. This approach can stretch towards different directions. In dating web sites, like Match.com or Nerve and Salon Personals, the profile is the critical component and there is no network of friends. In blogging sites like LiveJournal, Blogger etc profiles become secondary, networks may or may not be visible, blog entries take a central role. Online social networking thus can change into classifieds in one direction and blogging in another direction. The way people share information on these online social networks is very different and depends on the site under consideration. Using a real name to present an account profile to the members of an online community may be encouraged on sites like Facebook which focus on college students [14], such networks try to connect participants profile to their real life identities. Other web sites like Friendster tolerate use of real name; such sites create a thin layer of anonymity between the real life and online profile by making only a part of the real name visible on the online profiles, i.e. showing only the first name while hiding the last name. Other web sites like match.com discourage publishing real names and other personal contact information; such sites attempt to protect the real life identity of a person by making its link to the online profile more difficult.

Most social networking sites encourage the publication of personal and identifiable personal photos. The type of information revealed or found often revolves around different hobbies and interests, but can go to many other different directions, like information such as current and previous schools and employers; private information such as drinking and drug habits and sexual and political preferences and orientation, Relationship information, for example who is the girl friend / boy friend, or spouse etc.

The visibility of information on online social networks changes all the time. In some sites any member may view any other member’s profile. On other social networking sites access to personal information may be restricted to people that are part of the direct or extended network of the profile’s owner. However the visibility control of the information changes across different sites. People generally are happy to disclose as much information as possible to as many people as possible [6].

Different fields used in online profiles and percentage of users filling them [5].

1. 93.8% of users disclose their sex.
2. 83.3% of users disclose their hometown.
3. 87.1% of users disclose their high school.
4. 45.1% of users disclose their home address.
5. 59.8% of users filled out the About Me field.
6. 67.8% of users disclose their Instant Messaging address.
7. 83.8% of users disclose their birthday.
8. 92.3% of users disclose their email address.
9. 78.5% of users disclose their relationship status.

According to a report published by PEW Internet & American life project [10]:

1. 55% of online teens have online profiles, 45% of the online teens don’t have profiles online
2. 82% of profile creators have included their first name in their profiles
3. 66% have included photos of their friends
4. 61% have included the name of their city or town.
5. 49% have included the name of their school.
6. 40% have included their instant message screen name.
7. 40% have streamed audio to their profile.
8. 39% have linked to their blog.
9. 29% have included their email address.
10. 29% have included their last names.
11. 29% have included videos.
12. 2% have included their cell phone numbers.
13. 6% of online teens and 11% of profile-owning teens post their first and last names on publicly-accessible profiles;
14. 3% of online teens and 5% of profile-owning teens disclose their full names, photos of themselves and the town where they live in publicly-viewable profiles.

A. How much for my privacy

As we discussed about localization of social network for a specific society, we can notice that lack of comprehensive rules in some cases can cause violating users privacy rights and one of the obvious example is cloob12, this site which is titled by “Iranian social network” is violating the basic rights of the users to protect their own privacy, this website has some features like who saw your profile, finding out who login to the website, being invisible, and each one of them are enabled by paying different amounts of money to the website. This kind of services could be result of loosely tight rules and also lack of acknowledgment of users about their own rights, and being the target for complicated markets. We can prevent users from these websites by informing them, how their personal information can be used by others to maintain a beneficial goal.

B. Social network Theory and Privacy

The relation between privacy and a person’s social network is multi-faceted. In certain occasions we want information about ourselves to be known only by a small circle of close friends, and not by strangers. In other instances, we are willing to reveal personal information to anonymous strangers, but not to those who know us better.

Social network theorists have discussed the relevance of relations of different depth and strength in a person’s social network (see [11], [12]) and the importance of so-called weak ties in the flow of information across different nodes in a network. Network theory has also been used to explore how distant nodes can get interconnected through relatively few random ties (e.g., [20], [21]).

The application of social network theory to the study of information revelation (and, implicitly, privacy choices) in online social networks highlights significant differences between the offline and the online scenarios. First, offline social networks are made of ties that can only be loosely categorized as weak or strong ties, but in reality are extremely diverse in terms of how close and intimate a subject perceives a relation to be. Online social networks, on the other side, often reduce these nuanced connections to simplistic binary relations: “Friend or not” [8]. Observing online social networks, Danah Boyd notes that “there is no way to determine what metric was used or what the role or weight of the relationship is.

While some people are willing to indicate anyone as Friends, and others stick to a conservative definition, most users tend to list anyone who they know and do not actively dislike. This often means that people are indicated as Friends even though the user does not particularly know or trust the person” [8] (p. 2). Second, while the number of strong ties that a person may maintain on a social networking site may not be significantly increased by online networking technology,

Donath and Boyd note that “the number of weak ties one can form and maintain may be able to increase substantially, because the type of communication that can be done more cheaply and easily with new technology is well suited for these ties” [9] (p. 80).

Third, while an offline social network may include up to a dozen of intimate or significant ties and 1000 to 1700 “acquaintances” or “interactions” (see [9]), an online social network can list hundreds of direct “friends” and include hundreds of thousands of additional friends within just three degrees of separation from a subject.

This implies online social networks are both vaster and have weaker ties, on average, than offline social networks. In other words, thousands of users may be classified as friends of friends of an individual and become able to access her personal information, while, at the same time, the threshold to qualify as friend on somebody’s network is low. This may make the online social network only an imaginary community. Hence, trust in and within online social networks may be assigned differently and have a different meaning than in their offline counterparts. Online social networks are also more leveled, in that the same information is provided to larger amounts of friends connected to the subject through ties of different strength. And here lies a paradox. While privacy may be considered conducive to and necessary for intimacy, trust may decrease within an online social network. At the same time, a new form of intimacy becomes widespread: the sharing of personal information with large and potential unknown numbers of friends and strangers altogether. The ability to meaningfully interact with others is mildly augmented, while the ability of others to access the person is significantly enlarged.

V. PRIVACY IMPLICATIONS

It would appear that the population of Facebook users we have studied is, by large, quite oblivious, unconcerned, or just pragmatic about their personal privacy. Personal data is generously provided and limiting privacy preferences are sparingly used. Due to the variety and richness of personal information disclosed in Facebook profiles, their visibility, their public linkages to the members’ real identities, and the scope of the network, users may put themselves at risk for a variety of attacks on their physical and online persona. Some of these risks are common also in other online social networks, while some are specific to the Facebook.

A. Fragile Privacy Protection

One might speculate that the perceived privacy protection of making personal information available only to members of a campus community may increase Facebook users’ willingness to reveal personal information. However, the mechanisms protecting this social network can be
Adding to this the recognition that users have little control over the composition of their own networks (because often a member’s friend can introduce strangers into that member’s network), one may conclude that the personal information users are revealing even on sites with access control and managed search capabilities effectively becomes public data.

B. What technology can do to protect privacy

Social networks can make it easier for users to use privacy controls, so that even a new novice user can control what other people can see from their profile. When a user creates a new account on a social network the default settings should be so that the private profile entries are hidden or even the whole profile is hidden unless the user chooses to publish his profile to public or his friends later on. Warnings should be displayed and online easy to understand help should be available whenever user chooses to change any of the privacy settings. CAPTCHAs [1] can be used by the social networking sites to prevent information harvesting by automated bots, although these can be an annoyance for normal users however.

These can be quite useful when guarding against automated scripts.

VI. CONCLUSIONS

Online social networks are much vast and much more loose than real life, some people in such networks have hundred of friends in their profiles and may be even thousands through extended profile but hardly any of those are real friends, most of them are complete strangers, and still personal and sometimes sensitive information is freely and publicly available. Based on the information provided in their profiles, users expose themselves to various physical and online risks, these risks are not unique to just one social network, and it is common to all of the social networks.

When participating in such social networks, users should be vigilant and should take special precautions before they expose their identities, protecting privacy rights should be defined as a stable rule for social networking websites to be obeyed by them, technology should make it easy for users to protect their privacy, the privacy controls should be well placed an easy to use, so any one can use them. And if we want healthier society we should omit the dogma that is result of some untrusted websites and rules that has been abused by governments or other organizations. Social networking is still evolving, new innovations and ideas are coming out rapidly, social networks are now targeting different mediums, mobile media is one such medium, in the future we may see that social networking moves from web sites to handheld devices and technologies Bluetooth and GPS may play a crucial role in mobile social networking arena, however it remains to be seen how users privacy will be handled when such new ideas are implemented.

REFERENCES