Analysis of LinkedIn Privacy Settings
Are they Sufficient, Insufficient or Just Unknown?

Pilar Manzanares-Lopez, Juan Pedro Muñoz-Gea and Josemaria Malgosa-Sanahuja
Department of Information Technologies and Communications, Antiguo Cuartel de Antigones Campus Muralla del Mar s/n, Technical University of Cartagena, E-30202 Cartagena, Spain

Keywords: Privacy, Professional Social Networking, LinkedIn.

Abstract: Internet-based applications give users an easy way to communicate with each other on a scale and rate unseen in traditional media. Among them, the professional social networking sites (with LinkedIn as one the most widespread platforms) offer a useful way to create and maintain a professional contact network. LinkedIn is also a self-promotion tool, where employees, industries and communities get in touch. In this scenario, it seems logical to consider privacy as a fundamental subject. Controlling who can see our data may avoid that our information reaches our boss when we are looking for a job, a competitor, or even former or present work colleagues with whom we have had some conflict. This work analyzes deeply the privacy settings offered by LinkedIn, and also analyzes the privacy concerns among the users, examining how these concerns correlate to the knowledge of the privacy settings and the adequacy of their use.

1 INTRODUCTION

Social media is defined as a group of Internet-based applications that built on the foundations of Web 2.0 and allow the creation and exchanges of user-generated content (Kaplan and Haenlein, 2010). They give users an easy-to-use way to communicate with each other on an unprecedented scale and at rates unseen in traditional media (Gundecha et al., 2011).

Among the variety of social media, social networking sites are platforms that enable users to interconnect by creating personal profiles (a representation of themselves), inviting friends and acquaintances to have access to those profiles, and sending e-mails and instant messages between each other. The largest social networking websites are Facebook and MySpace. Also belong to this type LinkedIn and Xing.

LinkedIn and Xing are focused towards business users who would like to maintain and extend their professional networks. Thus, profiles are usually strictly professional, including education and experience. In this scenario, it seems logical to consider that users pay more attention to the information they publish about themselves, as well as give more importance to the issues of privacy and security. Controlling who can see our data may avoid that our information reaches, for example, our boss when we are looking for a job, a competitor, or even former or present work colleagues with whom we have had some conflict.

The issues of privacy and security in the framework of online social networks have been studied by the research community (Gross and Acquisti, 2005)(Acquisti and Gross, 2006)(Krishnamurthy and Wills, 2008)(Fogel and Nehmad, 2009)(Rizk et al., 2009)(Stutzman and Kramer-Duffield, 2010)(Krasnova et al., 2010)(Liu and Gummadi, 2011)(Nayak and D'Souza, 2011)(Egelman et al., 2012)(Johnson et al., 2012)(Staddon et al., 2012)(Johnson, 2012)(Magazine, 2012). Some works analyze users' awareness, attitudes, and privacy concerns in social network sites from a generic point of view, although most of the studies are focused on Facebook.

To the best of our knowledge, no previous work has addressed this subject in a professional social networking website. We have chosen LinkedIn because of its overwhelming popularity, with more than 225 millions of users. Its main features from a privacy perspective are scarcely summarized in (Barrigar, 2009). In (Skeels and Grudin, 2009), a very interesting study of the benefits and utility of LinkedIn is exposed, but privacy aspects are not covered.

The main objective of this work is to analyze the privacy concerns among the users of LinkedIn (are LinkedIn users concerned about privacy?), examine how these concerns correlate to the knowledge of privacy settings (do LinkedIn users manage their privacy

Manzanares-Lopez P., Muñoz-Gea J. and Malgosa-sanahuja J..
Analysis of LinkedIn Privacy Settings - Are they Sufficient, Insufficient or Just Unknown?.
DOI: 10.5220/0004795602850293
In *Proceedings of the 10th International Conference on Web Information Systems and Technologies* (WEBIST-2014), pages 285-293
ISBN: 978-989-758-023-9

settings correctly?) and observe the behavior the users take to protect their privacy (does the LinkedIn users behavior reflect their concerns?, do their privacy settings match their intentions?).

Social networking providers are often viewed as the source of privacy threats. Users fear that they can use their personal information for marketing purposes as well as share it with third parties. However, users may also face specific privacy-related dangers rooted in the public availability of their data.

The rest of the paper is organized as follows: section 2 describes the evolution of privacy subjects in the field of social networking websites. Section 3 describes briefly the website and analyzes deeply the offered privacy settings. The methodology used to collect the data to answer the formulated questions, and the analysis of the obtained data are described in Section 4. Finally, section 5 concludes the paper.

2 PRIVACY IN SOCIAL NETWORKING WEBSITES

Danah Boyd, one of the most influential women in technology, asserted that social media has prompted a radical shift from a "private by default, public through effort" world to "public by default, private through effort" one. In 2010, Facebook CEO M. Zuckerberg justified his company's decision to switch defaults to "everyone" with the logic that the youngest generation no longer cares about privacy. Similarly, Google CEO E. Schmidt claimed that if you have something that you don't want anyone to know, maybe you shouldn't be doing it. This thought was also shared by the founder of LinkedIn, when in 2010 affirmed that privacy is an issue for older people as younger people perceive the value of connection and transparency.

In this new scenario, privacy not only entails the personal action of deciding what we want to share and with whom, but also it is related to the knowledge, understanding and use made by people of the privacy settings offered by the social networking site.

One of the first studies about privacy revealed that FB users (basically university students) provided large amount of personal information, but privacy preferences were used by a small number of users (only the 0.06% of them) (Gross and Acquisti, 2005). A later study showed some changes. Although a relative majority of users was aware of the visibility of their profiles, still a significant minority wasn't (Acquisti and Gross, 2006).

In short time, Facebook stopped of being a social networking site limited to university students, and becomes the worldwide and intergenerational social networking website that we use today. In addition to a more wide variety of users, the increase of attention to privacy matters in the media caused that users increased the interest for the privacy subjects.

Although more users utilize the available privacy settings, researchers continue to identify inconsistencies between users' sharing goals and their privacy settings. (Liu and Gummadi, 2011) collected the privacy settings for all the uploaded content of 200 FB users, and reveled that 36% were shared with default privacy settings, a fraction higher than users who reported that this was the desired setting (20%). In addition, it outlined a more worrying conclusion. Even for contents for which the privacy settings have been modified, the modified privacy settings matched users expectations less than 40% of the time. This strongly suggests that users are having trouble to correctly configuring their privacy settings.

A study to evaluate how FB users react to limitations in the privacy controls was described in (Egelman et al., 2012). The results demonstrate that using the existing privacy controls many participants failed to complete the task, and that only ambiguity detection with actionable guidance improved participants' ability to complete the tasks.

(Johnson et al., 2012) measured the users' attitude toward privacy concerns on FB. They concluded that a great part of participants (86.2%) were either unconcerned with the threat of strangers viewing their content in FB, or they were able to mitigate those concerns through the use of global privacy settings. Thus, they belive that strangers are no longer the greatest thread. From their data, they conclude that threats from within users' friend networks are more concerning (because they are much less likely to be mitigated through the use of privacy settings).

In our opinion, this last conclusion is, perhaps, much more interesting in the field of LinkedIn, where our connections are not only friends or close colleagues, but also former and present bosses, colleagues and acquaintances in the work environment.

3 LinkedIn

The purpose and use of LinkedId will depend on each user, among its main objectives there is the self-promotion and maintenance of business and professional contacts. LinkedIn can be a great place to network with others in your career field and reconnect with some of your favorite former co-workers. It can be also considered as a free database of employees, industries and communities.

Controlling who can see your data or what infor-

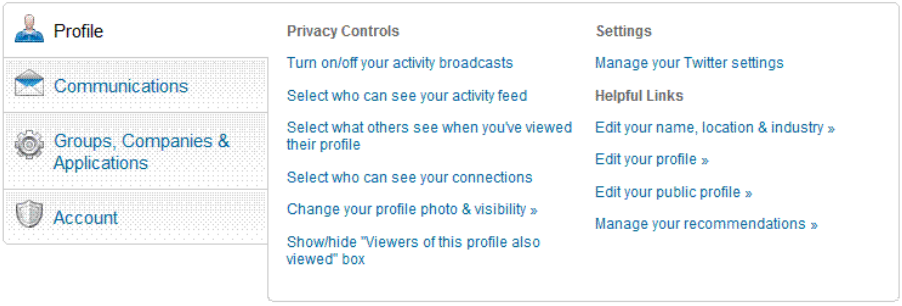

Figure 1: Settings page.

mation can be extracted from your actions and activities in this site, may avoid that your information reaches unwanted ears (for example, to your boss when you are looking for a new job) or falls into wrong hands with dangerous consequences for you.

3.1 A Brief Description of the LinkedIn Website

A key aspect to understand the LinkedIn privacy settings is to be clear about the difference between the user Homepage and the user Profile. When a user signs in on LinkedIn, the homepage is shown. There, a list of updates informs user about new connections of user's contacts, companies that are followed by user's contacts, modifications made by user's contacts to their profiles, about new groups joined by user's contacts, about information shared by user's contacts, about jobs, and of course about its own updates.

Unlike the user homepage, the user profile shows personal and professional information that it is wanted to be shared with others. All registered users can view a user profile, when they connect with him, search his name or click his name in an update, group, or other areas. The Profile can list your activities in LinkedIn (Activity Feed section), your education, past work history, and current and past projects (Background section), groups and associations (Groups sections), and more.

On the other hand, the user profile must be differentiated of the user public profile. The Public Profile appears when people search for a user using a public search engine like Google, Yahoo!, Bing, etc., that is, without being registered in LinkedIn.

Although professional, LinkedIn is a social networking site where users maintain a group of contacts. To facilitate the joining of new contacts to our network, LinkedIn offers two tools: the "People You May Know" list, and the "Who's Viewed Your Profile" list, which offers information about who has been looking at your profile in the last 90 days.

Finally, LinkedIn defines different levels of connections among users. 'Your connections' are 1st-degree connections, that is, people you're directly connected to because you have accepted their invitation to connect, or they have accepted your invitation. In addition, LinkedIn defines 'your network', that is made up of your 1st-degree, 2nd-degree (people who are connected to your 1st-degree connections), and 3rd-degree (people who are connected to your 2nd-degree connections) connections and fellow members of your LinkedIn Groups.

3.2 Privacy Settings

Users can change their account information and settings, through the settings page (https://www.linkedin.com/settings) or moving the control over the photo in the top right of the homepage and selecting "Privacy&Settings"[1].

Most of the privacy controls are located on the Profile tab (see figure 1). Below, the most important aspects of each one are described.

Turn on/off your Activity Broadcast. Some actions on LinkedIn trigger activity updates (also called activity broadcasts). By this option, the user decides whether or not to share these actions by means of activity updates. This control is on by default.

First of all, it is important to realize that this option only controls the generation of updates that will be displayed on the homepage of the others. Although this option is set to off, all those changes will be listed in the Activity Feed section of the user profile.

When a user accesses to this setting, LinkedIn advertises the following: *"Note: you may want to turn this option off if you are looking for a job and don't want your present employee to see that you're updating your profile"*. Although this note seems to be clear, a question is often repeated in LinkedIn discussion websites: if users turn off the activity broadcast,

[1]LinkedIn version at 24th. June, 2013.

make changes on their profiles and then turn on the activity broadcast, LinkedIn will provide feedback and report any changes made during the time the option was off? Clearly, the answer is negative.

Usually when a user is looking for a job, the profile is updated but also recommendations are posted. Regarding that, it is interesting to point out that an activity update is generated not only when a user makes a recommendation, but also when the user accepts a recommendation made by other LinkedIn member.

Finally, although the control description does not detail this aspect, joining a group (which gives tracks about our interests) or updating your photo generates an update although the control is turned off.

In our opinion, a possible improvement related to this control could be to offer a greater granularity. Thus, instead of activating or deactivating the generation of updates on the whole, users could select activate or deactivate the generation of updates associated with a certain activities in particular.

Select who can see your Activity Feed. A user can select who can see its Activity Feed section. The values are: 'Your connections' (the default value), 'Everyone', 'Your network', and 'Only you'.

Usually changing this control is associated to the previous setting. If you don't want to trigger updates to prevent your contacts being alerted about changes in your profile, you will not be interested in they can access to your profile and know, at a glance, your activities in the Activity feed.

Select what Others see when you've Viewed their Profile. This control helps you to protect your privacy when you are viewing other users profiles, selecting which information about your identity is shown. There are three options: 'Your name and headline' (Recommended and default option), 'Anonymous profile characteristics such as industry and title', and 'You will be totally anonymous'.

As can be seen, the first option is fully open, while the other two offer some degree of anonymity. The chosen value not only determines what information about us will get the owners of the profiles we have visited, but also determines what information we will get about the users who have visited our own profile.

If your LinkedIn account type is Basic and you decide to hide either partially or totally your identity (options 2 and 3), you will not get information about who has viewed your profile. The 'Who's viewed your profile' box will indicate the number of users who viewed your profile. But when you click on the link, the detailed information is not available. However, if you do not hide your identity, Profile Stats is available, offering the last 5 results of who's viewed your profile, the number of visits to your profile and the number of times you've appeared in search results.

On the other hand, the third option could be misleading. Although it is said 'you will be totally anonymous', the owner of the profile you have visited will see that 'Someone on LinkedIn' has viewed his profile, and this sentence is a link to a page called 'One of these people viewed your profile', where just a reduced set of 10 profiles are listed.

If your LinkedIn account is Premium, Profile Stats Pro is available independently of the selected degree of anonymity. Profile Stats Pro shows the full list of who's viewed your profile (you won't see additional information about a profile viewer if they've chosen to remain anonymous in their privacy settings), trends, total profile visits, keywords used to find your profile, number of times you've appeared in search results and industries of people viewing your profile.

In this case, the anonymity offered by the last two options is complete. Now, if option 3 is chosen ('totally anonymous'), the owner of the profile you have visited will see that 'LinkedIn Member' has viewed his profile, but now this sentence can not be clicked.

Select who Can See your Connections. Using this control, user can choose to show or not his entire list of connections. There are two options: 'your connections' (the default value), and 'only you'.

As advertised by a note, it is important to point out that although 'Only you' option is selected, people will always be able to see your shared connections.

On the other hand, users could think that choosing the 'only you' option, their list of connections will be safe. However, as described in (Staddon, 2009), that is not completely true. Using the LinkedIn Search engine, a user can discover, if not all, a large part of the list of connections of another user whose configuration aims to keep the list hidden. The procedure is briefly described below.

Consider that user A (the attacker) is a connection of user B (the target). B has set this privacy control to 'only you'. However, using the profile attributes configured by B, A will be able to discover part of B's contacts. For that, A must make note of the main attributes corresponding to the 'current', 'previous' and 'education' fields in user B profile. Next, A will use each of these attributes in the keyword field in the LinkedIn search tool. Then, for any returned user labeled '2nd', user A must click on the 'shared connections' link and check if B is listened there. If B is found, that user is a contact of B. This data mining process generates an incomplete list of B's contacts, which can be widen if the process is repeated using the attributes of the discovered contacts.

The cost of this procedure results in a repetitive task of introducing attributes and checking, one by

one, all the results. The higher the attacker's network of contacts, the longer the process. A large network will tend to lead to more hits for a given search, thus making the contacts of the target user harder to find.

Finally, the amount of connections discovered by the attacker is related to its type of LinkedIn account. If the attacker account is Basic, although the search returns more than 100 results, the attacker could only check the first 100 ones. If the account is Business, the number of results that can be checked increases to 300, to 500 if Business Plus, an to 700 if Pro Account.

Change your Profile Photo and Visibility. Users can upload a photo, which will be shown in their profile and also in the messages they send. A user can choose if the profile photo is visible to 'my connections', 'my network' or 'everyone' (the default value).

In our opinion, this control creates another point of confusion. Users who want that only their connections are able to see their pictures, would select this option, and trust on that nobody else can see the photo. However, this option only affects the LinkedIn profile, and not the Public profile. Although this control is used, the upload of the picture to the LinkedIn profile activates the showing of this photo in the public LinkedIn profile to everyone. If the user does not want to display the photo in the public profile, the corresponding control must be explicitly set.

Show/hide "Viewers of this Profile also Viewed" box. The "People also viewed" box, on the right side of the profile and homepage, shows some of the other profiles that viewers of your LinkedIn profile have also looked at. By this control, you can show (the default value) or hide this box. However, it is important to notice that disabling this option involves that your name won't show up in the "People Also Viewed" box on anyone else's profile.

LinkedIn advises that if you want to increase your visibility, keeping the module active can help potential employers, clients, recruiters and headhunters find your profile. By removing this module, you may decrease your visibility. However, the opposite can also occur. A potential employer could use the list shown in the "People also viewed" box, as a list of similar profiles that have been visited by other employers, that is, a list of competitors.

All the controls described up to now are located on the Profile tab and grouped under "Privacy Controls" header. However, another feature related to privacy is situated also on the Profile tab, but under "Useful Links" header (see figure 1).

Edit your Public Profile. Users can select 'Make my public profile visible to no one' or 'Make my public profile visible to everyone', the default option. In the last case, a user can choose what information will be viewable, selecting a combination of basic information (name, industry, location, recommendations), profile picture, headline, current positions, education, additional information and interested in.

Finally, another control related to privacy is located on the Groups, Companies&Applications tab, under the "Groups" header.

Turn On/off Notifications when joining Groups Users can set if they want to update to their network when they join a group. The default option is 'yes'.

The joining to new groups can give clues about our interests in new professional issues, for example when you are looking for a job. Thus, these notifications may be undesirable when our employers belong to our network. For this reason, LinkedIn advertises that *"You may want to turn this option off if you're looking for a job and want to be more private about which groups you join"*. However, it is important to remind that although the activity updates are disabled, a user always can visit our profile to check our information and updates.

4 METHODOLOGY AND RESULTS

The main objective of this work was to analyze the privacy concerns among the users of LinkedIn, examine how these concerns correlate to the knowledge of privacy settings and observe the behavior these users take to protect their privacy.

To collect data to answer these questions, we designed a questionnaire about the use of LinkedIn and in particular, privacy concerns, and which actions are taken by respondents to address these concerns[2].

The initial target population was composed of friends, former and current work colleagues, and acquaintances of the authors of this work. They received an invitation via e-mail to complete a web-based questionnaire. In addition, the invitation friendly requested their help in spreading the questionnaire, encouraging the receivers to forward the invitation to their contacts. They were informed about the objective of the study and were also informed that all information they provided would remain confidential.

A total number of 75 replies were collected during a period of 10 weeks in the middle of 2013. We expected a higher number of participants: we directly contacted with 500 people, each with an average of

[2]The questionnaire is available in https://docs.google.com/forms/d/1aTf1DlXakB8R9zfHS98LVtBWQQIYmz_M0uhCs6KBl1s/viewform

Table 1: Demographic characteristics of the sample and some data about the use of LinkedIn.

Question	Results
Q1. Gender	
Male	78.6%
Female	21.33%
Q2. Age	
under 21	0.00%
between 22 and 35	6.76%
between 36 and 50	86.49%
over 50	6.76%
Q3. Current professional status	
current or recent student	5.33%
worker	89.33%
unemployed	5.33%
Q5. Type of LinkedIn account	
Basic	97.30%
Premium	2,70%
Q6. How often do you visit LinkedIn?	
Several times per day	5,33%
Daily	22,67%
Occasionally	50.67%
Have profile, rarely use	16.0%
Have profile, never use	5.33%
Q11. Approximately, how many LinkedIn contacts do you have?	
less than 50	29.33%
between 50 and 100	22.67%
between 100 and 200	26.67%
more than 200	21.33%

100 friends, the collaboration in forwarding the questionnaire was asked, and other social networks were used. However the collected data allow us to extract very interesting conclusions, as described later.

Anticipating those conclusions, the number of participants is, in turn, a first and important finding. As it will be confirmed with the analysis of the results, anonymity in LinkedIn, the knowledge and use of privacy settings, and the consequences are unknown issues to users of LinkedIn, and even undervalued subjects. In our opinion, that is probably the reason the participation was low.

Table 1 shows demographic characteristics of the sample, and also general information about the use of LinkedIn. Most of the respondents are between 36-50 years old (86.49%). The number of users over 50, range that as the previous one belongs to the working age range, is much lower (6.76%). This large difference could be motivated by the technological gap between generations. The percentage of users within the range 22-35 years old, that corresponds to recent graduated users or in their first years of work, for which a tool like LinkedIn would be very useful for job search or promotion, is also low (6.76%).

Table 2: Statistics about non-professional information provided by users in their profiles.

Question	Results
Q7. Your profile name is...	
my real name	84.0%
my real name, but not complete	14.67%
a fake name	1.33%
Q8. Your profile photo is...	
No image	30.67%
I'm easily recognizable	68.00%
Semi-identifiable	1.33%
Group image	0.00%
Joke image	0.00%
Q10. Do you provide any fake information in your LinkedIn profile?	
Yes	5,33%
No	94.67%

One of the centerpiece of a social networking website's privacy posture is the privacy policy. In LinkedIn, the privacy policy is reachable by a link situated in the footer of the website. In spite of its importance in terms of privacy, a first result extracted from the data collected in the study is that only the 16% of respondents affirm that have read the LinkedIn privacy policy, and even 4% of participants affirm that they didn't know that the privacy policy exists.

Before evaluating in detail the privacy related results, we consider important to discuss the result from Q23 (*Do you feel that your information in well-protected by LinkedIn?*). Half of the respondents consider that their information is not well-protected. That is, the LinkedIn users still view the online social network providers as a source of privacy threats.

Table 2 shows statistics about non-professional information provided by respondents in their profiles. Almost 100% of them use their real name, and only one participant uses a fake name. Although it is a low percentage, 5.33% of respondents admit that they provide some fake information on the LinkedIn profile.

If we consult the existing literature in the writing of a traditional c.v., we can see that, depending on the geographical area, it is considered appropriate or not to include a picture. In Anglo-American contries, it is recommended not to include your picture, to avoid the possibility of being discriminated against for any reason associated with our appearance (sex, race, ...). However, in Spanish-speaking countries, a photo is generally expected at the top of the c.v.

This decision should be reconsidered in the new scenario created by the emergence and successful of professional social networking sites. Experts highlight that you are seven times more likely to have your

profile viewed if you have one (Kane, 2013). Another study reveals that recruiters spend an average of 19% of their time on your LinkedIn profile simply viewing your picture (Sullivan, 2013). Analyzing the results, the 30.67% of respondents indicated that they don't include a photo.

LinkedIn privacy settings not only allow users to decide if including or not a profile photo but also controlling its visibility. Q27 (*Do you think that it is positive that everyone can see your profile photo?*) measure the need of this privacy option according to the users perception. The 69.86% think that is positive, the 15.07 % think that is not positive and have limited the visibility, and the 15.07 % think that is not positive and they would like to limit the visibility.

However, in our opinion, it is also interesting to analyze the relationship between that perception and the inclusion of a photo in their profile. First of all it is interesting to realize that the 47.82% of participants who don't include a photo, consider positive its inclusion even if everyone can see it. Given that laptops, tablets and smartphones have integrated cameras, a possible improvement of LinkedIn could be the inclusion of a built-in tool to take and upload a photo when a user creates a LinkedIn account, instead of having to use an already existing one. This functionality would facilitate and encourage the use of a photo in the LinkedIn profile. The 21.74% of participants who do not include a photo indicate that they would like to limit the visibility, and 26.08% have decided to limit the visibility, just not using a photo. In regards to respondents who include a photo but do not consider positive that everybody could see it, slightly more than half do not know how to limit it.

The procedure to limit the visibility of the profile photo is extremely simple. The window, from which you upload a photo, asks you if your profile photo is visible to 'your connections', 'your network' or 'everyone' (the default option). However, in our opinion, this privacy setting could be confusing, since it is not clear if this control also affects to the public profile. Asked by this detail, our hypothesis is corroborated due to the fact that a high percentage of users do not know that the visibility of the photo in the public profile must be configured in other place (64.38%).

The existence of a LinkedIn profile and a public LinkedIn profile allows to configure in a different way the visibility of our information within and outside the LinkedIn network. Analyzing the obtained answers, it can be concluded that more than 80% of respondents do not feel the need to restrict the visibility of its public profile (Q12). For those that want to restrict the visibility of the public profile, only about half know how to do it. Q16(*Are you OK with (a) your classmate/collegues (b) your professor/boss (c) an employer (d)acquaintances (e)strangers looking at your LinkedIn profile?*) also asks about the need of profile visibility control, but now, in the LinkedIn network scope. From the results, Q16.(a) 97.33%, Q16.(b) 94.67%, Q16.(c) 98.67%, Q16.(d) 97.33%, Q16.(e) 90.67%, it can be observed that whatever the relationship with the visitor of the LinkedIn profile, less than 10% of respondents are bothered with the fact that the profile is visited. Comparing the results of Q12 and Q16, it can be inferred that the majority of LinkedIn users do not care that their profiles are completely visible, with even less concern if the visit is done from the own LinkedIn network.

Previous questions had as objective to evaluate the user attitude to the sharing of its profiles, from a global viewpoint. However, LinkedIn is not a simple website where to upload a digital version of our curriculum. In fact, our actions and activities, our contacts and a variety of data offer additional information about us. Only 16% of respondents affirm that they are concerned about the fact that people they know can obtain information about them from their LinkedIn activities. However, this percentage doubles if the observers are strangers.

LinkedIn allows to control the visibility of the Activity box, and also the generation of activity updates. Asked about both issues, approximately 80% of respondents affirm that they didn't know the former control, and approximately 70% affirm that they didn't know or were wrong with respect to the latter. Considering only those respondents that correctly defined the privacy setting "Turn on/off your activity broadcasts", the 27.27% of respondents indicated that they didn't know the existence of this option, 40.90% consider unnecessary its use, and only the 31.81% affirm that they have used this control.

Joining a group generates an update although the control is turned off. Asked about this detail, only one of them claimed to know this detail and how to modify the diffusion of this activity.

We have just analyzed the need and knowledge of the users about the visibility of their LinkedIn activities shown in the Activity Feed section. However, there are other actions that are not included in that section but offer information about us, and therefore, they are directly associated to privacy. On one hand, information generated from the visits made by users to other profiles, and on the other hand, information obtained from the list of connections of a user.

More than 90% of respondents want to know who has visited its profile. However, only the 61.33% do not care that the owners know that you have visited their profiles. That is, when the user is the agent of

the action, the privacy requirement increases. As previously mentioned, a privacy setting allows to control how our identity is shown. Asked about the knowledge of this control, it is very interesting to remark that, although more than half of respondents would prefer not to show its identity when consulting other profiles, a similar percentage are unaware of this option (concretely, the 68.92% do not know what information about them is shown when they visit a profile, the 34.32% have selected the option 'Name and Headline', the 5.41% have selected the 'partially anonymous' option, and the 1.35% have selected the 'totally anonymous' option). Finally, it is interesting to note that even those who know this control, largely are unaware of the result of using some kind of anonymity.

Next, we are going to analyze privacy concerns of users related to their connections. First, we would like to verify the need for the users of the privacy setting that allows to show or hide our list of connections. As in previous questions about other privacy controls, around the 60% of respondents do not consider negative that the list of connections is visible. Among the users that consider necessary to control the visibility, just 17.85% have hidden the list. An easy way to widen our list of connections is making use of the 'People you may know' tool. Due to the fact that we could appear as a possible contact of others, this tool affects our privacy. Observing the results (the 72% of respondants have added people using the 'People you may know' box), this tool is considered very useful and. In addition, a large majority (93.33%) of the respondents are not worried of appearing there.

Finally, the last question of the survey was on open question where the respondents were invited to indicate any privacy setting that they would like to establish and which is not currently offered in LinkedIn. Next, the contribution of participants are listed:

- *"I think that activities related to job search (headhunters, groups, following a company) should have a specific labelled or category which allows to easily avoid its broadcast."*
- *"I would be interesting to be able to manage the visibility of our information with a tool or concept such simple and intuitive as the Google 'circles'. I have created groups in LinkedIn, but its usage is not so easy."*
- *"I would like complete control over privacy."*
- *"Turn off activity broadcast means turn of ALL activity. Some of my activity still shows up for connections in the home feed."*
- *"I would like that LinkedIn were not so 'stool pigeon' as Facebook."*

However, some participants use this question to Zuckerberg and Schmidt:

- *"No, I don't care. I have nothing to hide. Being a free service, although with all their limitations, I think that it is wonderful."*
- *"The truth is that I have not been interested in the privacy settings of LinkedIn, so I don't know which are offered and which not."*
- *"I use this social networking site to make public the information I want to share with others. People who see and consult my information, the more the merrier. I think the LinkedIn is a tool which offers professional advertising that can become useful for me. I only upload what I want to be visible of my professional activity."*
- *"No. I think that it is useful to the professional promotion. You only must be careful with the information you upload, period."*

5 CONCLUSIONS

The first objective that we set in this work was to analyze the privacy settings offered by LinkedIn, mainly those which are oriented to allow users to control the visibility of the data and the actions they make on the professional social networking site. Through this analysis, we have been able to identify aspects that, in our opinion, are not sufficiently clear and could involve difficulties or even cause confusion.

On the other hand, we have been able to answer the questions posed in the objectives of this work. As a global conclusion, it can be affirmed that a considerable percentage of LinkedIn users are not worried about the privacy. Asked about the fact that their photos, profiles or their activities could be visible and known by colleagues, bosses, acquaintances or even strangers, a great majority do not express concern. However, approximately half of the participants consider that their information is not well-protected by LinkedIn. Users still continue identifying the social networking provider as the problematic agent which risks their privacy and security. However, users do not identify their own actions and choices (what and how they share their information) as a key aspect related to privacy and security. The above conclusion supports another one deduced from the conducted study: there is an important ignorance of the privacy settings offered by LinkedIn. Even considering those users who show interest and who have used some controls, there are constraints and consequences related to the used settings that are out of their knowledge.

Although it goes against the "public by default, private through effort" policy, which is assumed in this new online scenario, LI and other similar websites, should improve the way in which users perceive how their data are protected and how their privacy is guaranteed. After all, improving this perception will be translated into a greater trust and a more intensive and wider use of the social networking. In our opinion, a solution could be to change the privacy settings interface, which is composed by multiple items located separately, and offer a simpler, explanatory and self-guided tool to configure the privacy settings. This interface should be shown to users when a LinkedIn account is created, and later, periodically.

ACKNOWLEDGEMENTS

This research has been supported by project grant TEC2010-21405-C02-02/TCM (CALM). It is also developed in the framework of "Programa de Ayudas a Grupos de Excelencia de la Region de Murcia, de la Fundacion Seneca, Agencia de Ciencia y Tecnologia de la RM (Plan Regional de Ciencia y Tecnologia 2007/2010)".

REFERENCES

Acquisti, A. and Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the fb. *Privacy Enhancing Technologies*, LNCS 4258:36–58.

Barrigar, J. (2009). Social network site privacy. a comparative analysis of six sites. Commissioned by the Office of the Privacy Commissioner of Canada.

Egelman, S., Oates, A., and Krishnamurthi, S. (2012). Oops, i did it again: Mitigating repeated access control errors on facebook. In *Proc. of CHI'12*. ACM.

Fogel, J. and Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concers. *Computers in Human Behavior*, 25(1):153–160.

Gross, R. and Acquisti, A. (2005). Information revelation and privacy in online social networks (the facebook case). In *Proc. of WPES'05*. ACM.

Gundecha, P., Barbier, G., and Liu, H. (2011). Exploiting vulnerability to secure user privacy on a social networking site. In *Proc. of ACM SIGKDD'11*. ACM.

Johnson, M., Egelman, S., and Bellovin, S. M. (2012). Facebook and privacy: It's complicated. In *Proc. of SOUPS'12*. ACM.

Johnson, M. L. (2012). *Toward Usable Access Control for End-users: A Case Study of Facebook Privacy Settings*. PhD thesis, Columbia University.

Kane, L. (2013). 8 mistakes you should never make on linkedin. http://www.forbes.com/sites/learnvest/2013/03/04/8-mistakes-you-should-never-make-on-linkedin/.

Kaplan, A. and Haenlein, M. (2010). Users of the world, unite! the challenges and opportunities of social media. *Business Horizons*, 53:59–68.

Krasnova, H., Kolesnikova, E., and Gunther, O. (2010). Leveraging trust and privacy concerns in online social networks: an empirical study. In *Proc. of ECIS'10*.

Krishnamurthy, B. and Wills, C. (2008). Characterizing privacy in online social networks. In *WOSN, 1st Workshop on Online Social Networks*. ACM.

Liu, Y. and Gummadi, K. (2011). Analyzing facebook privacy settings: User expectations vs. reality. In *Proc. of IMC'11*. ACM.

Magazine, C. R. (2012). Facebook and your privacy: Who sees the data you share on the biggest social network? http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm.

Nayak, A. and D'Souza, R. M. (2011). Who do you trust? information sharing, privacy concerns and trust in an online social network. *Explorations Journal*.

Rizk, R., Marx, D., Schrepfer, M., Zimmermann, J., and Gunther, O. (2009). Media coverage of online social network privacy issues in germany - a thematic analysis. In *Proc. of AMCIS'09*.

Skeels, M. and Grudin, J. (2009). When social networks cross boundaries: A case study of workplace use of facebook and linkedin. In *Proc. of GROUP'09*. ACM.

Staddon, J. (2009). Finding hidden connections on linkedin an argument for more pragmatic social network privacy. In *Proc. of AISec'09*. ACM.

Staddon, J., Huffaker, D., and Brown, L. (2012). Are privacy concerns a turn-off? engagement and privacy in social networks. In *Proc. of SOUPS'12*. ACM.

Stutzman, F. and Kramer-Duffield, J. (2010). Friends only: Examining a privacy-enhancing behavior in facebook. In *Proc. of CHI'10*. ACM.

Sullivan, J. (2013). Why you can?t get a job recruiting explained by the numbers.