

**Implementation of the Safer Social Networking Principles for the EU:
Testing of 20 Social Networks in Europe
February 2010**

NETLOG

Michel Walrave, MIOS, University of Antwerp, Belgium

Introduction

Netlog is a leading social networking platform, targeted towards European youngsters, with almost 60 million users. Its interface is available in 38 languages. The SNS provides tools to build an online identity (profile), connect and communicate with friends and other persons. Moreover, members can play online games, post and watch videos, share information on events and music and access information on brands. A mobile application gives subscribers the opportunity to be connected everywhere. Subscribers must be at least 13 years old. According to the provider the majority of members are aged 13 till 24 (<http://nl.netlog.com/go/about/press>, 29/10/09).

Test

Test performed in the Dutch language version on 24-25 October 2009

Summary

The SNS users have easy access to well structured texts including the Terms of Services and the Privacy Statement. Inappropriate conduct and its consequences are also summarized in a Code of Conduct. However, some essential information can be difficult for young users to understand, as formal language and (legal) jargon is used in some parts. In the Security Centre, some important online safety issues are clearly summarized. Yet, information for parents and teachers on how to advise their youngsters concerning their SNS use, is lacking. Although the provider offers the user a very broad range of privacy options, more awareness raising initiatives could be taken. The protection of minors' profiles for adults and the feedback to abuse reports should be assessed and enhanced. Concerning the minimum age of registration, it's not clear how the provider is assessing compliance to this condition. Finally, the provider does clearly indicate how age inappropriate content is blocked and provides prominent abuse report mechanisms.

Reporting on testing results

Principle 1: Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner.

According to the self-declaration, the provider states that a link to crucial information, namely Terms of Service («Algemene Voorwaarden») and Privacy Policy («Privacy Statement»), is easily accessible from each webpage. The SNS stresses its commitment to security and

privacy, especially when minors are concerned. That's why the provider states to have invested a lot in extensive privacy options and several initiatives to remind users of these privacy settings. Moreover, the provider summarizes inappropriate behaviour in a Code of Conduct («Gedragscode») that is accessible from every webpage. Next, some tips and tricks about safely using the service are grouped in a security centre («Veiligheid»). Finally, a detailed FAQ webpage is devoted to several issues SNS users can encounter. Even links to national and international suicide prevention centres are included. What's more, trained staff members are at users' disposal to give personal assistance. The SNS Community Managers post also blog messages and videos on security and safety topics. Issues are also announced in the SNS news and in privacy messages. All information comes in the language the members speak and understand.

In the social networking site, links to several sections dealing with safety, security and privacy are grouped in the footer of each web page. Even a non-registered visitor can consult this information. However, during the test it was observed that the user is confronted with 13 links on the bottom. Just above these links, 6 columns of in total 51 links refer to several services and information of the SNS.

The Terms of Service are well-structured and written in short paragraphs. However, the length of this text will not encourage young users to read the Terms of Service. This text consists of 14 paragraphs and a total of 145 lines, 1181 words. Moreover, legal jargon and, in some parts, very formal language is used. This full-fledged legal text will therefore not increase the comprehension of young users about usage restrictions.

The Code of Conduct («Gedragscode») summarizes several prohibited conducts. The provider clearly stipulates that in some cases of law infringements, police services will be alerted. The provider will undertake action to stop illicit activities on the SNS (a.o. blocking or deleting the user's account). Yet, this crucial information is not presented in an attractive way for young users. Although the code of conduct is, in general, easily phrased and structured in short paragraphs, some parts are written in rather formal language using legal jargon, which is not suitable for young users.

The Help & FAQ-page is devoted to all sorts of issues users can be potentially confronted with. Therefore also links to national and international suicide prevention centres are provided. Several FAQ questions refer to the Security Centre and the options to adapt the privacy settings.

In the security centre («Veiligheidscentrum») several important issues are highlighted (passwords, privacy, spam, phishing etc.). Short and understandable paragraphs are written on each issue and some advice is included. Yet, no appealing graphs or videos are included to, for instance, recognize specific problems. Moreover, no information is included about how to deal with requests for offline contact by peers or older online contacts and how to cope with harassment or other negative online contacts. Nevertheless, users are informed on how to report abuse using the provider's abuse-email address, when they feel at risk, or to contact eCops (with a link to the website of the online police report system). The «abuse button» is briefly mentioned.

The provider states also community managers post messages on security issues as news items and send also private messages. However, no links to centres of expertise providing tips and tricks for young Internet users, are present. Yet, the e-mail address of the Belgian Safer Internet Centre is included in the Code of Conduct.

Although Principle 1 stresses the crucial role of parents and teachers, the provider does not refer to these key partners in the self-declaration form. Moreover, no references are made to information and educational material, including technical control features for parents in the SNS.

Principle 2: Work towards ensuring that services are age-appropriate for the intended audience.

In the self-declaration the provider states that the minimal user's age is 13. Nobody under that age can register. If staff members happen to find out that some user is lying about his/her age, the account is blocked immediately. As the target group of the SNS is 13-24 year-olds, the provider declares to be very strict concerning the types of content that are appropriate for the users. Therefore, pictures and videos are moderated. Inappropriate content is blocked and hashed to prevent it from being uploaded again. Users can also use an abuse button, to report inappropriate content. Trained staff members review those reports on a 24/7 basis.

In the self-declaration the provider explains that a *wordlist* with inappropriate words, and a *blocklist* with inappropriate website addresses are used. Both lists are constantly updated. Moreover, the access to specific brand pages, ads and applications (for instance alcohol related) are only accessible to adults.

The provider clearly states in the Terms of Service (« Algemene Voorwaarden ») that minimum user age is 13 and nobody below that age can register. Moreover, the provider states that minors need their parents' consent. However, no information is given if and how this possibly will be checked. During registration, visitors can select their year of birth using a drop-down menu (reaching from 1900 till 1996). Yet, younger teens or children can subscribe if they select a 'suitable' year of birth in the drop-down menu. The self-declaration does not refer to technical or other mechanisms used to promote and control minimum age requirement.

No information is given on functionalities that are provided to partners to label/rate or age restrict their content, nor how young users are informed when services/information are not age appropriate. However, the provider states that young users are prevented from seeing pictures, videos, as all content is moderated. The SNS also restricts some brand pages, ads and applications to ensure that they are accessible to adults only. Indeed, when trying to visit the profile page of renowned alcohol brands, access was denied to the 15 year-old user, whereas the 32 year-old user could access the profile pages of alcohol brands. The younger user was warned that the brands choose not to disclose their profile: only 'friends' of the brands and some SNS-users have access. The 15-year-old therefore sent a message to the brands to become friends. One of the two tested alcohol brands accepted.

Principle 3: Empower users through tools and technology.

According to the self-declaration, extensive privacy settings are available to enable users to tailor their availability to others. The provider states that « by default privacy settings of all minors are closed, i.e. they cannot choose to show their profile to everyone, adults cannot contact minors unless they are friends, the friendship requests that are sent to them cannot be motivated (...), adults cannot see their MSN details and cannot search for minors etc. ».

Moreover, users have the possibility to block others to access their profile, to pre-approve comments and also to adapt the privacy settings of each image and video separately.

Concerning the default privacy settings of minors, the following measures are in place. By default, registered users only have access to limited profile information, whereas friends and their friends can see the entire profile. Only friends and their friends can send messages. Ratings and comments can be posted by all registered users. However, only comments of friends appear immediately online, whereas reactions of others are pre-moderated by the profile owner¹. Although minors cannot choose to make their profile accessible to *everyone*,

¹ The user can adapt this in the privacy settings and has the choice between three levels of control: (a) all reactions appear immediately, (b) reactions of friends appear immediately, other reactions after approval, (3) reactions appear after approval. Moreover, in the privacy options a user can select SNS member categories that can post comments (only friends, all users, friends and their friends or nobody).

they can make it accessible to *all SNS users*. The provider offers also the possibility to limit the access to one's profile to a group of SNS members sharing same characteristics (country, region or age group that can be defined by the user, for instance). Moreover, users can decide to make their profile only accessible to members of *Trust*². Profile owners can choose who is able to contact them (by adapting the privacy settings and also using a *whitelist*) and block certain users from accessing their profile (by means of a *blacklist*). Users can easily reject a friendship request and also add a person to their *blacklist*. A clear sign and short description is used. Moreover, the user can choose the privacy settings of each image/video separately. Concerning the protection of minors' profiles for adult subscribers, tests have been conducted. According to the self-declaration, adult users cannot search for minors. Indeed, an adult member using the SNS search engine's filter to look for profiles based on, for instance, age can only search for 18 year-olds and older users. However, by searching for (nick)names, minor users can be easily found. In some cases, the adult member can have access to the entire profile. Yet, an adult user receives a warning message (*you are about to see a minor's profile*) before accessing the profile. Although the messenger account of the minor remains undisclosed, during the test it was observed that an adult user has the possibility to send a personal message through the SNS. This contrasts with the self-declaration stating that adults can only contact minors if they are friends and that friendship requests cannot be motivated. Finally, although Principle 3 suggests the need of assisting parents, no information is given concerning the elaboration of specific information for parents on how they can use tools (like filters or parental monitoring) to help them accompany, monitor or advise their youngsters.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service.

Users can easily report inappropriate content in several ways. In the self-declaration and the social networking site as well, several mechanisms are explained. Users can hit the abuse button to report inappropriate content. Moreover, a specific e-mail address is provided to contact the SNS's team members. Not only registered users, but also visitors can contact the Community Managers and Assistants who check reports on a 24/7 basis.

In the Security Centre and the FAQ users are informed about the report mechanisms. First option is to send a message to an abuse e-mail address. What's more, next to user generated content (comments on a profile, e-mails, pictures/videos, blogs, ...) an easily accessible and clearly identifiable button is presented (with the figure of a policeman) and a short but clear description (« Meld misbruik »: report abuse) leads to an online form. In this short form the user is asked to select from a list of content types (for instance: blog, comments, private message, video), insert a hyperlink to this content and explain why he/she considers this content inappropriate or abusive. The provider states in the self-declaration that « All users get the opportunity to report any inappropriate content by simply hitting the report abuse button. Our experienced and trained Community Managers and Community Assistants check the reports on a 24/7 basis». As part of this study an e-mail was sent (on 25 October 2009) seeking assistance as the user receives « scary messages ». A message appeared on the screen confirming that the report was sent. No answer was received during the week following this request.

Principle 5: Respond to notifications of Illegal content or conduct.

In the self-declaration, the provider stresses its close collaboration with eCops, the Belgian governmental contact point for Internet abuse where users can report crimes committed on or

² This security label of the SNS depicts a specific icon on the profile, messages etc.. To become a Trust-member one has to communicate a mobile phone number to receive a code.

through the Internet. Moreover, the provider declares to report all legal violations (racism, child porn...) to eCops and makes sure all data for further investigation is saved. In case of offences that are prosecuted only in case of complaints, the provider's personnel guides the member to the correct authorities, and makes sure all data is saved in case the police should need it. Although the SNS refers to national and international suicide prevention centres, no information is given concerning possible collaborations with other relevant hotlines and awareness raising services. Yet, the e-mail address of the Belgian Safer Internet Centre is provided.

Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy.

The provider underscores in the self-declaration that users are enabled to manage the extent to which they want to expose themselves to others. Next to extensive privacy settings, information is provided in the FAQ and the Security Centre, to raise awareness on privacy and online safety issues. The trained staff is said to « keep an eye on everyone's safety, and react promptly if someone's privacy is at stake ». How this is achieved is not explained in the self-declaration form.

Concerning the opportunities offered to users to manage their personal data, the following observations were made. During the registration procedure, a user only has to provide few personal data (name, e-mail, date of birth, chosen password and CAPTCHA³). While registering, a link is provided to the Privacy Statement. Moreover, registration is only active when the new user clicks on a hyperlink sent to the disclosed e-mail address.

By default, personal data that are inserted in the online form are shown in the profile, as the box indicating that a certain piece of information may be shown in the profile is *pre-checked*. However, the user can decide not to include personal information in the profile by *unchecking* the box next to a specific piece of information. A user can also conceal his/her online status. Furthermore, members have a wide range of privacy setting choices. First, they have the opportunity to decide if they want to use their profile to meet new people (choice for basic privacy settings or high level of privacy protection), or to keep contact with the friends they already know (also two levels of privacy settings). By selecting one of these *privacy sets*, a user can have a group of privacy measures that is tailored to his or her purposes and privacy concerns. A brief overview summarizes the settings linked to a specific *privacy set*.

Moreover, all individual settings can be easily adapted. However, no specific awareness raising measures are taken in this context to encourage users to make informed decisions. Yet, in the Security Centre users are informed about how they have to protect sensitive data like passwords and how they have to react on requests to provide sensitive information (their password, for instance). The possibility to adapt privacy settings is briefly mentioned. Finally, in the *settings*, one can easily find the *account* section where a user is given the possibility to delete his or her profile.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct.

In the self-declaration the provider stresses its commitment to enhance the prevention of abuse and inappropriate content. Therefore the SNS personnel members are engaging in debates with users, police and governmental authorities as well as other organizations to improve its systems.

Moreover, the provider declares that automated and human moderation is used (cf. Principle 2). The provider uses a list of words and URL's to prevent youngsters to be confronted with

³ *Completely Automated Public Turing Test to tell Computers and Humans Apart* is a challenge-response system test designed to differentiate humans from automated programs (searchsecurity.com).

age inappropriate content (pictures, websites, brands, ads). The provider indicates that messages can be sent concerning security issues and that community managers post these kinds of issues as news items and send private messages (cf. Principle 1).

No information is provided in the self-declaration form concerning steps taken to minimize the risk of employing candidates who may be unsuited for work that involves real-time contact with children or young people.

Summary of results and Conclusion

First of all, the several efforts that have been made to inform users about their rights and obligations, have to be stressed. Generally speaking, the members have easy access to well structured texts including the terms of use and the privacy policy of the SNS. Moreover, inappropriate conduct and its consequences are also summarized in a Code of Conduct. Yet, in some parts of this essential information formal language and specific (legal) jargon is used. To inform and sensitize young users only textual information could be found, no tips or tricks are explained using different formats like for example illustrations and videos. Although the SNS offers the user a very broad range of privacy options, few information is given on how to use them and the possible consequences of disclosing specific information. Moreover, the protection of minors' profiles for adults and the feedback process to abuse reports should be assessed and enhanced. The security centre clearly summarizes information on some important security and safety issues. However, no links to online safety information of safer Internet centres are included. Yet, the close collaboration with eCops is a very important initiative.

Although some information is provided for users to raise their online safety awareness, no information for parents and teachers could be found. Concerning the minimum age of registration, it's not clear how the provider is assessing compliance to this condition. No references are made to technical or other mechanisms to promote and control minimum age requirements. Yet, the provider does clearly indicate how age inappropriate content is blocked (*wordlist* and *blocklist* of websites). Moreover, the report abuse button is prominently present and easy to use.

Assessment of the Principles vs. the Self-declaration

Principle	Compliant	Partially Compliant	Not Compliant	Not Applicable	Comments/Clarification
1		X			
2		X			
3		X			
4	X				
5		X			
6	X				
7		X			

Assessment of the Self-declaration vs. the measures implemented on the SNS

Principle	Compliant	Partially Compliant	Not Compliant	Not Applicable	Comments/Clarification
1		X			
2		X			
3		X			
4		X			
5	<i>Not Tested</i>				
6	X				
7	<i>Not Tested</i>				

The copyright of this report belongs to the European Commission. Opinions expressed in the report are those of the authors and do not necessarily reflect the views of the EC.