"My Life Doesn't Have to Be an Open Book": A Model to Help Designers to Enhance Privacy Controls on Social Network Sites

Francine B. Bergmann and Milene S. Silveira

Faculdade de Informática – Pontifícia Universidade Católica do Rio Grande do Sul
Avenida Ipiranga 6681, Prédio 32, 90619-900 – Porto Alegre/RS, Brazil
francine.bergmann@acad.pucrs.br, milene.silveira@pucrs.br

Abstract. Social network sites (SNS) are powerful technologies to bring people together and share information, changing the way society interacts in contemporary days. SNS such as Facebook have grown in popularity in recent years, reaching 1,3 billion monthly active users. However, as this network helps to make the world more open and connected, participants inevitably end up losing control over the extent that their personal information may reach among people that belong to their social circle or not. In this context we present +PrivacyCTRL, a model to enhance privacy controls on SNS, which supports the design of privacy settings in order to give users more autonomy over what they publish in these networks. +PrivacyCTRL was applied – via paper prototype technique – to three well-known SNS and showed promise in clarifying the privacy settings and improving the user's choice about what to reveal and to whom.

Keywords: +PrivacyCTRL, privacy model, social network sites, Facebook.

1 Introduction

Social Network Sites (SNS) are powerful technologies that enable their users to share information and stay connected with friends and the world. They have gained popularity in recent years and are now considered to be one of the fast-growing internet sites in the world [17]. To build this network, SNS allow the creation of online profiles in which users can exchange messages, tag photos/videos, "Like" and "Comment" on friends posts and share publications. Among all, Facebook is considered to be the largest and most famous site with more than 1,3 billion users and approximately 125 billion connections between friends and 300 million photos posted per day [7]. This explains Facebook's mission to make the world more open and connected [7].

Since SNS are virtual spaces that allow several possibilities for self-expression and social interaction, their use ends up creating significant challenges regarding the management of the users' privacy. There are many cases in which it is possible to find personal information of individuals in SNS and use it for malicious and/or illegal

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2014, LNCS 8533, pp. 387–399, 2014.

purposes [1]. For example, photo albums may contain personal data in subtitles, places people visit, geolocation or information about friends. Nevertheless, because of the inherent desire to share their moments, people often prefer to be relied to the existing settings on SNS than not publishing content [3,8]. As a consequence, users can be not only putting their privacy at risk, but also their friends' privacy.

Following this subject and assuming that current SNS have insufficient manners to rule the privacy of their users, the objective of this work is to propose a model[1] called +PrivacyCTRL, in order to help the designer to build and develop SNS enhancing the privacy controls, and also to allow the users to understand and configure their social network account in an intuitive way that they can choose the amount of information they want to reveal and the people who can have access to it.

Next chapter of this paper addresses related researches, followed by the presentation of the model. The work ends with conclusions and future work.

2 Literature Review

Johnson [10] discussed privacy even before the diffusion of SNS, demonstrating there are several ways in which information can be created, collected, moved and used by computational technologies, all this motivated by public and private companies who want (and use for profitable purposes) information about individuals.

A group of researchers [1,8,14] discovered that SNS users frequently publish personal information such as address, phone number and photos. Most of them are aware of the privacy settings available, but some just relied and remained with the default settings or had not even read them. The small group that made changes complained about the lack of control over the material others post about them. Also, there is a serious discrepancy between the users’ intentions and reality when speaking about privacy definitions of SNS [12, 14].

One study [20] investigated users' strategies to avoid unauthorized access to their profile contents, like sharing private messages rather than public comments and even falsify data to restrict the possibility of strangers to gather sensitive information. In other research [13], approximately 90% of users accepted the invitation of fake profiles, demonstrating the lack of concern by adding a stranger as friend in SNS.

The study by Pimenta and Freitas [16] discusses the privacy issue from the point of view of SNS developers, focusing in problems such as time pressure and cost. Thus, the authors explore several SNS and list the main privacy issues found in order to create a "manual" of standard procedures and solutions that would help professionals to build a secure platform prioritizing the privacy rights of the end users.

The work of Dhia [5] affirms that it is necessary to increase the users control over the distribution of their personal data, since they generally do not want to share life details with everyone. Thus, the author proposes a model of access control for social networks based on the characteristics of connections between users. The model

[1] The term model [19] was chosen because represents processes, variables and relationships without providing specific guidelines for implementation, which are at the discretion of the developer.

provides conditional access to shared resources based on limitations of scope between the owner and the requestor of a piece of information, showing the results through social graphs. All studies presented in this chapter show that we cannot ignore the vulnerability inherent to the growth and popularization that these sites are having today.

3 The Proposed Model

This chapter describes three sections of investigative procedures. Only the most relevant results to create +PrivacyCTRL will be presented.

3.1 Investigating Privacy-Related Issues

First, we spread an online survey [2] which had the collaboration of 255 volunteers from all ages, 30 questions and was available for 10 days, useful for understanding what information users protect more, what kind of privacy issues they have, their interests in changing existing settings and their concern about having their privacy violated when using SNS. Based on the results, people seem to be aware of the existence of privacy settings, however, their responses suggest they do not use the help systems or maybe the SNS is failing to provide easy and safer solutions. For example, users were asked if they had any information completely public in their profiles, and 28% (72) of the participants said "No". The first 15 of these 72 people had their Facebook profiles analyzed, and surprisingly, they all had at least one public information such as birth date, relationship status, workplace, photos or wall posts. Through other similar questions, it was observed that there were controversial points between what people perceive as private and what the SNS really provide [2].

After the survey, we applied the Semiotic Inspection Method (SIM) and the Communicability Evaluation Method (CEM) over the interface of Facebook (chosen because it is one of today's most popular SNS), in order to identify the settings offered by the SNS, what they allow to protect and how they are distributed in the interface. These methods were selected because assess in greater depth the communication quality, since it is through the interface that the designer tries to transmit to the users what they can do and how to perform their actions [18]. For its application, 9 people [18] were selected and 7 were aged between 19 to 29 years old. Also, 2 participants aged between 40 to 50 years old were invited to the tests to verify if their behavior would be distinct from the younger ones. The application of both methods was performed with the creation of five scenarios inspired by the most important features of Facebook's privacy settings (according to the online survey):

1. Local Settings: who can see users' posts in the Timeline and News feed area;
2. General Settings: who can see posts from users and their friends in the Timeline;
3. Photo Tagging Settings: who can see tags, automatic tagging and tagging removal;
4. Possibility to hide activities on News feed and Timeline;
5. Preservation of personal identity in Facebook's search system.

Through the application of these methods, we identified several communication breaks in the interface, such as: decisive icons for privacy control with low visibility; inconsistency between options along the interface (often 3 or 4 ways to do the same thing); lack of metalinguistic signs to alert the user during interaction (and existing ones are sometimes confusing to interpret), among others. Also, we found problems related to the control over the information published, such as: privacy settings scattered throughout the interface; content published in News feed to strangers without users' knowledge; initial Facebook settings defined as public by default; tutorials that appear only once in the system, without the possibility of new access; unclear explanations about external search systems (which expose users' data on the Web); inability to disable functions such as "Like" and "Share" (which are mainly responsible to spread the information on SNS) and automatic features like geolocation (list of places that users visited) and tags; settings that cover many items that should be individual. Finally, it is understood that the user needs to be experienced and enjoy exploring the interface to find (and understand) all existing settings and possibilities.

With all these items explored, the next stage of this work addresses how the information obtained was arranged to create +PrivacyCTRL.

3.2 Building the Model

Gundecha et. al. [9] affirm that an individual is vulnerable if any of his social network friends has insufficient privacy settings, impacting in the protection of the entire network. For all exposed until now, it is noted that current SNS are not fully adequate to manage the privacy settings of its users. Simple cases such as initial settings on Facebook being public are enough to cause serious damage to the integrity of users who do not usually explore the environment they interact. In this ambit we present +PrivacyCTRL, which attempts to minimize users' exposure and increase control over their content on SNS, supporting the design and improvement of privacy settings.

Through the results of the survey and the application of SIM and CEM over Facebook, added to the literature review and the practical exploration of common social networks like Twitter, YouTube, LinkedIn, Orkut and Google+, it was possible to make several assertions with regard to the composition of social networks, which are the main ways to interact in them, what types of content are published therein, how their privacy settings are and what they should (or may) protect.

To support creation and diagramming of +PrivacyCTRL, some terms related to the main features that compose SNS are presented, helping to organize all the information collected until now. They were created based on practical and theoretical research and also incorporated from other existing works. The terms are as follows:

- Resources: characterized by all sorts of content that the user can publish on the network, such as photos, videos, messages, map locations, lists of friends etc.;
- Activities: refer to what the user can do with the resources, as, for example, share, favorite, like, post, comment, tag, follow etc.;
- Individual Attributes: actions that the user makes on his profile and in the general interaction areas of the SNS [9];

- Community Attributes: actions that other people do on user's profile or in the general interaction areas of the SNS that involves the user somehow [9];
- Local Settings: made directly in publications, usually when the user performs some Activity over a Resource;
- General Settings: made once and valid for all profile items and publications;
- Help: detailed and complete explanation about Resources, Activities and Settings.

Then these described, the elements were grouped in a diagram (Fig. 1) according to their relationships, and to what is essential to have in a social network that allows the users to control their privacy and autonomy on SNS.

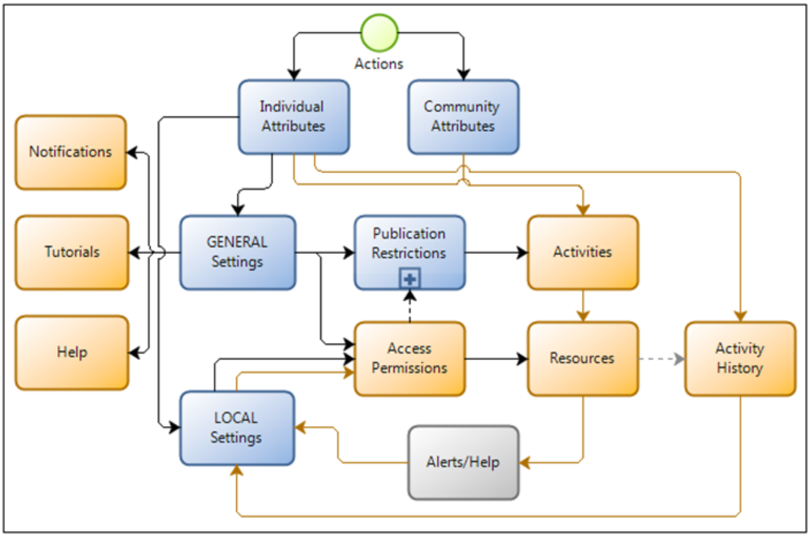


Fig. 1. +PrivacyCTRL, a model to enhance privacy controls on social network sites

This diagram represents the proposed model, which helps the designer to enhance privacy controls on SNS. The green circle refers to the beginning of an action by the user, and the blue squares are steps taken until reaching a final phase, this last one represented by orange squares. The arrows, which flow according to their type and color, represent the relationship between each square. Dotted arrows represents only system actions, not user's, unlike the others. The gray square is an optional function.

To better understand the flow among the elements and how to use +PrivacyCTRL, the model will be described in parts in the following sections. Some design recommendations proposed by other authors are cited to complement the model.

Settings. In Fig. 2-A, which is a cut of Fig. 1, we observe the flow of the General and Local Settings. It is important to keep these two areas separated, since there are many configurable items on SNS and exposing them all together to the user may be confusing. During the application of CEM it was seen that the first place user seeks for privacy solution is in a local area (easiest and fastest way possible). If he fails, he looks for a more complete area which will ensure his privacy more broadly, encompassing all publications.

The action in Fig. 2-A starts with the Individual Attributes, i.e., with the possibility of the user makes actions over his own profile. In this case, the path he has to follow would be the General or Local Settings. Following the flow of both, the user would be taken to the most basic configurations: the Access Permissions over the Resources, better seen in Fig. 2-B. The Access Permissions are composed by [11]:

- Private: the resources are private to the user;
- Friends: the resources will be visible to all friends of the user;
- Friends of Friends: the resources will be displayed for user's friends of friends;
- Public: the feature will be visible to anyone on the social network;
- Custom: the action may be viewed by specific friends the user defines;
- Groups: the resources will be visible to the groups that the user creates or that are recommended by the social network, such as family, work, college etc.

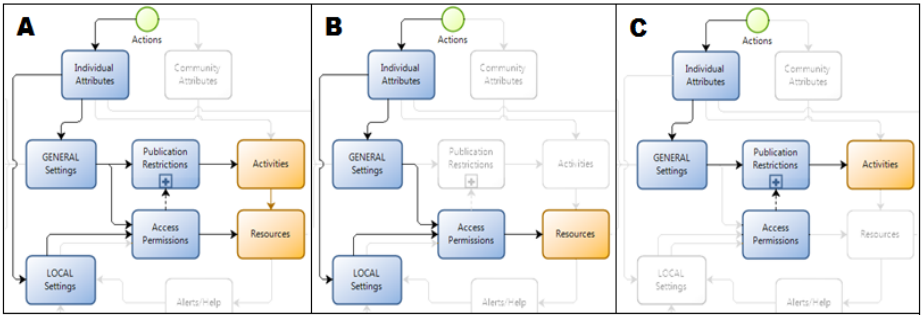


Fig. 2. A – Flow of General and Local Settings. **B** – Access Permissions. **C** – Publication Restrictions (this image's purpose is to focus the colored areas from Fig.1 to be discussed).

The orange item Resources (Fig. 2-B) represents the completion of the action. Then, this part of the model allows the user to access the Local Settings of a Resource on SNS. For example, the user can set that only his "Family" (Access Permission) could view a photo (Resource), and then go back surfing on the site. He could do a similar action through General Settings, selecting that only his "Friends" can view his publications. Due to problems stemming from privacy settings defined as Public by default on SNS, it is recommended Access Permissions be set for "Friends" by default. This would prevent the spread of information, bringing the user some kind of trouble. Later, if the user wants, he can any time make all its resources Public through settings.

Looking at Fig. 2-C, we see the items related to General Settings, which are the Publication Restrictions, to be applied exclusively over the Activities. The Publication Restrictions determines who can perform any Activity over the user's Resources, and shall comprise three main items:

- Disable: indicates the user could disable completely the possibility of any person to accomplish any Activity over his Resources;

- Enable: indicates the user could allow anyone who is viewing his Resources to perform Activities over them;
- Enable with Permissions: indicates the user could allow the execution of Activities over his Resources by certain people, and this can be set through the item Access Permissions, which is "embedded" in Publication Restrictions and can be seen through the "[+]" in Fig. 2-C, also indicated with a dotted arrow.

This feature allows the user to control unauthorized actions over his publications. For example, the user can set friends to comment his photo albums or that only one group can favorite his posts. One of the users interviewed during the application of CEM had his whole photo album shared at once by a friend, and to manage the situation, he changed the visibility of the album to "Private" on Facebook's general settings. Through +PrivacyCTRL, the user would have control to restrict the group of people that can share his resources, and would not have to hide them permanently.

The item Enable with Permissions could also include broader solutions for specific activities, such as Tagging. Added to the fact that shall be an option on SNS that allow users to "disable" this functionality, another research [15] proposes a "hiding" feature, which allows the tag visualization only by the photo's owner and the user tagged, not needing to be deleted. Thus, the user does not lose the interaction with the photo and can have more control over the publication, allowing or not the tag to be visible to others. If the tag is hidden, he turns it difficult for others to trace his profile data, avoiding the visitors to obtain information about him without authorization.

Another solution found in literature [4,15] suggest that when a user upload photos of people to the SNS, the system keeps all the faces blurred and the only person that can undo this action is the face's owner (not the photo's owner), after he is tagged. Then, the face will be allowed or not to be displayed to other people by its real owner.

Notifications, Tutorials and Help. An important point of any interactive system refers to help, which must assist the user when he interacts to the interface, when he needs to change settings to ensure his privacy and mainly to alert about the consequences (and range) of the configurations he has made.

+PrivacyCTRL provides three help approaches through General Settings: Notifications, Tutorials and Help (Fig. 3-A).

Notifications are areas of the interface designed to inform the user about updates on the SNS when he is involved somehow, for example when he is mentioned (or tagged) in groups, events, publications, applications, communities etc. The user shall be able to set *what*, *how*, *when* and *if* he wants to receive warnings about his profile, and they may be displayed by the interface of the social network, by email or even by phone. Another feature of the notifications area is to alert users of any kind of changes relating to privacy issues in the interface (e.g., to notify when there is a change on the user settings page in a transition of interfaces, or inform future updates on site policies).

The Tutorials cover quick access to areas of little help, by which users quickly learn about the features of the network, how to use them properly and how the items related to privacy work, always having easy access to them when visiting the General

Settings. Moreover, the tutorials may also pop up during the user interaction, in order to help when he is using the SNS for the first time, for example. We observed during the application of CEM that users do not lose more than 30 seconds on the same screen looking for help, so the more focused, clear and direct the tutorial steps are the better and more interesting they will be for the users.

Recently Facebook has implemented tutorial boxes to teach their users quickly how to use the system. This shows that these changes come to reinforce what is suggested in this work through +PrivacyCTRL. The only problem that has been noticed is that, once the access to these tutorials are lost, or if the user chose to stop reading it (button "Close") after the first time it is displayed, he can no longer go back and view it again.

Help areas of the SNS must always be of easy access to the users, allowing them to find the solution of their problems through topics, FAQs (Frequently Asked Questions) or search mechanisms, for example. This is the way the designer will pass to the user his main message about the interface, therefore, it must be clear and cover (if possible) all areas of interaction of the social network.

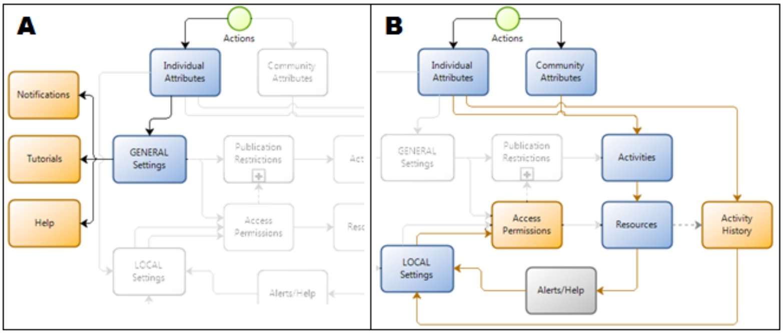


Fig. 3. **A** - Notifications, Tutorials and Help. **B** - Activity History and Alerts (this image's purpose is to focus the colored areas from Fig.1 to be discussed).

Activity History and Alerts. It is necessary to specify the actions related to the Activities and Settings area on SNS. In Fig. 3-B we note two possibilities of interaction: one through the Individual Attributes and the other through Community Attributes.

We found during the application of SIM that it is important to keep a record of all the activities made by the user on the SNS: people he adds, posts he comments, groups he joins, publications he makes etc. Thus, starting the flow with the Individual Attributes, we see that this record would occur every time the user performs an Activity over a Resource, and it would automatically be part of an Activity History, shown in Fig. 3-B with a dotted arrow (see better details in Fig. 1). This history (every move the user makes on the SNS) would be displayed in the user's profile to be set locally, choosing what to display to whom. Or else, the Activity History could be in a separate area of the interface, keeping user's personal profile only for displaying the main activities related to himself (for example, a comment he leaves on a friend’s post would appear only in the Activity History, not in his profile). The most important is the Activity History function shall be present in some area of the interface, so the user can easily control which of his activities should be visible to others.

Alerts/Help (gray square in Fig. 3-B) are optional under certain conditions, and should appear when the user perform an Activity over a Resource. The purpose of this function is to alert the user about the risk of privacy violation when doing any activity on SNS. If the user posts a photo and his settings were previously set as "Public", it is important that the interface alerts the publication will be visible to anyone, and immediately offers a path to Local Configurations for the user to change its Access Permissions settings, giving him the choice to control the exhibition of his information.

Further, we need to address the Community Attributes, i.e., what other people make in the user profile and elsewhere in the SNS involving the user. Since the main items of +PrivacyCTRL have been described in the previous section, watching the flow of steps in Fig. 3-B we can exemplify an action: if a user's friend makes a comment (Activity) in a photo (Resource), he (the visitor) can also set the privacy level of this activity. However, it will always be subjected to the original settings established by the owner of the content, i.e.: if the user sets the Access Permissions of his photos to Friends, the person who wants to leave a comment cannot turn publication "Public" somehow, but can further restrict his comment viewing for "Only me and the owner".

Through +PrivacyCTRL, we expect that developers can better build and develop an interface, since the model covers the essential parts of SNS and how they can be protected. Thus, with a well designed and comprehendible interface that offers more ways to control personal data, users could easily understand the system, configure their settings and thus have an intentional choice about disclosing their information.

3.3 Analysis with Users

The analysis of the model was made through the redesign (via paper prototype technique) of the interfaces of three well-known social networks in Brazil (Facebook, Orkut and Twitter). The users who participated were the same of the CEM (9 people).

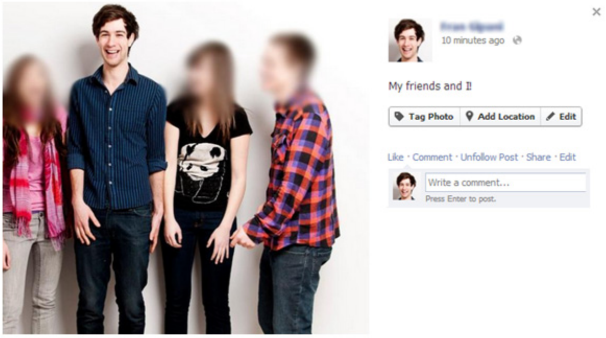
The tests were made individually, and to each user was explained the actions allowed by the model, its utility for developers and how an interface could have its settings improved through its use, becoming a suitable environment to protect users' information. The interfaces were presented in its original form and after the application of +PrivacyCTRL, having some privacy issues fixed.

The following sections describe some interfaces presented to the participants and their most significant responses to the survey.

Redesigned Interfaces. Eight examples of redesigned interfaces were presented to the users, and the personal profile area of Orkut was one of them. Currently, the privacy setting applies to the overall contents in the users profile and cannot be restricted individually according to the users preference. Then, if the user wants only his coworkers to see his e-mail, for example, he can do nothing about that. As stated by the model (Fig. 1), a user must have the possibility to set, through the Local

Settings, the Access Permissions of an Activity over a Resource. Thus, the proposed solution in this example occurs through the introduction of small icons (padlocks) along the interface, allowing the user to configure the Access Permissions for each of the personal data in the page, such as address, birthday, relationships status etc.

In Fig. 2-C, we have the explanation of the item "Enable with Permissions" that belongs to the square Publication Restrictions, which brings suggestions for better controlling tags, like the face obfuscation feature (Fig. 4).



My friends and I!

Fig. 4. A photo on Facebook with blurred faces. The photo's owner (who published it) lies in the center of the image (Source: adapted from Google Images).

In the example of Fig. 4, when a user uploads a photo with several people in it, the faces in it are blurred until the owner of each face is tagged by the user. This manner, each one can authorize (and control) his face to be displayed or not. Other tagging features suggested by +PrivacyCTRL, like "disable" and "hide" (explained in Fig. 2-C) were flagged during the tests via quick access to Facebook and Twitter settings (this last one has the tagging feature similar to Facebook), showing that this type of configuration could be applied along the interface with other tagging options.

The next section presents the survey applied to users after the presentation of the redesigned interfaces.

Post-test Survey. The survey was divided into two main parts: the first one consists of general questions about privacy and the second part were questions about +PrivacyCTRL. Only the main questions and results are commented.

One of the questions was if users would publish more content if they could better manage their privacy in social networks, and 6 out of 9 participants (67%) said "Yes". Next, 8 people (89%) think it is important to receive notifications about all activities involving their profiles on SNS, and 7 people (78%) say they have already deleted posts or didn't publish content for not knowing how to protect them. All 9 participants said they would not want complete strangers seeing what they publish.

The following questions comprehends specifically the functions proposed in the model. In the case of tagging, 8 out of 9 users (89%) said they would like to use the mechanism to "blur faces" in photos they were tagged, or totally disable photo tagging. All 9 participants would use the "hiding tags" feature suggested in the model, which makes the tag visible only to the owner of the photo and the person tagged.

When asked whether with +PrivacyCTRL users would have the opportunity to better control their privacy and the content that their friends post about them on SNS, all participants said "Yes". A problem cited by one volunteer was he couldn't hide his Likes and Comments updates from Facebook's Timeline. Using the model to redesign the interface, he'd have more autonomy to control his actions, activities and those who can see what he shares. Other user commented: "*Some strangers were commenting my photos and I think it's quite unpleasant. If the network was properly suited to the model, I could control this kind of activity*". About the redesigned interfaces, one user said that "*these few examples we saw were enough to better control the privacy of our publications and see that the model appears to be very promising*".

As the results shown here, we observe that users are concerned about who has access to their information and they want to have more control over their exposure on SNS. The redesigned interfaces through the application of +PrivacyCTRL demonstrated to be very useful for users, who saw in practice how a secure interface would looks like. Simple problems like photo tagging had easy and quick solutions for users who do not like to be labeled. The study indicates that the model shows promise in improving the interfaces and helping to correct some existing privacy problems.

4 Conclusions and Future Works

Social networks sites became part of human culture and totally changed the way society interacts today. However, the consequence of their popularization gives rise to frequent privacy problems, highlighting the need for actions and solutions that will help the user to better control their exposure online.

Thus, this work presented a series of procedures, researches and tests performed to understand how people have faced the privacy-related issues in SNS, what are the main existing problems and why they occur. With these results in hand, we proposed +PrivacyCTRL, model to enhance privacy controls on SNS which helps the designer to better build and develop the interface, allowing the user to understand and configure the system according to his needs and preferences. At the same time, the tests with users indicated that the model shows promise to help fixing several existing privacy problems and could be used to help building safer SNS in the future.

With all these exposed, we see that it is still a challenge for social networks being suited to the privacy demands of its users, and alternatives such +PrivacyCTRL proposes are crucial to help in the evolution of privacy treatment of SNS. Also, the model cannot yet be the solution for all privacy problems, but it certainly helps the designer to focus on the points that should gain more attention to build a safer system.

It is also known that the activities and resources present are constantly evolving, since the demand for content is always increasing. It is crucial that these networks should enhance their system to serve people better and ensure that new features are equipped with good privacy settings like the ones suggested through +PrivacyCTRL.

In 2013, reinforcing the results of this work, Facebook casually updated its privacy settings. The main changes were the addition of local help and tour areas along the interface, explaining more about features and privacy, and the centralization of the privacy settings, that were previously scattered in different areas of the interface.

There is still the human factor in the history: social networks are composed of content that others choose to share and distribute, and, at these times, wondering if this type of information will harm someone or not remains a question. As said by Eric Schmidt, CEO of Google [6]: "*If you have something you do not want anyone to know, maybe you should not do this in the first place*". This could prevent a lot of problems, and educating users to use their common sense in SNS is a difficult and challenging task, but basic to success.

As future work, +PrivacyCTRL could be applied more deeply in the studied SNS, trying to cover a wider range of issues and thus see how it could be refined and complemented. It would be important that the model was applied by other specialists than the authors, to verify if the instructions are comprehensible for the designers who may want to follow it, for example.

At the same time, the implementation and reformulation of the model presented here to build safer mobile interfaces would be an interesting alternative, since the use of social networks on smartphones and tablets is increasing nowadays.

References

1. Ai, H., Maiga, A., Aimeur, E.: Privacy protection issues in social networking sites. In: IEEE/ACS International Conference on Computer Systems and Applications (AICCSA 2009), pp. 271–278 (2009)
2. Bergmann, F.B., Silveira, M.S.: Eu vi o que você fez.. e eu sei quem você é!": uma análise sobre privacidade no facebook do ponto de vista dos usuários. In: 11th Brazilian Symposium on Human Factors in Computing Systems (IHC 2012), pp. 109–118. Brazilian Computer Society, Porto Alegre (2012)
3. Besmer, A., Lipford, H.R.: Moving beyond untagging: photo privacy in a tagged world. In: 28th International Conference on Human Factors in Computing Systems (CHI 2010), pp. 1563–1572. ACM, New York (2010)
4. Cutillo, L.A., Molva, R., Önen, M.: Privacy preserving picture sharing: enforcing usage control in distributed on-line social networks. In: 15th Workshop on Social Network Systems (SNS 2012), p. 6. ACM, New York (2012)
5. Dhia, I.B.: Access control in social networks: a reachability-based approach. In: 15th Joint EDBT/ICDT Workshops (EDBT-ICDT 2012), pp. 227–232. ACM, New York (2012)
6. Dwyer, C.: Privacy in the Age of Google and Facebook. IEEE Technology and Society Magazine 30(3), 58–63 (2011)
7. Facebook Newsroom, `http://newsroom.fb.com`
8. Faliagka, E., Tsakalidis, A., Vaikousi, D.: Teenagers' Use of Social Network Websites and Privacy Concerns: A Survey. In: 15th Panhellenic Conference on Informatics (PCI 2011), pp. 207–211 (2011)
9. Gundecha, P., Barbier, G., Liu, H.: Exploiting vulnerability to secure user privacy on a social networking site. In: 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD 2011), pp. 511–519. ACM, New York (2011)

10. Johnson, D.G.: Computer Ethics. Prentice Hall, Englewood Cliffs (1999)
11. Liu, Y., Gummadi, K.P., Krishnamurthy, B., Mislove, A.: Analyzing facebook privacy settings: user expectations vs. reality. In: 11th ACM SIGCOMM Conference on Internet Measurement (IMC 2011), pp. 61–70. ACM, New York (2011)
12. Madejski, M., Johnson, M., Bellovin, S.M.: A study of privacy settings errors in an online social network. In: 10th IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom 2012), pp. 340–345 (2012)
13. Michalopoulos, D., Mavridis, I.: Surveying Privacy Leaks Through Online Social Network. In: 14th Panhellenic Conference on Informatics (PCI 2010), pp. 184–187. IEEE Computer Society, Washington (2010)
14. Osman, F.Y., Ab Rahim, N.Z.: Self-disclosure and Social network sites users' awareness. In: 2nd International Conference on Research and Innovation in Information Systems (ICRIIS 2011), pp. 1–6 (2011)
15. Pesce, J.P., Casas, D.L., Rauber, G., Almeida, V.: Privacy attacks in social media using photo tagging networks: a case study with Facebook. In: 1st Workshop on Privacy and Security in Online Social Media (PSOSM 2012), p. 8. ACM, New York (2012)
16. Pimenta, P.C., de Freitas, C.M.: Security and privacy analysis in social network services. In: 5th Iberian Conference on Information Systems and Technologies (CISTI 2010), pp. 1–6 (2010)
17. Rauber, G., Almeida, V.A.F., Kumaraguru, P.: Privacy Albeit Late. In: 7th Brazilian Symposium on Multimedia and the Web (WebMedia 2011), p. 8. ACM, New York (2011)
18. de Souza, C.S., Leitão, C.F.: Semiotic Engineering Methods for Scientific Research in HCI. Morgan and Claypool Publishers, San Francisco (2009)
19. Tomhave, B.: Alphabet Soup: Making Sense of Models, Frameworks, and Methodologies. George Washington University (2005)
20. Young, A.L., Quan-Haase, A.: Information revelation and internet privacy concerns on social network sites: a case study of facebook. In: 4th International Conference on Communities and Technologies (C&T 2009), pp. 265–274. ACM, New York (2009)