Evaluation of the Implementation of the Safer Social Networking Principles for the EU Part II:

Testing of 20 Providers of Social Networking Services in Europe

By request of the European Commission
under the Safer Internet Programme

Edited by:
Bojana Lobe, University of Ljubljana
& Elisabeth Staksrud, University of Oslo

European Commission
Information Society and Media

JANUARY 2010

PLEASE CITE AS FOLLOWS:

Lobe, B. & Staksrud, E. (Ed) (2010) Evaluation of the implementation of the Safer Social Networking Principles for the EU Part II: Testing of 20 Providers of Social Networking Services in Europe, European Commission Safer Internet Programme, Luxembourg

Contents

OVERVIEW OF SIGNATORIES AND TESTERS	4
ARTO	5
BEBO	9
DAILYMOTION	14
FACEBOOK	19
GIOVANI.IT	25
GOOGLE	31
HYVES.NL	37
MICROSOFT EUROPE	44
MYSPACE	53
NASZA-KLASA.PL	61
NETLOG	65
ONE.LT	72
PICZO	77
RATE.EE	82
SKYROCK.COM	89
SULAKE	95
TUENTI	101
VZNET NETZWERKE LTD.	105
YAHOO!EUROPE	112
ZAP.LU	120

OVERVIEW OF SIGNATORIES AND TESTERS

This part consists of the reports submitted by the expert testers on each signatory Social Networking Site. Below is a summary of the participating Social Networks, the date of submission of their self-declarations (SD), the version tested, and the name and affiliation of the expert tester. For further information on the methodology and testing details please refer to the first part of this report and the annexes.

Signatory	SD submitted	Version	Tested by	Affiliation
Arto	15 April 2009	Danish	Ditte Berg	IT University of Copenhagen
Bebo	17 April 2009	British	Simon Grehan,	National Centre for Technology in Education (NTCE), Dublin
Dailymotion	10 April 2009	French	Cédric Fluckiger	University of Lille 3
Facebook	16 April 2009	British	Bojana Lobe	University of Ljubljana
Giovani.it	*Not Available*	Italian	Giovanna Mascheroni	Univ. of Torino & Università Cattolica di Milano
Google	15 May 2009	British	Leslie Haddon	London School of Economics
Hyves.nl	17 April 2009	Dutch	Michel Walrave	University of Antwerp
Microsoft Europe	17 April 2009	British	Elisabeth Staksrud	University of Oslo
MySpace	17 April 2009	British	Bojana Lobe	University of Ljubljana
Nasza-klasa.pl	1 May 2009	Polish	Barbara Giza	Warsaw School of Social Sciences and Humanities
Netlog	28 May 2009	Dutch	Michel Walrave	University of Antwerp
One.lt	17 June 2009	Lithuanian	Rytis Rainys	Regulatory Authority of the Republic of Lithuania
Piczo	16 April 2009	British	Simon Grehan	NTCE, Dublin
Rate.ee	9 June 2009	Estonian	Andra Siibak	University of Tartu
Skyrock.com	29 April 2009	French	Cédric Fluckiger	University of Lille 3
Sulake	15 April 2009	Finnish	Mika Rantakokko	Center for Internet Excellence
Tuenti	12 June 2009	Spanish	Charo Sádaba	University of Navarra
VZnet Netzwerke Ltd	17 June 2009	German	Jan-Hinrik Schmidt	Hans-Bredow-Institute for Media Research, Hamburg
Yahoo!Europe	17 April 2009	British	Leslie Haddon	London School of Economics
ZAP.lu	17 April 2009	Luxembourgish	André Melzer	Université du Luxembourg

ARTO

Ditte Maria Bergstrøm, IT University of Copenhagen

Introduction

This paper will report the results of the evaluation of the internet site Arto. The evaluation was done by testing the site from a user perspective. This SNS is for users in the age from 12. It provides the participants the possibility of sending messages to each other, of posting pictures, writing in their diary, participating in clubs etc. The user can also engage in an "A marriage" with another user.

The test was mainly performed during the period from the 23.d – 28.th of October 2009. Quotes from self-declaration are underlined and "…".

The main findings in this report are that

- When signing up to the Arto website, the users do not have to agree to the *Terms of use*
- It is not possible to find the *Terms of use* at the website
- The information regarding safety is clearly stated, easy to find and in clear wording, but the content is deemed as insufficient as it is only targeted parents and not the young users.
- It is easy for a user to sign up stating an incorrect age
- The site exhibits support within 24 hours
- It is very easy to block a profile

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

Terms of use

According to the self-declaration the provider – regarding *Terms of use* – states that "The page informs users what they are agreeing for by signing up to the site and what they allow users to do with their information.".

When tested, the site displayed, that the user does not agree with any *Terms of use* in the process of signing up, nor is it possible to find the terms at the website. When seaching for them at google.com using "site search" and "arto.com" they were found, and as the URL indicates they are hosted at the site, but by seaching the SNS they were impossible to localize.

Information on safety

According to the self-declaration it "explains what the site does to ensure the users safety …". According to the testing, this information is pointed out in 10 statements: 24 hours response time (from support), word filter, reporting (of a user, that violates the rules), CPR control, chat robot, Access Restriction (to certain functions), administrators (over a 100 volunteers), blocking (the access of others). Log report (all written communication is registered and will be turned in to the police) and support. The 10 statements are easy to understand and clear in wording. The safety page is targeted specifically for parents.

Without registering as a user

As noticed before, it is not possible to find the *Terms of use/service* at the website. The *Safety policy* was easy to find (when scrolling), but placed at the end of the page following a list of other suggested sites (see picture). To find the *Code of conduct* the user should go to *Guidelines* and under there find the *code of conduct*. There are no targeted safety tips for children and youth. Under *Parent information* in *Safety*, there is advice like "don't use challenging pictures in your profile", "don't reply to unpleasant messages, but delete them and report the user". There are also links to educational material, but all this information is solely for parents and not for the young user. The material is easy to understand, clear in wording and all available in Danish. The information provided on specific risks of using ARTO is deficient. There is only one sentence hidden in plain text stating: "Some people might bully or submit offensive content".

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

According to the self-declaration it is not possible to sign up at ARTO being under 12 years old. Upon creating an account the user has to enter the year of birth. According to the self-declaration the age registered will determine which categories the user has access to. Some categories may only be used if the user is below 15 years of age, some categories may be used by users above 15 years of age and one category is reserved for users above 18 years of age. According to the self-declaration, the banner advertising targets the user's age and gender to avoid inappropriate advertising, but there is no mention of time of day specifics. During testing it showed that there are no precautions made to ensure the impossibility of using a fake birthday and signing up even if the user is under 12 years of age. There is no e-mail verification and it is possible to register with a fake or even non-existing e-mail account. In the self-declaration it is outlined that, on the public bulletin board, users may chose to see messages from other users around their own age. The test showed that it is possible to search, find and contact all ages.

Principle 3: Empower users through tools and technology

According to the self-declaration there is no information regarding the possibility of private profiles of users under the age of 18 are searchable within the service or via search engines. During testing it was possible to search any contacts in any age at the site, and a search for "maria-pigen" [a randomly user name] at google.com gave direct profile results. According to the self-declaration it is stated that "As Arto is designed with teenagers in mind, we do not set profiles as private.". In testing the only default information is first name, school and profile picture (if this is uploaded, hence it is optional). A user may choose to block other users, which makes it impossible for the blocked to contact the user. Users may also set up an age bracket for which users may contact him or her. E.g. should a user place the bracket between 13 and 15, a 16 years old will not be able to contact the user. It is very easy to block another user from contacting you, since there is a "block this person"-button in every message and at every profile. It is easy to delete postings and pictures at the users own profile, but a user cannot delete own postings on other users profiles if regretted later on. The user can filter who can comment on the profile, regarding 1) all users 2) age bracket or 3) only friends, but the personal information is visible for all other users. The user is notified when s/he is tagged in pictures, but does not have to approve before being published. It is not possible to delete a profile – the user can only deactivate it and ARTO keeps everything, Re-logging into the account re-activates it. The user is not informed of this, as there is no signing any *Terms of use* during the process of registering, but it is stated under "deactivating your profile" in "settings".

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the terms of service

According to the self-declaration it is stated that Arto "offers several tools for reporting violations of the guidelines and for requesting general support by the staff." As stated earlier on it is very easy to block a

profile. The user can contact support in two ways – write them directly or report a profile. There is a button at each profile, where the user can report it. It transfers the user to the report section, where the user must confirm three times that s/he is sure that s/he wants to report this person. In the report section the user can choose between 10 predefined things to report (maximum 24 hours response time regarding the subjects: ”inappropriate contact between old and young user” or ”sexual harassment”). When contacting support, the user has to write min. 250 signs or the report cannot be submitted. It does not mention why. In testing[1], in reference to the message in the instructions, it took under 24 hours from reported to being contacted by the support at Arto. When the report was delivered, tester received a page stating that it would be treated ASAP.

Principle 5: Respond to notifications of illegal content or conduct

According to the sites self-declaration, the provider will ”immediately close the profile in question as soon as we can verify the validity of the report.” and that they will send report to the NITEC, the Danish Center for National IT Investigation (Det Nationale IT-Efterforsknings Center, in Danish) if they can gather enough material. The provider will cooperate with the police when a court warrant is provided.

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

In the self-declaration the provider states, that they only ask for very basic information, name, e-mail, birthday, gender, zip code and native language. These things are mandatory. During testing first name, e-mail, birthday, zip code, native language and gender were required. Only first name was automatically included in the profile . There was no warning of this. During testing, it was possible to put in last name, municipality, school, year of beginning/end and profile picture as optional but not mandatory. All of there were automatically included in the profile without any warning. The user has to access privacy settings to change settings, but name and online status can not be changed.

Additional feature: After notice from the provider, who states that: ”When a user attempts to write his or her e-mail or phone number to another user, they are warned of the risk of this, and are asked if they wish to proceed.” In an after testing this feauture worked when writing at a users wall, but not when sending a private message from one user to another.

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

According to the self-declaration the provider manually checks all uploaded media, pictures and videos, ARTO has a filter that searches for expressions that are classified as harmful or unwanted. Since all written communication is logged, it is also possible to generate a chat log showing the messages between two users.

[1] Due to a misunderstanding, this test was performed outside the originally period of testing.

Summary of Principles

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			Only information towards parents. Test showed that it is not possible to localize the *Terms of Use* at the website nor are the terms signed in order to open an account.
2		x			The user don't agree to the *Terms of Use* in order to open an account. It is very easy to sign up with a fake age.
3	x				
4	x				
5	*Not Tested*				
6	x				Only first name is displayed in the profile as default.
7	*Not Tested*				

BEBO

Simon Grehan, National Centre for Technology in Education, Ireland.

Introduction

Bebo is an online community where members can find and communicate with others as well as browse and share user-generated content. Users interact with friends' profiles, send messages to other users, join groups, become fans of bands, use third party applications, and upload and share photos and videos. Users must be 13 or older to use Bebo.

Each member creates their own personal page called a profile, on which they can post their own content. Users can create profiles containing personal blogs, photos and other applications. They also allow users to embed media such as music files and video clips into their profiles and to share their original content with others by uploading it to the site. Users don't need any coding or mark-up skills to create glitzy, interactive, professional looking profiles. Users simply complete text based forms and choose skins (graphical styles) to create their profile

Once a user creates their profile, they can connect with other community members. During registration users are prompted to invite their existing contacts to join their profile. They are invited from their existing e-mail and messenger contact lists. Users can also request to connect with other community members by clicking on the 'add as friend' button on their profile. Bebo provides multiple ways for users to interact using synchronous chat, asynchronous messaging, email, blogging, discussion groups, and so on.

Each profile must include two specific modules, a comment section where other users can leave a message, and a list of the user's friends. They can select from many more modules to add. There is an large selection of "Apps" that can be easily embedded in the user's profile. Many of the modules are developed by third-party developers.

Summary findings

The self declaration provided by Bebo was in-line with the Safer Social Networking Principles. Bebo proved to be compliant with the Safer Social Networking Principles for the EU although some areas for potential improvement were identified.

Bebo provided clear safety information for children, parents and teachers. It also has developed a repository of links to well-being services for young people on its site. Bebo has a range of technical tools that empower the site's users to block unwanted contact and moderate comments they are published.

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

Testing found that the safety information is linked to directly from a hyperlink in the footer of the homepage. The footer containing links to Safety, Privacy and Terms of Service is available on all pages within the site. Bebo provides safety information for parents, teachers and young users. The general safety information is easy-to-find and easy-to-understand. The same can't be said of the privacy and terms of service information that is semantically dense and riddled with legal and technical jargon.

On testing, it was discovered that the code of conduct for young users is not explicitly stated but rather contained in animated instructional pieces on the **Safety** page. There are 12 content objects that are playable through an Adobe Flash player embedded on the page. The content includes simple graphic and audio animations providing Bebo-specific advice and general internet safety awareness raising videos that have been developed by third-party online child protection initiatives. There is a considerable amount of safety information provided; it would take approximately half an hour to play all the content.

Step-by-step 'how to' instructions were found in the **Help** section of the site detailing how to configure all aspects of the Bebo site including how to configure user profile settings to facilitate a safer experience on the site. The **Help** page provides instructions on how to: delete comments, block users, report abuse, moderate comments, and cancel membership. This information is not linked to from the **Safety** page and cannot be found using the search functionality on the toolbar.

Bebo provides information and educational resources for teachers. These documents can be downloaded directly from the **Safety** page where links to third-party sources of information for teachers are also available. Similarly, relevant third-party sources of information for parents are also prominently linked to from the Safety page.

In addition to providing safety and privacy education to their users, Bebo declared that they have created a well-being centre, which allows support providers to use the Bebo platform as a means to engage with young people in need of their services. Bebo has partnerships with support organizations on issues such as depression and self-harm. The well being centre is not linked to from the **Safety** page or the footer on any of the pages within the site. Locating this area of the site proved to be difficult. This is reflected in the low level of user engagement with the profiles of the service providers. For example, the "Technology for Well-Being" group is mentioned in the self-declaration, this profile has been viewed 920 times since June 2007.

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

Bebo relies on self-declaration of age by the user in the registration process as the key mechanism for ensuring that the services they provide are age-appropriate for their audience. Bebo's self-declaration indicates that users must be 13 or older to use Bebo. It was proven that if the date of birth entered by the user during registration indicates that they are below the permitted age, they are prohibited from registering.

Bebo claim to use content moderation solutions to identify and remove any content or members that break their terms of service and acceptable use policy (TOS). According to their self-declaration, they use image filtering solutions to flag images that might be pornographic and inappropriate URLs and HTML codes are blocked from being posted on member sites. They also claim to remove the accounts of users for excessive and/or repeat offences. No pornographic content was encountered during testing.

In testing, Bebo's claim that users who declare they are younger than 13 are not permitted to join the community was validated. When trying to register as an 11-year-old permission was denied and a cookie was placed on the machine preventing re-registering as older from that machine. In the self-declaration Bebo claims it conducts textual searches to help identify users that have provided a date of birth that indicates that they are 13 or older, but who subsequently post information on their profile that indicates that they are below 13. They say that upon discovery that a user is not 13 or older, they will delete that user's account and profile.

Bebo's self declaration outlines its policy for managing access to professionally produced content to ensure that content is age-appropriate and in-line with applicable national laws and regulations. Using the profile of

a 14 year old, I was unable to get access to video content from the Skins TV series that is rated as 18+ content. No information as to why access to this content was being denied was provided.

Principle 3: Empower users through tools and technology

Bebo claims to have taken measures that can help minimise the risk of unwanted or inappropriate contact between children and young people and adults. Websites and profiles of children under the age of sixteen were not found by searching for them in Google. When registered as an under sixteen the profile was categorized as 'Private', this means only users that accepted as friends are able to access the profile or make contact. They claim it is possible for users of any age to alter their privacy settings at any time. Also, even with their profile categorized as 'Public' it is also possible for Bebo users to block other users. The declaration states that it is possible for users to configure their account to allow only 'friends' to post comments on their profile and can delete unwanted comments before they are published on their profile.

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

Bebo provides prominent mechanisms for reporting inappropriate content, contact or behaviour. These mechanisms are easily accessible to users at all times and are easy to use. However users are not given sufficient information about how their reports are being handled nor are they given any feedback on how these reports were resolved.

It was found that once logged into Bebo, the report abuse link is prominently displayed on most content modules in the site. On Bebo's Report Abuse page users are alerted to measures they can take to prevent similar abuses in the future such as blocking users and moderating comments. On the reporting form, the tester was asked to categorise the abuse type from a dropdown list, provide reasons for making the report, and provide examples of the abuse. They were also asked to agree that invalid reports would result in future reports being ignored before the report was processed. This condition could act as a deterrent to reporting. Users are not told what constitutes an invalid report.

The report abuse function was used to log the following report; "I am writing to you because someone is sending me scary messages. What should I do about this? Please help me." Text was displayed on screen indicating a report has been sent. However, no specific communications were received in response to the report indicating how it would be handled. No feedback on the outcome of the report was received. No reference number was provided that could be used to follow-up or track reports.

Principle 5: Respond to notifications of Illegal content or conduct

Bebo recognizes the importance of working with law enforcement in their declarations and outline the processes they have in place to review and remove offending content. They have arrangements to share reports of illegal content or conduct with relevant bodies. In its self-declaration, Bebo mentions its distinct route to report suspected online predator behaviour. It claims reports received through this route are dealt with as high priority and reports are disseminated to the appropriate law enforcement agency. Other mechanisms are in place to support law enforcement with investigations and prosecutions. Bebo engages with the enforcement authorities (including the UK Home Office's Single Point of Contact training program) to educate investigators about how to lawfully obtain data from Bebo.

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

Bebo describes a range of awareness raising and technical measures they have taken to encourage users to make informed decisions about the information they post online. They also outline privacy options that are prominent in the user experience and accessible at all times.

Bebo describes several technical tools for refining access to users' information. This is just as well since they ask for a considerable amount of personal information during registration including details of the user's home address, relationship status, and mobile phone number. Disclosing all this information is optional. Users are able to access and alter their privacy settings at anytime using a link in a prominent place at the top of every page or from the 'edit profile' link underneath their photograph on their profile page.

Bebo claim that details provided while registering on Bebo are not directly mapped onto the user's profile. In some cases users are given the option at registration of whether to display details or not (as in the case of their age). The Bebo self-declaration says that context specific privacy messages are provided in areas where young people make decisions about privacy. While privacy options are available during the registration process and when uploading photos; very little information about the implications of choosing the available options were found. There are safety tips close to the 'Name' and 'Age' fields in the registration process but no information is given beside all the other fields. For example, there is a field for 'Mobile Phone' in the registration process but no contextual information about where this information is published and who has access to it. No context specific privacy messages were encountered while uploading photos or tagging subjects in photos. Testing validated the claim that users need to give permission before Applications could be installed and integrated with users' profiles.

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

The SNS provider did not detail in their submissions how they assess their service to identify potential risks to children and young people in order to determine appropriate procedures for reviewing reports of images, videos and text that may contain illegal and inappropriate/ unacceptable/prohibited content and/or conduct. They detail measures they take to promote compliance with the Terms of Service and Acceptable Use Policy (TOS) including a hybrid technical and human content moderation solution that identifies and removes content or members that break their TOS. According to their self-declaration, users who are found to be in breach of the Terms are either issued a conduct warning or have their accounts deleted depending on the severity of the breach.

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	Not Tested				
6	X				
7	Not Tested				

DAILYMOTION

Cédric Fluckiger, University of Lille 3.

Introduction

As Dailymotion itself states in the self-declaration: "Dailymotion is more of a video platform than a "social networking service". Therefore, some questions and tests proposed in the evaluation methodology are not relevant (eg: no easy possibility to report a conduct, only offending videos can be reported). However, in order to post a video, users have to register and get a profile. Users can comment other's videos, send messages to other users, add users to a friend's list. Dailymotion therefore provides some tools such as the possibility to block a user, reject or delete a comment, and so on… It provides therefore some of the main features of SNS's.

Dailymotion is not especially designed for children or teenagers, though these users can use the platform, either to browse the videos, or to create their own profile and post their videos. There is no minimum age for registering on Dailymotion specified in the self-declaration.

Conduct of the testing

The testing was conducted from October 25th to October 30th 2009. The testing language was French. For the testing, the screen resolution was set to 1024*768. Note that the accessibility of information and readability is lower at that resolution than it is at a higher resolution. For instance, one can access terms of use and safety information from a menu at the bottom of the page, less visible with a low resolution screen setting.

Summary of findings

Since Dailymotion is a video sharing platform, regarding safety and children issues, accent is put on age appropriate content. Key findings are:

- There is a "family filter", set to "ON" by default. However, one can easily set it to to "OFF" even when logged in as a minor (Lucie Martin, 11 year-old), could easily set parental control to "OFF".
- The report mechanism is present on each video. It is easy to use and easy to find. However, information on the reporting process can be found in a hard to find and not so easy to understand "legal" section. Very little information is provided after reporting content.
- It is easy to block a user, delete a comment or unwanted message. However, report tools are only provided for video content. There is no easy way to report conduct from another user.
- Information in the legal and terms of use sections is not designed for children, parents or teachers. Information is sometimes hard to understand for non-specialists, in particular for children.

Reporting the results

Principle 1: Raise awareness of safety education…

Dailymotion has a quite complete set of pages dedicated to "legal" considerations, including child protection. However, these pages do not take into account the different types of potential users (children, parents, teachers) and their specific needs.

The content could be quite difficult to understand for children. There is no dedicated page for them. Information focuses on the data protection, data retention, etc., more than on children protection, contact, conduct or content risks…

As stated in the self declaration, a video is provided: "Dailymotion also published an educational video for young people, which outlines safe and responsible Internet use so that young internet users can be more confident when browsing".

The terms of use details content that is not allowed on the site, consequences of engagement in prohibited, age requirements. However, this information, is presented in a "legal" language, that can be hard to understand for adults, and that is not adapted to children (even though children are not the targeted audience of the site, they can consult videos).

Since Dailymotion is more a video sharing platform than a SNS, contact risks are less taken into account. One can easily report when a video is not appropriate, but there is no easy way to report a contact.

Principle 2: Work toward ensuring that services are age-appropriate…

Creating a profile

In the self-declaration, there is no reference to the use of cookies. There is no reference either to "promoting the uptake of parental controls which allow parents to manage their children's use of the service". Therefore, when a child (11years-old) creates an account, he or she receives an e-mail, but parents are not warned.

You cannot create a profile with an existing address: in the registering form, a message is displayed indicating the e-mail address is already used.

In the self-declaration, Dailymotion indicates that: "When a French user is under 18, according to the birthdate provided during the registration process, they receive a specific email reminding them of the different features on Dailymotion (sharing videos, commenting on others' videos, creating groups…) and asking them to watch with the above-mentioned E-Enfance video with their parents".

Indeed, in the confirmation email received, two lines are added when the user is under 18: "In order to actively participate in the sensibilization of Internet risks for youngers, Dailymotion closely cooperates with the association E-Enfance. We invite you to visit a video explaining good practices in order to surf safely: http://www.dailymotion.com/video/x62m01_protegeons-ensemble-dailymotion_people » (translated by the tester).

Parental control

No adult content is allowed on the site, however, there can be some content Dailymotion refers to as "explicit". This is why Dailymotion states in the self-declaration it has a parental control device: "Once the

filter is turned off, the user can access explicit content (no adult content is allowed on the site). He still needs to either login or register AND confirm he is over 18 to view the explicit content".

The self-declaration states that it "provides a Family Filter, which is "on" by default. A user may turn off the Family Filter, but must explicitly confirm their age beforehand." The filter is actually set to "on" by default. When the filter is "on", the "sexy" video section appears but is not accessible: you are asked to set the filter to "off".

However, the filter is very easy to set to "off". Age is asked, and one just has to click on the 'I am over 18" button. Note that one can set parental control to off even when logged in as a minor (Lucie Martin, 11 year-old). There is no control that the user logged to the platform is logged as a minor and says he is over 18!

Principle 3: Empower users through tools and technology…

The self-declaration states (under principle 6) that "Accounts of users less than 18 years old do not appear in search results." However, the test shows that users under 18 do appear in search results when searched by username.

One can REJECT friend requests, BLOCK users or DELETE unwanted comments. In particular, nothing is said about tools to report inappropriate contact from another user. Indeed, contact is not the main objective of Dailymotion, the possibilities are not very wide. As stated in the self-declaration, one can block a user, cancel a friendship. However, one cannot easily report a conduct: the "flag this content" option only works on videos, not on messages.

Tests show that it is very easy to delete postings, either comments left on a video or messages sent by another user. It is also easy to remove a posting made on someone else's video. However, all users, as long as they are not blocked, can post a comment on a user's videos

Deleting a profile

Profiles can be fully deleted. However, information about deleting a profile is not easy to find. It can be found in the FAQ section. Even if that information helps, there is no clear link to delete a profile.

Information on what personal information is collected after deleting my profile can be found in the "legal" section. The information is quite difficult to understand for a child. This information is shortened in English: "Data is stored on the premises of the Website host and is kept only as long as necessary for the purposes set out above. After that point, data is kept only for statistical purposes and shall not be used for any other reason."

Principle 4: Provide easy-to-use report mechanisms…

In the self-declaration, the only information given is that "a link « This video may offend » is provided on each video". Nothing is said on the reporting procedure or if reports are acknowledged. It is very difficult to send the message "someone is sending me scary messages…" as Dailymotion only provides an easy to use mechanism to report a video. The possibility exists but the tester was only able to find it after the SNS pointed it out.

Reporting

The testing on the reporting procedure confirms that there is an accessible link for each video to report an abuse. This link leads to a form where one has to enter:

- Select a category (pornography, racism, etc)
- e-mail
- comments

The procedure is quite easy, however the information on what to block is available only in the "legal" section, that is not easy to find (very bottom of the page) and not so easy to understand for children/young people.

Contacts

Contacts are not the main objective of Dailymotion, the possibilities are not very wide. However, as stated in the self-declaration, one can block a user, cancel a friendship. One can block a user, and unblock him later. However, one cannot report a cyberbullying: the "flag this content" option only works on videos, not on messages. One can delete a comment or block a user, he/she must confirm he/she wants to block this user. A message confirms that the blocking is effective "we took care of lucmartinssnpt09. You should no longer hear from him". When Lucie (11 y-o) wanted to block a "friend" user, he switches from the "friends" list to the "blocked users" list. She can unblock him. However, this user could still access Lucie's profile, and she still appears as a "friend" in his profile. He never was notified he was blocked. However, when he wants to send Lucie a message, he is told that she does not want to receive messages anymore.

Principle 5: Respond to notifications of illegal content or conduct

In the self-declaration, Dailymotion states that a support team works 24/7 to deal with and act upon all notifications.

Principle 6: enable and encourage users to employ a safe approach…

In the self-declaration, it is said that "Users can choose to hide any personal information provided during the registration process". No information is given in the self-declaration on the privacy options, if these options are accessible at all time or what information is automatically uploaded onto their profile. Age, gender, home town and real-name are automatically uploaded onto the profile.

It is quite easy to change privacy settings. One can for instance change information, decide whether the age or family name are publicly displayed.

One can look for users of all age, but only by their pseudonyms, not by their age or other characteristics.

What's on the profile: Nothing is said in the self declarations about what information is available in the profile. When creating a profile, the name and age are automatically inserted into the profile, but can be set to "private" by the user. The full address is not public: only the country and town are public. The user can add a picture once the profile is created.

Searching a profile: Any users (even unregistered) can search a profile, including children's profile. Information displayed are the nickname and the online status.

Principle 7 : assess the means for reviewing illegal…

In the self-declaration, Dailymotion states the "the support team then reviews the videos to make sure there is no inappropriate content uploaded to the site". It is also said that "Dailymotion Support team works 24/7 to deal with and act upon all notifications". In the self-declaration, there is no information on the filters or technical tools used to flag potentially illegal or prohibited content.

Conclusion: global assessment of compliance

Assessment of the Principles vs. the Self-declaration

Principle	Compliant	Partially Compliant	Not Compliant	Not Applicable	Comments/ Clarification
1	X				One thing missing: the self-declaration does not mention targeted information for teachers.
2		X			Nothing is said about parents being able to "manage their children's use of service"
3	X				
4	X				
5		X			- Notification possible only on content, not on conduct "link: this video may offend".
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			- No targeted information for parents. No educational materials. Legal language difficult to understand for children.
2		X			- No measures are taken to "prevent users from attempting to re-register" - Age restriction (parental control tool) is not effective, as an underage registered user can access explicit content
3	X				- Users under 18 do appear in search results when searched by username, though the self-declaration states they do not.
4		X			- Notification possible on content, very difficult to find on conduct "link: this video may offend".
5	Not Tested				
6	X				
7	Not Tested				

FACEBOOK

Bojana Lobe, University of Ljubljana

Introduction

Facebook is a service that connects people with friends and others who work, study and live around them. People use Facebook to keep up with friends, to share links, to share photos and videos of themselves and their friends. The minimum age required to join Facebook is 13. Users can add friends and send them messages, and update their personal profiles to notify friends about themselves. Additionally, users can join networks organized by city, workplace, school, and region.

The following is a report based on the testing of social networking service Facebook. The main English version was tested.

Summary of findings:

- Safety information is available to all, also those not signed up.
- The safety information is targeted to parents, but not to teens and teachers.
- Parental control tools are very limited.
- Report mechanisms are partially efficient as they are not visible at all times.
- Users are provided with various tools to control their privacy settings.
- Minors are not searchable through search engines.
- Applications (3rd party, external or additional programs and/or services) need permission from
- the users to be installed and/or pull info from user's profile.

Principle 1 "Raise Awareness"

In the Self-Declaration:

The self-declaration does not include information neither on Terms of use nor on privacy. The information on safety is modest, focusing on the accessibility through the links and special search term results to allow easy navigation to safety principles.

Safety information is stated to be targeted towards specific user groups, declaring that Facebook has participated in educational efforts "for each of these groups" (where it is assumed that the provider refers to the groups listed in the Principle 1: users, parents, teachers and carers). It does not mention children. The provider does not specify whether the information is presented in a prominent way and a practical format nor whether it is easy understandable.

The self-declaration does not state that the safety information provides guidance regarding inappropriate content and conduct and information on the consequences of breaching the Terms of Service.

Moreover, it is not stated that the service includes information on links to educational material and technical controls for parents. Despite not addressing this issue and not mentioning parents explicitly the provider states that they have participated in educational efforts for parents and teachers. Further the

provider mentions the participation in "Teach Today", an industry consortium working with stakeholders throughout the EU to provide material for teachers about internet safety.

On the site:

In **Facebook** both the Terms of use and the Privacy Policy are very easily found on the site. It is also easy to find the Safety Policy and safety tips/information for parents as well as links to educational material or organizations active in child safety. Safety tips/information to parents is in general sufficiently easy to understand and to access.

Safety tips/information for children and teachers could not be found, apart from recommendation that the minors aged 13 or older should consult parents for permission before sending any information about themselves to anyone over the Internet.

The provided information is in textual format. Information on safety settings of the user's profile is briefly addressed (just stating that one can have control over it). External links to professional safety organizations and authorities are provided.

The Terms of use clearly list content and conduct that are not allowed, as well as the minimum age requirements (age 13). Further, the consequences of engagement in prohibited behavior are also listed.

In general, information on specific risks is not found apart from information on seeing an objectable photo (does not mention what kind), hate speech and bullying. The information on bullying as well as how to report or respond is sufficient.

Principle 2"Ensuring Age Appropriate Services"

In the Self-Declaration:

The self-declaration does not outline how it is made clear to users when services are not appropriate for children and young people neither how it is made clear to users where a minimum age applies. But it does outline the steps taken to deny access (the users are required to provide birth data), delete under-aged users (the analysis of friend connections by age) or to prevent under-aged users to attempt re-registering with a different account. They use cookies to make re-registration difficult once a user has given a birthdates indicating they are under 13.

Further, the provider mentions built-in tools for users of Pages and Applications that allow restriction of content provided through these channels to certain age groups. The provider also outlines other means they have employed to limiting exposure to potentially inappropriate *content* (special restrictions on advertising targeted to minors).

The provider does not address in the self-declaration how uptake of parental controls is promoted on the service.

On the site:

When signing up to the Facebook, no age verification is needed, meaning one does not have explicitly state (or tick a statement) that the user signing up is above certain age. However, the service requires you to list your year of birth (but not the date). Also, email verification is needed. The attempt to sign up as a 11-years

old failed. One is prevented from re-registering by use of a cookie. Once the cookie was removed, the sign up as a 15-years old was successful.

On Facebook, no parental control tools can be found. In the Facebook safety section, the provider explicitly states that it is generally forbidden by privacy laws to give unauthorized access to someone who is not an account holder. However, if parents believe their under-13 old child has created an account, they can request Facebook to permanently delete such account.

Principle 3 "Empower users through tools and technology"

In the Self-Declaration:

The provider does not indicate in the self-declaration any employment of tools and technologies to assist children and young people in managing their experience on their service. The mention that Facebook provides users with extensive controls around their profiles and content and with setting reasonable defaults for minors, mentioning the restrictions of creation of public search listings and the possibility for users to choose who can access their information and who not. However, the provider does not address any further details.

On the site

The information on how to report abuse or bullying, how to block other users from contacting you and on the possibility to specify who or which groups of users that could contact you can easily be found on the site.

Once signed into the profile, the user is able to delete/remove posting and photos on their profile as well as those they put on other profiles.

Other users cannot post comments on the profile as only users' friends have this possibility. Also, personal information (the one user decides to share) is not visible to other users but only to friends. The default setting for personal information is to be visible only to friends for all users (set to private as opposed to public). The user also has the possibility between choosing online or offline status when signed into Facebook. However, there is no possibility to be invisible (which means that one is able to see other users but other users are not able to see them). The user is also notified when tagged in a photo by friends but does not have a chance to approve the photo before being published. However, one can remove a tag once the photo is published and has been notified of being tagged. Also, there are privacy controls for 'photos tagged of me', which a user can set to reduce the visibility of who can see a tag.

Safety tips and/or guidance about publishing personal information or a photo on the profile is not provided.

In case of attempt to delete the profile, information can be found in the Privacy Policy page. There is also a clear link provided in the account-setting page that enables deactivation. On the site, only a link for deactivating a profile is provided. However, if user would like their account permanently deleted with no option for recovery, one has to submit a request to Facebook[2]. The provider does not state any information

[2] To get to this information, one has to go to settings, and click on help. Then one has to search for "delete account" and as a result a list of FAQs is displayed. One can then click on the FAQ "I want to permanently delete my account. How do I delete my account?" and the above procedure is described there.

about what personal information the SNS collects/retains after deleting/deactivating my profile or how it is used.

The under age users can search for users their own age (17 and below) and are not searchable through search engines such as Google. Interestingly, when trying to search for a 13 years old, it was searchable through Facebook both through adult and minor account whereas the 15 years old was not found in either case.

Principle 4"Provide easy-to-use mechanisms to report violations"

In the Self-Declaration:

Facebook provides contextual reporting links on content throughout the site and has led in setting service levels around response times for reporting nudity, pornography, and inappropriate contacts directed to minors.

However, it does not say whether the mechanism is understandable to all users, and that reports are acted upon quickly.

The declaration does not indicate that the reporting procedure is age appropriate or that reports are acknowledged, or that the users are given indications on how such reports are typically handled.

On the site:

When signed into Facebook profile, a link for reporting other users is not visible at all times, as one can only report users who are not one's friends (the link to report/block non-friends always appears under the basic version of their profile) No link is provided to report friends or block them, as only a link to remove a friend is provided. Therefore, one cannot report friends' profiles or messages, but one can report their photos, videos, and notes. Once a friend has been removed, and becomes just one of other users, that friend can also be easily reported or blocked. However, one can go to "settings" and then click on the "block list" and search for a person one wishes to add on a block list. That person can also be a friend. If a friend is added to the block list, then it is immediately removed from friends. Also, one can decline a friend's request.

The information on how to report a friend is not directly found. The link/tool where one can report abuse/violation of terms is also not provided or visible at all times.

As stated above, one can only report photos, videos and notes but not other content (e.g. wall posts or comments). The button to report photos is easily found below photo.

The report mechanisms are in general easy to understand (one just has to click on the link and gets further information on what the reports is being about).

When the report is sent, one immediately receives the message: "An administrator will review your request and take appropriate action. Please note that you will not receive a notification about any action taken as a result of this report. We apologise for any inconvenience this may cause."

After sending a test report, one only receives the above message but as indicated in the message above, one does not receive a notification about any actions taken as a result of the report.

Principle 5 "Respond to notifications of illegal content or conduct"

In the Self-Declaration:

The provider states they have integrated a real-time blocking and reporting system based on NCMEC's list of known internet URLs hosting child pornography and deployed multiple systems to detect and respond to anomalous behaviour on the site. The provider also states they work with law enforcement and affiliated agencies, including NCMEC. However they do not provide any details on how they link with law enforcement and affiliated agencies.

On the site:

The reporting mechanism was not tested for illegal content or contact.

Principle 6 "Encourage users to safe use of personal info and privacy"

In the Self-Declaration:

Regarding enabling and encouraging users to employ a safe approach to personal information and privacy, the provider states they seek to assure that the users understand the site's powerful privacy setting (not providing any details) and that they conduct regular education campaigns to assure that users are aware of potential risk information sharing and knowledgeable about the extensive privacy settings available on the site.

On the site:

On Facebook it is quite easy to change one's privacy settings. At the registration, the user is asked to age, email, gender and real first and last name. Optional, user is asked to provide school or workplace information and a photo. A range of other information can be provided once registered by the user if wished so (political views, religion, relationship status, interests etc.).

From the provided information at the registration, the age, real name, gender and email are automatically inserted into the profile. Other information is inserted once the user provides it (if decides so).

Also, applications (3rd party, external or additional programs and/or services) need permission from the users to be installed and/or pull info from user's profile.

Principle 7 "Assess means for reviewing illegal or prohibited content/conduct"

In the Self-Declaration:

The provider mentions that they are regularly assessing ways to optimize their systems to detect and remove inappropriate content and conduct, engaging in discussions with government and other stakeholders to ensure constant improvement. They do not provide any other information on this in self-declaration.

On the site: This principle is not tested on the site.

Summary of results

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	*Not Tested*				
6	x				
7	*Not Tested*				

GIOVANI.IT

Giovanna Mascheroni, University of Torino & Università Cattolica di Milano

Introduction

Giovani.it (http://www.giovani.it/) is part of the SMG (Studenti Media Group) which provides others social networks and websites for young people: Studenti.it (where to share and access school related material), girlpower.it ('the websites for trendy, fashionable girls'). Giovani is comprised of a variety of interrelated areas and tools for communicating and networking, which are described in the menu bar at the top of the homepage:

A forum, whose threads are organized in the following categories: sex; love; literature; music; news, politics, society and religion; mobile phones; videogames; computer and the internet; sport; forum editorial staff; helpline (with forum code of conduct and abuse reporting, specific to the forum area); XXX (fetish, pornographic, and encounters offline)

- The community, that is blogs and personal profiles
- Groups, a database of the groups formed by the members (the two most populated are MSN and 'Against paedophiles')
- A gallery of pictures from blogs
- A video gallery, also from blogs

Under the menu bar, the homepage is organized in some sections showing respectively: the latest blog entries and, beside, the picture of those users who are online; underneath a photo gallery from blogs pictures; then news (mainly concerned with cinema, celebrities and sport); and again a list of forum channels; at the very bottom of the page celebrities photos and polls. The terms and conditions, privacy policy and help button are linked on the small menu bar at the very bottom of the page, and the user needs to scroll the whole page in order to find them.

Once logged in, the page accessed has a menu bar on the top and on the left side (in the middle of the page just a welcome message appears). Starting from the left hand bar, there is a 'gallery' link, where you can access you friends galleries; 'blog' where you can post new entries and manage your blog layout (upload pictures and videos, choose the layout etc.) and check your friends' latest posts; 'groups' to manage your membership to groups or to see your friends' groups; 'events' where you can check your network's events (my network is by default the network of people from my city); 'I like', where you can pick your favourites from a weekly top 20 list of music, movies, and books; 'mystudy' to share and access school notes, look for mates to prepare for exams, etc.; and 'mobile' where you can match you mobile phone number with your login information so as to upload new posts and MMS by mobile.

The top page menu consists of: 'profile' where you can manage personal data, upload an avatar or picture for the profile, set the privacy settings etc.; 'friends' where you get friendship requests, or are able to invite new friends, or manage the 'enemies list' (the list of undesirable friends banned from your blog); the 'network' of the city of Milano, divided in 'events', 'the wall' (mainly requests for help with schoolwork), and members; 'messages' that is the inbox; and 'online users' where to access the list of people online.

Though not specifically mentioned under the service's terms and conditions, access to Giovani is restricted to 14-15 years old (people born in 1994) or older.

The SNS has not yet published a self-declaration of Safer Social Networking Principles, so the following report will be based only on the expert's observations and testing.

The test has therefore measured the compliance of the tools implemented on the SNS with the Safer Social Networking Principles. To sum up the major findings, the provider has fully adhered only to the second Principle. While providing some useful tool to ensure a safer experience for children, the SNS still shows some critical points, related to information on safer use and privacy settings.

The report of findings will be articulated according to the 7 Safer Social Networking Principles.

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

The SNS provides a 'terms and conditions' statement, and a privacy policy but has no explicitly stated safety policy nor safety tips customized and targeted at parents and carers. Helpful information for children regarding code of conduct, inappropriate content and safety tips is disseminated in different areas of the website, rather than being located in a single page/section.

The terms and conditions, accessible from the menu bar at the bottom of the homepage, which is common to all the Studenti Media Group, states the inappropriate and illegal content (see terms and conditions 1.6) and code of conduct but adopts a legal language which may result difficult for younger children. Similarly, the privacy policy page includes information on the treatment of personal data by the SNS provider, in the same legal language.

Far more helpful are other sections of the website, specifically:

The Help page, accessible from the menu bar at the bottom of the homepage, provides general information on the services provided and general tips for new users, as well as some specific safety information. Safety information include: a box on the left side of the page called 'Report misuse and children safety' containing a link to an online form and the address of the help desk; a link 'Profilo, interessi e dati personali' (Profile, personal interests and data) where children are provided information on how to manage personal information and how to set privacy settings (the default setting is a profile visible to all visitors, but you can turn it into a profile visible only to logged in users, or only to friends). There is also a link to the help channel in the forum. The Help page provides information relating also to technical problems (explaining for example to newbies how to upload blog entries and pictures; or how to join or crate groups, etc.)

The help blog (http://helpblog.giovani.it/), accessible by a link on the help page, which provides information on how to solve problems with the blog management, including some safety information: children are told how to block undesired users and comments (the process follows two steps: add a user to the 'enemies' list, and a filter to restrict friendship requests and comments by age or online activity specifications. It is for example possible to block users who have more than 10 'enemies').

The help channel in the forum, which addresses issues concerning the use of the forum, including the forum code of conduct and abuse reporting.

Useful information, therefore, is disseminated in a variety of places. Therefore, some of the most useful safety information requires some steps before being accessed, and this may result in difficulties for some users in accessing the information they need.

To sum up the type of information available and its location:

- Information on inappropriate or illegal content is available in terms and conditions (1.6) and help blog (http://helpblog.giovani.it/diari/2598748/quali_sono_i_contenuti_non_permessi.html)
- Information on inappropriate behaviour or misconduct is provided both in the terms and conditions and in the help blog. The terms and conditions, anyway, provide a general reference to inappropriate behaviour with no clear examples of misconduct (see 1.4): it just tells that 'the user agrees to use the service only for legal purposes and respectful of the protection of personal data according to the law on privacy'. The help blog, instead, (http://helpblog.giovani.it/diari/2598748/quali_sono_i_contenuti_non_permessi.html) lists inappropriate content and (implicitly) behaviour.
- Information on consequences of engagement in prohibited behaviour is clearly stated in Terms and conditions 1.6.
- Information on specific risks regarding using online services is not explicitly provided within the above mentioned documents.
- Overall, the information provided is only textual and poor of concrete examples and anecdotes, resulting somewhat impersonal (especially the terms and conditions). No references to institutions and NGOs concerned with online safety are provided.

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

Though age requirements are not explicitly stated in the terms of use and privacy policy of the website, the service is age restricted enabling registration only by children born at least in 1994 (so 14 or 15 years old is the minimum age allowed). The child is not asked to state being above a certain age by ticking a box, but she/he needs to declare being assisted by one parent in the registration process.

The registration process is successfully completed only after email verification, since login is unsuccessful and the user is not recognised unless she/he clicks through the link provided in the verification email.

Cookies prevented the tester from re-signing up as a 15 years old child: the registration form was completed and sent, but apparently it was not accepted by the service, since any verification email was received. Therefore login with the second was unsuccessful. Only after deleting cookies and completing a new registration with a third profile, the tester was able to join the community as a 15 years old girl.

Despite the need to state that parents are aware of the registration and assist their child in the process, no parental control tools are provided.

Principle 3: Empower users through tools and technologies

Information on how to report abuse or bullying is not immediately available on profile settings, but accessible from the homepage in the help section. However, the user has the power to block unwanted users, turning them into 'enemies' and report them to the SNS provider.

As soon as logged in during the performance of the test, the tester has been contacted twice (both as a 15 years old girl and as an adult) by an online user, whose name was Andrea, who sent the following request of contact: 'Hi I am Andrea From Milano, are you interested in offline meetings?'. Thanks to the above mentioned possibilities to block requests of contact, the tester added the user to the 'enemies' list and reported him to the helpdesk through the notification of misconduct form (see principle 4).

Users are provided with the possibility to specify who or which groups of users can contact them by setting filters which parameters are represented by age, and by their online activity (how much personal information do they disclose in their profile, how many blogs do they have, how many friends, how many enemies, etc.)

Information on restrictions on search options for profiles (for example if adults are not able to search for minors) is not clearly provided.

User can find clear information on how to remove postings on her/his profile but the tester was not able to find information on how to remove pictures posted by other people, or personal comments and pictures posted on other people's profiles.

The possibility to restrict posts on a user profile only to friends is given, though the default option is that all logged in users can post comments on other people's profiles. No default option, instead, is provided for the blog, where user needs to choose among these restriction possibilities: nobody, everybody, only friends, all users except enemies, only users can post comments on the blog.

Regarding the possibility to restrict personal information only to friends, the information is misleading at this respect: on the help blog it is stated that information is available to all users, while on the privacy settings in the profile the default options is that your blog and your profile gallery is visible only to friends.

Users are given the complete control over the display of their online status by choosing if making their status visible to all users, only to friends, or invisible.

When setting the profile and uploading personal information (tastes and interests, school, etc.) or uploading picture no safety tips or guidance is offered.

The tester was not able to find information about the notification when user is tagged into other people's pictures.

The user has the chance to delete her/his profile, thanks to a link in the 'options' under the profile settings. The information on how to delete the profile is available under the FAQ lists in the help page but the information is misleading: here it says deletion is immediate, while on the profile options it says it needs 7 days to become effective. No information on how the provider uses personal information (if it is retained) after deactivating the profile is available in the help page nor in the options in the profile setting area.

Principle 4: Provide easy-to-use mechanisms to report content or conduct that violates the terms of the service The form to report misconduct, abuse or bullying is available on the left side of the Help page, or in a pop-up when receiving a message from another user. A link/tool where to report abuse or violation of terms visible at all times is missing from the profile page and tools, but as the link is provided when receiving messages or requests for friendship by other users, its lack is partially solved this way.

Information on how to block a user is provided once receiving a message or within the privacy options in the profile settings (under the voice 'block users').The user has the possibility to approve or decline a contact request.

When blocking a user and reporting his/her behaviour as inappropriate or offensive, no notifications messages are sent back in the profile's inbox, nor in the mailbox of the email address provided at registration.

According to the methodology, while performing the test the tester has sent a notification through the report abuse mechanism, asking for help because someone was sending scary messages. Until now (almost one month later) the tester hasn't received any response by the helpdesk to the request for help.

Once completed the abuse form on the Help page a notification message appears at the end of the process indicating that the user has sent a notification about a violation on a certain date.

However, the helpdesk where the abuse report is received and managed does not send any information on how the report will be handled nor provides any feedback to the user message explaining the abuse or violation of terms.

Principle 5: Respond to notifications of Illegal content or conduct

The principle has not been tested on the site.

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

Privacy settings are easily changeable and manageable from the profile setting options.

Apparently there are no additional applications apart from the option to combine a mobile phone number to the profile so as to upload pictures and post via mobile (and a registration process is required), or from the newsletter which is considered an integral editorial service of the provider (therefore un-subscription is impossible unless you deactivate your account). Part of the information provided during registration (age, gender and city of residence) is visible to all users. The information provided during registration includes: age (birth date), gender, educational level and name of the school or the University attended, email address, postal code of the city of residence (but not the home address), first and last name. Apart from education and school attended, all these fields are mandatory. Of the personal information used for registration only age, gender, first name and city of residence have been automatically inserted into the profile.

When signing in the service for the first time a pop up button appears announcing that for new safety policy the provider decided to make also name and surname available on the profile, and not only nickname. But then the user is asked to choose if she/he wants her/his surname to be visible to all users or if you want to be identified only by your nickname and first name.

The list of the online contacts is not age restricted, so any user can search for younger users (up to 14 years old) and the tester had no problem in searching for her 15 years old profile by inserting the nickname.

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

Since the provider has not yet published a self-declaration, assessing the means for reviewing illegal or prohibited content/conduct is not possible at this stage

Summary of results and conclusion

Since the provider has not yet published a self-declaration, the test has only assessed the level of compliance between the Safer Social Networking Principles on the one hand and the measures implemented on the SNS to adhere to each principle. The following table provides the results of this comparison.

Assessment of the Principles 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	*Not Tested*				
6		X			
7	*Not Tested*				

As we can see from the above table the provider is fully compliant only with the second Principle. The provider includes some useful tools (the report mechanism, the filter tool to block some contacts and the 'enemies' list are the most evident) to promote a safe environment for users.

Nonetheless, the testing of the SNS has pointed out some critical aspects of the service. These are articulated in two main areas: information and privacy settings.

As far as information is concerned, as we have seen, safety tips are confusing due to their fragmentation and dissemination in different areas of the website. Fragmentation and dissemination may result in misleading information, as regards for example the process of deleting and deactivating the account.

As regard privacy, the default settings (profiles are by default visible to all users and so is the online status of the user) tend to expose younger users to risky contacts or contents.

A further critical aspect concerns the report of abuse and violation mechanism: though reporting an offensive message is easy (since the possibility is provided contextually to the reception of the message), reporting inappropriate contact or conduct independently from the reception of a message might be more difficult (since the form is provided in the help page not on the profile itself). Moreover, feedback on how the report was handled by the provider was not made available to the user reporting violation.

In conclusion, the provider has only partially implemented measures to empower users and to encourage a safer approach towards the display and management of personal data online.

GOOGLE

Leslie Haddon, London School of Economics and Political Sciences

Introduction

YouTube, owned by Google, is primarily a site for posting videos and viewing other people's videos. The reason why it is included in this test is that it has some SNS elements, mainly user profiles, but also the opportunity for users to communicate e.g. in terms of comments regarding videos posted. The minimum age of users is 13 years old.

At times YouTube provides multiple approaches addressing the same issue, elements that go beyond the minimum stated in the principles and features that exist in practice but are not in the self-declaration (as in the case of material for teachers). Some other elements of the principles have not been addressed in the self-declaration. Sometimes in testing the mechanisms could be better or the information/options could be made more visible (principles 2 and 6) but they are compliant with the claim in the self-declarations that they exist.

The principles

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

The self-declaration includes information on the terms of use to which users should abide, located in the Community Guidelines. Information about safety is covered at various points in the document, mainly in relation to their Safety Tips facility. The self-declaration notes that YouTube encourages and advises upon privacy issues, as well as providing tools (such as the ability to hide personal information) and a complaint mechanism. The declaration indicates the importance specifically of educating children about online safety and points to the various sections in which to find safety information, including additional advice on how to use tools in the Help Centre. It notes these are accessible, by virtue of being at the bottom of every page (there is no comment about it being 'prominent'). The declaration also notes that the tools are written in an easy to understand, user-friendly format and indicates the type of content and conduct that will not be tolerated, as well as the consequences of breaching terms of service. There is information aimed at empowering parents, but in the declaration there are no comments about advice specifically aimed at teachers

All the policy statements (terms of use, safety, privacy, code of conduct) are easy to find through links at the bottom of the page. Safety tips could also be found there and there was also a dedicated Safety Centre, with information for children and resources for parents. Although the declaration itself says little about addressing teachers, apart from mentioning that they too can watch the safety videos, there are, in practice, educational resources for them. The advice was always easy to understand for children of various ages and adults, and certainly sufficient in terms of raising a range of issues. The videos were useful for showing both how to report problems and illustrating specific situations, and there were some links to other agencies. Clear examples of the types of content and conduct that will not be tolerated are easily accessible, as is an

indication of the consequences of breaching the terms of conduct (e.g. account can be terminated). All of the items listed in the test can be found (i.e. hate speech, porn, violence, stranger danger, bullying, divulging personal information, posting sexually provocative photos and images of child abuse – the latter discussed in relation to child exploitation). One the other hand, the list of prohibited items goes beyond those tested to include gory content and content that incites violence as well as videos of reckless and dangerous conduct.

In sum, as regards the self-declaration, there are no comments about teachers, therefore it is partially compliant to the principles. However, in terms of testing the educational material is there, all the policy statements can be found at the bottom of the pages and are clear. The advice is reasonable, videos quite useful and what is not tolerated is in place. Hence this aspect is judged to be compliant.

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

The self-declaration notes that 'age-restricted' content is only viewable by those over 18, that there is a minimum registration age of 13, and that if children enter a birth-date revealing they are below that age they will be denied entry. The provider does not outline the steps taken to delete under-age users, but says that a cookie will be placed on users' browsers to stop them trying to re-register with a different age. There is no information on any additional means to enforce compliance with minimum age requirements, nor how, in detail, to actually promote the uptake of parental controls, nor if professionally produced content is only shown at particular times of day (although the essence of YouTube is that it is mainly amateur produced content). One key mechanism used for limiting exposure to potentially inappropriate content is the 'flag' system, enabling the wider YouTube community to mark video content that is dubious for various reasons. This material can then be excluded from certain listings and areas. In addition, YouTube has implemented automated systems to help classify content.

It was clearly stated on the YouTube site that the minimum age is 13. As the first part of the registration process, one has to acquire Google or YouTube account, which means providing a date of birth, gender and post code. When applying to YouTube in the test the system did indeed reject the application whose birth date meant they were younger than 13 at this early stage in the registration process, before the verification phase described below, with system providing the message that this rejection was 'based on the information submitted'. If the user then applies as a child over 13, the system moves to the next stage asking for an email address that is to be verified (i.e. YouTube then sends a link to that address that the user needs to click on). If the user uses an address the system recognizes as being used by a previous account, the system asks the user to open that existing account and so the 'child' does not get further. However, if the user ('child') has set up a different email (e.g. hotmail) address for verification, YouTube lets the user open the new account. So if a cookie is indeed placed on the PC, it does not stop this tactic of setting up a new address for verification. Hence, while the verification plus cookie tactic may stop the fainted hearted, a determined, knowledgeable under-age user can get round it by setting up new accounts. As regards the 'age-restricted' content this was, the over 18 adult user could access this material (e.g. when searching for 'porn') but the 15 year old user could not. The message said 'you must be over 18 to view this group – hence the system works. When navigating 'as a child' and 'as an adult' there were no noticeable messages about this, but this may be an automated process that only operates when searching for videos. There is an extra way of checking age not mentioned in the self-declaration – we are told on the YouTube website that if a video is flagged by someone, the images on it may give rise to doubts about that user's age and the account may be closed.

In sum, in the self-declaration the provider has addressed sufficient suggestions and volunteered mechanisms to be viewed as being compliant to the principle. In terms of testing, there are controls in place on what under-18s can view, as claimed in the slef-declaration. As regard minimum age of access, we need to consider the following (a) the provider's self-declaration says that a cookie is placed on the browser to stop re-registry of under-age users with a different age b) an under 13 year old re-registering on the same browser simply with a different age is not successful but (c) an under 13 year old re-registering on the same browser and PC with a different name and age (i.e. pretending to be older) can register. In other words, the mechanism could be more effective but since the test shows the provider adhered to what they claimed in the self-declaration, then they have to be judged compliant at this level.

Principle 3: Empower users through tools and technology

Google makes it clear that YouTube's profile pages are not the same as standard SNS ones, since the aim is to encourage the sharing of user-generated content rather than encouraging social networking per se, and hence searches are searches for videos rather than for profiles (here called 'channels'). The declaration notes that users can volunteer information about themselves. Although the default is not 'private' it is the user name, not the actual name, which will appear. The declaration does not say that users have control over who can access their profile, but it does say that they can choose to only share a video with friends/family, and that they can block comments posted by other, as well as pre-moderate and post-moderate them, which implies the ability to delete unwanted ones. Users can report inappropriate contact such as violation of privacy, harassment and cyberbullying. The introduction to the self-declaration says that parents are given tools to protect children, but does not say how it educates parents in relation to principle 3.

As specified in the self-declaration, it is not possible to search for user profiles, and that means adult profiles let alone child ones. Users have controls to block others (or rather 'specific others', rather defining which groups - e.g. by age - can make contact), and they can remove any postings from others on their profile. Some parts of the profile appear to be visible to all viewers by default (e.g. user name and statistics about usage, such as when they joined and number of videos watched). In addition to advising parents to talk to the child as a first step, parents are also given some tools and clear information about how to use them (e.g. 'hide objectionable words', 'hide comments', 'restrict search options'). Parents do not have to verify the child's (initially very limited) profile before it can be used, although they can monitor what the child has viewed (although YouTube acknowledges that the child can get round this). Ultimately the provider can shut down the child's access, although this involves the parent contacting YouTube.

Google notes that the profile is limited, reducing stranger danger. Of course, if children then volunteer more about themselves they could be identified, but they are given advice about this.

In sum, given that various measures that may be included according to principle 3 are in fact noted in the self-declaration, this must be judged to be compliant with the principle. In terms of testing, the system does what is claimed in the self-declaration and is therefore complaint.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the terms of service

The 'flagging' system noted above provides a method for reporting inappropriate content, while the Help and Safety tool provides a way to report contact and conduct, and these channels are available at all times. The self-declaration does not comment upon whether these reporting procedures are reasonably

understandable, age-appropriate or whether reports are acknowledged, but it does say that flagged videos are reviewed promptly (within the hour), although there is no comment specifically about the speed of reacting to other types of report (although there is a note that YouTube reports child exploitation to the police). In the self-declaration there is also no comment about the information to make an effective report (although this is fairly clear when you actually try to do this), nor an indication of how, in terms other than speed, reports are typically handled.

The test shows that users can report inappropriate contact and conduct (e.g. with the Health and Safety tool), with slightly different mechanisms operating for different types of reporting, e.g. content of videos vs. hate speech. These reporting tools are easy to find and understand – the user is offered various options. For example, in the case of unwanted contacts the system asks the user name of the person and how they are harassing you – the user does not write a message, but picks from choices, (which means that the actual wording of the test could not be used). While there is no message notifying the user with the words 'the report has been received', in the test the automated system made one first check of the claim of harassment and immediately displayed results that no-one could be harassing in the test because there were no messages from outsiders to the new account.

In sum, the self-declaration does not comment on some of the provisions of the principles (reporting procedures are reasonably understandable, age-appropriate, whether reports are acknowledged, the speed of reacting to reports other than those relating to content) and so should be judged partially compliant. In the test the reporting mechanism is clear enough and the automated system detected no harassment and therefore has to be judged compliant with the self-declaration claim that a reporting mechanism is in place.

Principle 5: Respond to notifications of Illegal content or conduct

As indicated above, the self-declaration provides information about the content reviewing process, noting that offending material will be 'dealt with appropriately'. There is additional information about technologies to prevent the re-upload of removed material – indicating that some such material might be removed. The self-declaration says that there are arrangements to report criminal content and conduct to the relevant law enforcement agencies, and there are links with a variety of other relevant organisations. If these measures are in place then the provider has to be judged compliant.

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

A range of privacy setting options is implied by the declared ability to hide information or share videos selectively, and the self-declaration says that users are provided with tips to make informed decisions about the information they post, tips that are accessible at all times (the declaration does not comment on the availability of privacy options, although in practice they are always there). While there are no comments on the implications of automatically uploaded registration information for profiles, notification to users that this information is used in profiles and the ability of users to edit this information, to put this into perspective, the initial profiles on YouTube are very limited (user name, when joined, when last signed in, number of videos viewed, country). Later one can choose to add more information. There is no comment on the ability to view privacy settings 'at all times', but self-declaration says they are 'on the site' and so this if they are always on the site it is implied that they are always available.

In the test, a user can change the privacy setting in Google Accounts at any time e.g. so that only friends can send messages and share videos. The privacy policy online indicates the type of information that YouTube collects about users and that email addresses may be passed on to third parties. On registering for YouTube, users provide information about age, their email and gender, but, unless they have read the privacy policy, the user is not warned at this point about what information might be used in the initial profile that is generated. The location of the profile details could be clearer – the option appears only when moving the cursor over the user name, so if you just look for it on the screen it is not visible.

In sum, he provider has to be judged complaint with the principles, given that the initial profiles generated are very limited. In terms of testing, the information provided could be clearer, but in general the site does what is claimed in the declaration and so is complaint.

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

The flagging system noted earlier provides the human form of moderation (to flag potentially illegal of prohibited content), which is complimented by automated systems to classify content. The declaration notes that it responds to this flagging of content, but says nothing in detail about it's response to conduct reports. There is no comment on the steps taken to vet any human moderators (although nothing has been said, either, about moderators contacting children in the first place, so it is unclear whether this is an issue).

In the self declaration that there are multiple systems in place, and so this must be judged complaint with the principle

Summary of results and conclusion

At times YouTube provides multiple approaches addressing the same issue, elements that go beyond the minimum stated in the principles and features that exist in practice but are not in the self-declaration (as in the case of material for teachers). Some other elements of the principles have not been addressed in the self-declaration. Sometimes in testing the mechanisms could be better or the information/options could be made more visible (principles 2 and 6) but they are compliant with the claim in the self-declarations that they exist.

Assessment of the Principles vs. the Self-declaration

Principle	Compliant	Partially Compliant	Not Compliant	Not Applicable	Comments/ Clarification
1		X			There are no comments in the self-declaration about teachers
2	X				
3	X				
4		X			Does not comment on some of the provisions of the principles
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				Since the test shows the provider adhered to what they claimed in the self-declaration, then they have to be judged compliant.
3	X				
4	X				
5	Not Tested				
6	X				But the information provided could be clearer
7	Not Tested				

HYVES.NL

Michel Walrave MIOS, University of Antwerp, Belgium

Introduction

Hyves is one of the most visited websites in The Netherlands and counts more than 9 million members. This social network platform started five years ago and is available in two languages (Dutch and English). The founders refer with the name of their SNS to a *beehive*, full of activity. Members can keep contact with friends and meet new people. Next to their profile, users can develop and consult blogs, post comments on profile pages, upload and browse through users' pictures and videos. Also 'gadgets' can be added to one's own profile (embedded third party applications). Moreover, users can create groups ('Hyves') that gather persons sharing, for instance, the same interests. The SNS has created also a mobile application, giving the possibility to be connected everywhere. Persons younger than 16 years need their parental permission to subscribe. According to a recent study, three quarters of the Dutch 8 till 17-year-olds has a profile on Hyves (*Mijn Kind Online*, 2009[3]).

Test

Test performed on 28-29 October 2009.

Summary

The SNS provides information on safety and security issues in a dedicated webpage (Hyve safely). Moreover, links are included to websites that offer more practical advice. Also the FAQ-page is in general well organized. However, the length and the inclusion of legal jargon in the Terms of Use will prevent users to read this essential information. Concerning minimum age requirements, the provider states that users younger than 16 years need parental consent to subscribe. How this requirement is assessed, stays unclear. Users are given a broad range of privacy settings that are easy to find. Yet, more awareness raising initiatives could be taken. According to the self-declaration, profiles of users younger than 16 are by default private. However, tests concluded that adults are able to find and have access to profiles of minors. Finally, users can easily report inappropriate content or conduct. An abuse report that was sent to test this service, has led to positive conclusions on the speed and the adequacy of the answer.

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 social networking site (SNS) provides tips to users on, amongst others, sharing personal information online. The provider also states that educational campaigns are run with *Mijn Kind Online* (My Child Online) on a regular basis. The SNS participates in the Safer Social Networking Task

[3] *Krabbels & Respect plz ? Hyves en Kinderen*, September 2009, http://www.mijnkindonline.nl

Force and works in close collaboration with the Dutch Police Online Task Forces. Users can contact the SNS's personnel members through the help-link available on every page.

During testing, it was observed that the SNS includes links to several sections dealing with safety, security and privacy.

In the Hyve safely (« Veilig hyven ») webpage, accessible for subscribed users and also visitors, the provider gives an overview of important safety and security hints. Handy tips are formulated in short paragraphs that address several important issues (for instance, how to choose a 'strong' password, how to protect sensitive information like phone number, e-mail, location). The provider also urges users to watch out for fake sites and to think before they post. How to report abuse and how to take screenshots as 'proof' of for instance, inappropriate comments on a user's profile, is briefly touched on. Yet, no clear overview of tips and tricks, do's and don'ts using, for instance, appealing graphs or videos are included.

Moreover, links to websites dealing with safety online are included. These links to leading organizations' websites offer users more safety tips, not only for children and teens, but also parents and teachers.

The link to the safety page is situated at the bottom of the webpage that is divided into ten sections, including a total of 29 links. Yet, the links are divided in sections that facilitate users to search for specific information (for instance, the link to the safety-page is situated under the heading « Hulp nodig? », Need help).

In the footer of the homepage a link leads to the Terms of Use (« gebruiksvoorwaarden »). However, during the test it was observed that the link was not clickable for visitors who haven't subscribed. One has to start a subscription procedure to be able to click on the link. The Terms of Use webpage outlines extensively the prohibited activities and refers to the consequences of such behaviour (like for instance the discontinuation and/or removal of the user's account temporarily or permanently, or the removal of specific content). Furthermore, users are informed on how to report unlawful content. The information needed in this report is clearly described. Yet, the Terms of Use constitute a full-fledged legal text that is not adapted to young users. What's more, this text consists of 14 paragraphs and a total of about 340 lines and 3060 words, which is not appealing for (young) users to inform themselves on their rights and obligations.

The Privacy Statement clearly informs users about the uses of disclosed personal data but also automatically generated data (like IP address, cookies etc.). The fact that advertisement is adapted to the user's profile is explained clearly (including some examples). Moreover, users are informed about their privacy rights (like for instance right of access, correction and to object to e-mail notifications of the SNS, to grant or withdraw consent to receive e-mails from partners).

A link to a FAQ-page is also inserted in each webpage's footer. The answers to frequently asked questions are categorized in several topics (for instance: general, sections, photos etc., abuse & spam,…). Users can easily contact the SNS personnel using an online form that is accessible from every page (in the footer, under the header « Need help? »).

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

According to the self-declaration, no explicit restrictions are made concerning minimum (or maximum) age for registration. Yet, persons younger than 16 years need parental permission to subscribe (cf. also Terms of Use and Privacy Statement). However, no information is given in the self-declaration nor in the website how this will be checked. Subscribers are only told that « By accepting these Terms of Use you guarantee that you are aged sixteen (16) or over or have the consent of your parents or guardian to create an account ». However, when registering users are asked to select their year of birth from a drop-down menu (reaching from 1900 till 2009). Therefore it was possible to subscribe as an 11 year-old, without further questions or remarks.

The provider states in the self-declaration that, on request, parents can have their IP address blocked to prevent their child from joining the SNS against their consent. However, no specific information for parents could be found in the site. No information is given in the self-declaration on how the uptake of parental involvement or control is promoted.

Although no information is given concerning the functionalities that are used to label, rate or restrict content, the provider states that « Alcohol related ads are not targeted to under 18 ». Moreover, no information is provided in the self-declaration on what functionalities are possibly provided for content providers, partners or users to label, rate or age restrict content.

Principle 3: Empower users through tools and technology.

The provider briefly states in the self-declaration that « No user can search for under 16s ». Moreover, the provider declares that 'new' profiles of under 16 year-olds are automatically defaulted to private.

Concerning the default privacy settings of minors, some supplementary information can give a more detailed view of the measures that are in place to protect minors' profile. Not only in the privacy settings (accessible through a drop-down menu) but also when checking the personal data through the account webpage, users can adapt the access to their personal data. By default, registered users have limited access to profile information of a minor user (picture, age, online status, first and last name, day of birth), whereas friends can have access to the e-mail address and memberships (of online groups). By default, nobody sees the messenger account, mobile phone number (and also position on Google maps). Furthermore, supplementary profile information can be added (like religion, favourite books, films, food, destinations, games, …). Users can set their profile to private and allow only those users they have proactively added to their contact list to see when they are on IM and to be able to contact them. Finally, subscribers can refuse a friendship request and add a contact to a blocklist, preventing them from seeking contact again. An easily accessible and recognizable button can be used to block a contact. Also comments on one's profile page can be deleted.

By default all users can post comments. A subscriber can restrict posting comments and also the access to comments to specific groups (for instance: nobody, only friends, friends of friends). Users can also choose which images/videos will be visible for friends, their friends or everybody. What's more, users can conceal their online status.

Concerning the protection of minors' profiles for adult subscribers, tests have been conducted. An adult user (32 year-old) could find the profile of the young SNS user (11 year-old) and send a message. Yet, the adult user could not see the profile of the minor user. However, by searching for other (nick)names

through the SNS search engine, minor users could be found. Some profiles were not accessible, while full access to profiles of some 12, 14 and 15 year-olds was possible.

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 help their youngsters.

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

In the self-declaration the provider states that users can easily report abuse. Wherever user-generated content appears, complaints can be easily filed. Also inappropriate behaviour or other types of abuse can be reported. Users are also given the possibility to provide reasons when reporting Terms of Use violations.

When assessing the report mechanism in the SNS, it was observed that users can easily report inappropriate content in several ways.

First, in the Terms of Use page a link to the online report form is included. Users are also informed about which information is needed to report abuse. In the FAQ-page, a specific section is dedicated to abuse («Misbruik, pesten & spam »). Also in the Hyve Safely-page, users are informed about this option. The form is well designed and gives the user the possibility to choose between several categories of questions or abuse reports (for instance: I am bullied on Hyves, I have found a spammer, I have found a profile with porn, …).

What's more, near the section of user generated content an easily accessible and recognizable picture (figure of a policeman) and a link (Flag as offensive, « Dit is niet OK ») are available leading to a pop-up form offering the user the possibility to select a category of abuse (bullying/stalking, spam, discrimination/racism, …) and to add comments[4]. In this online form, the provider states that when specific content is « flagged » six times, it is the automatically and temporarily made unavailable. SNS personnel will check the content and decide to delete it permanently or put it back online.

In sum, the procedure is easily accessible, understandable and age-appropriate for young users. The provider stipulates that « reports of abuse are acknowledged immediately and acted upon expediently by dedicated teams ». As part of this study an e-mail was sent (on 30/10/09) seeking assistance as the user receives « scary messages ». A message appeared on the screen confirming that the report was sent. The next day, an extensive and personal answer was sent giving concrete tips how to deal with this situation (amongst others, how to block a user). The moderator concluded by informing the user that, if the aggressive contact continues, the victim could send more information to the moderator (namely the nickname(s) of the perpetrator(s) and screenshots as proof).

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

The provider declares that the Customer Care Service handles questions and users' complaints. The provider stresses also its close collaboration with the Dutch online Police report systems.

When assessing the social networking site, it was observed that the safety-page includes hyperlinks to Dutch organisations dealing with online safety. Next to several informative websites (like for instance

[4] If the user needs more space, the provider refers to the contact form (hyperlink to the form is provided).

http://www.mijnkindonline.nl[5], http://www.internetsoa.nl, http://www.surfwijzer.nl), also a link is integrated to an online report system, part of the Inhope child abuse report system (http://helpwanted.nl/). Moreover, a link is included to the Dutch Safer Internet Centre (« Digivaardig & Digibewust » http://www.mijndigitalewereld.nl).

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

In the self-declaration the provider refers to some issues discussed under Principle 3 for more information on how measures are implemented. First of all, the provider stresses the protection of profiles of users younger than 16 years old (namely, new profiles are defaulted to private and no user can search for under 16s, cf. assessment under Principle 3). Next, the provider refers to tools to manage their profile information, block users from contacting them and conceal their online status. Finally, applications are governed by the same privacy controls available in the SNS.

When analysing the processing of personal data and the users' privacy settings, the following observations were made.

To register, a visitor has to provide first and last name, e-mail, date of birth, user name and password. Other data are optional. Although the inclusion of a mobile phone number is not compulsory, the provider encourages users to include it in the form by noticing: «Niet verplicht, wel handig! » (*Not compulsory, however handy*). This remark could stimulate youngsters to include this (sensitive) information in the online form.

A link to the Terms of Use and to the Privacy Statement is provided at the end of the online form. New subscribers have to check a box stating that they agree with the Terms of Use.

The SNS is also using a *CAPTCHA*[6] in the subscription form to prevent the use of automated systems to subscribe and engage in spam. Moreover, an e-mail verification system is used to prevent unwanted subscriptions.

By default some personal data (name, age, gender, day of birth and place of residence) are visible for all SNS subscribers. The user's e-mail address is by default only displayed to friends. Other contact details such as a phone number or a messenger account, but also place on Google maps is by default not visible for others.

A subscriber can change his/her privacy settings and restrict the access to friends, friends of friends or make personal data invisible to all users. Users can restrict or make public several personal data in their account profile. They can also easily adapt their privacy settings. A link can be found on the menu link on top of the page (« My account » and « Privacy »). In specific webpages (« Hyve safely » page and the FAQ, for instance) users are informed about how they can protect sensitive data, how to adapt their privacy settings and how to delete their account (cf. e.g. http://www.hyves.nl/index.php?l1=ut&l2=da). The deactivation of a profile is not possible. When removement of the profile took place, this is permanent.

---

[5] For instance, hints for parents are summarized in two handy reports « Mijn puber op Hyves » (for parents of + 12-year-olds) and « Mijn kind op Hyves » (for parents of 6 to 12-year-olds), cf. http://www.mijnkindonline.nl

[6] *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).

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

The provider refers to the information included in the self-declaration under Principle 2 and 5 for more information about measures that were taken.

Automated as well as human moderation is used in the SNS. For instance, the provider states that alcohol related ads are not targeted to under 18 year-olds. Furthermore, near all content a notification link is provided, to report abuse.

The provider states that the Customer Care Team handles « sensitive user issues ». Moreover « a dedicated security team … works to identify potential problems and takes immediate action when security issues occur ».

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 efforts of the provider to inform SNS subscribers about safety and security have to be underscored. In the Hyve Safely page, users are sensitized about several issues. Moreover, references are included to websites that offer practical advice to children, teens, parents and teachers. Yet, to inform and sensitize young users only textual information could be found, no tips or tricks are given using graphs or videos.

The Terms of Use and Privacy Statement are quite long. Especially the Terms of Use are not appealing for young users. In fact, the length and the inclusion of legal jargon will prevent users to take the time to read this essential information. Although the FAQ-page is in general well organized, questions concerning security, safety, etc. could be grouped. Users can easily report inappropriate content or conduct. An abuse report that was sent to test this service, has led to positive conclusions on the speed and the adequacy of the answer.

The provider states that users younger than 16 years need parental consent to subscribe. Yet, no information is provided on how compliance with this requirement is assessed.

In the self-declaration the provider refers to the specific possibilities for parents to block the access to the SNS. However, during the test no information for parents could be found on the SNS to use this option. According to the self-declaration, profiles of users younger than 16 are by default private. Yet, testing revealed that adults can find and have access to profiles of young users.

Finally, users are given a broad range of privacy settings and these options are easy to find. Still, these privacy options are not accompanied with awareness raising efforts to encourage users to make informed decisions.

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	*Not Tested*				
6		X			
7	*Not Tested*				

MICROSOFT EUROPE

Elisabeth Staksrud, University of Oslo

The testing of the services was performed October 31st and November 7th 2009 on the UK version of Xbox Live and Windows Live.

Xbox Live (information at www.xbox.com/live, the service is accessible through an xbox360 gaming console) is an online gaming and entertainment service from Microsoft.

Windows Live (http://www.windowslive.co.uk/index.aspx) is a service integrating a wide range of tools and applications such as e-mail, photo management, sharing of files, communicating with others through instant messaging services (MSN/messenger) etc. According to the "member qualifications" in the Codes of Conduct "the services are designed for individuals 13 years of age or older".

It should be noted that as the self-declaration specifically mention these two services, the testing has been done with the aim to find information on the sites/service itself, or directly linked from the service rather than explore the overall company website (www.microsoft.com), as this is perceived to be the normal form of use of the services.

As the Xbox Live service requires credit card information to allow underage users (below 18) signing up, only adult testing profiles have been used-Similarly, since the reporting mechanism would have to involve real players, stage two of the reporting (delivery and receipt) has not been tested.

Summary of findings:

Windows LIVE:

- Safety information is limited for users who have not signed up
- There is a strong focus on technical parental control and surveillance on the site itself. General safety information and tips for children are found on the Microsoft general site, not on the service, and is complicated to reach from the Microsoft Live site.
- Some of the safety related links provide circular references, sending you back to the site you started from. It is difficult to find information on specific risks and other resources/organizations
- Parental tools are easy to find
- A wide range of privacy tools and settings are provided
- Report mechanisms are provided and almost always visible. The reporting form is a complicated for children and is closed in the sense that you can only send notification on pre-defined issues and concerns.

Xbox LIVE:

During the testing no information on Terms of Service were found to be available until during signup, and thereafter not within the service at all.[7] This applies to all information on the service; none of it is available in the service, only on external websites. It should be noted that the information in these external sites is

[7] After then test was conducted Microsoft informed that The Terms of Use is available at any time from the Dashboard. Users need to click the large X button on the center of the controller to open the Dashboard on the console, then choose Settings, then Account Management and then Policy Info and then the Terms of Use.

comprehensive and available at e.g. www.xbox.com/en-GB/playsmart but it is, as mentioned, not accessible from the Xbox Live service. This external information is therefore not tested.

- Settings for parental control/"Family settings" are built into the console's software and easily accessible
- Available tools are easy to use and find
- The signup process requires that underage users trying to sign up with their real birth date must get help from an adult who provides credit card details for age verification
- User control over the profile's privacy settings is extensive, defaults for underage profiles are set to hide/private/friends only
- User profiles contain little to no personal information, without the user specifically putting it in
- The reporting mechanism is slightly convoluted

Testing results:

Principle 1 "Raise Awareness"

In the Self-Declaration:

Relating to both the **Windows Live** and **Xbox Live** services, the self-declaration includes information on terms of use, privacy (stating that the general company policy is accessible from every page of each major online service they operate).

The provider does include information on safety in their self-declaration, but by referring to other sites within Microsoft or cooperating partners, not specifically on the Windows or Xbox Live services themselves. Similarly, safety information is stated to be targeted towards specific user groups, but with a referral to the general company site, not the service. The information is not explicitly said to be easy to understand nor presented in a prominent way, but is said to be accessible and practical stating that it "seamlessly integrates family safety options for Windows live services", mentioning specifically to include information on links to educational material and technical controls for parents. The self-declaration does not state that specific advice is given to teachers on the SNS website, but it does list cooperating organizations that do and emphasizes the importance of safety information and education in schools.

It is stated that the safety information provides guidance regarding inappropriate content and conduct and information on the consequences of breaching the Terms of Service, but with without any reference to safety services in particular, but rather referral to the very existence of the terms of service.

On the site:

In the **Windows Live** service both the Terms of service and the Privacy Policy are very easily found on the site, as are safety tips/information for parents. The terms of service clearly listed content and conduct that were not allowed, as well as the consequences of engagement in prohibited behavior. The Terms of service also states that the services are intended for users "13 years of age or older". This is not emphasized in the self declaration report. This does not apply to **Xbox Live**, where the Terms of Service is displayed once during signup, whereupon neither the Terms of Service, nor safety tips for parents could be found on the service itself during the testing.

The **Windows Live** information provided for parents was found to be easy to access but extremely limited as it gave only a few not self-explanatory screenshots along with brief textual information referring to the need to download the tool in itself in order to receive further information

The Code of conduct could not be found at the first stage of the test at all. (However, this was discovered at a later stage of the test, when searching for "pornography" under the "live help" section.)

Any parent, teacher or potential user wanting to obtain information regarding Internet safety will not be able to access this information directly from the www.windowslive.com site, nor through Xbox Live. A Windows Live link to "family safety" is provided on the first page of the service, but when clicking on the link you are redirected to a site where you need to sign up in order to get more safety information. When clicking the "learn more" button on "Windows Live Family Safety" http://windowslive.com/Desktop/FamilySafety one gets more info on how to sign up to various services (messenger) not more safety information.

Safety information directed towards children or teachers could not be found when not signed in as a user, nor links to educational material or and if the organizations active in child safety that was listed in the self-declaration report. When searching for such partners/organizations, after clicking "explore" on the site, once comes to a new site with information also listing "partners". Clicking on this link only made the same site reload.

Information on specific risks are not found on the Windows Live website, nor in Xbox Live, with the exception that information on bullying was found after going to the Windows Live privacy policy, then clicking "safety resources" where one was re-directed to www.microsoft.com and then from there go to resources and download a folder. When going on the Microsoft online safety site (www.microsoft.com/protect/family) some information regarding specific risks can be found. In an attempt to find information on specific risks, the search engine provided at the safety site were used. Searching for information on specific harms on the Safety Site using terms such as pornography or violence gave no results at all.

Principle 2"Ensuring Age Appropriate Services"

In the Self-Declaration:

The self-declaration outlines how it is made clear to users when services are not appropriate for children and young people, most importantly by the existence of filtering services. The declaration states that "generally speaking, Microsoft services with social networking capabilities are general audience services and do not target particular age groups". Hence, no specific steps to deny access to e.g. under aged users or refusal of attempts to re-register with a different age are relevant to these services. However, extensive parental tools are implemented, including limitation of inappropriate content and control over who can communicate with the child. For the gaming service Xbox Live, the declaration states that adherence to content rating systems is implemented. This is tied to the console's "Family Settings", where parents can limit access to games based on their rating(s).

On the site:

When signing up to the Windows Live site, no age verification is needed; however, the service requires you to list your year of birth (but not the date). The testing profile of 11 years was therefore successfully used for the remaining relevant parts of the test. It should be noted that this was under the recommended age for the site (above 13 years). For the Xbox Live service, although not mentioned in the self-declaration, a birth

date is requested, and parents' consent, verified by entering credit card details, for users under 18. This being a requirement meant that finalizing the signup process for underage users was not done.

When signed in to Windows Live parental control tools can easily be found, give sufficient information and allows for monitoring the child's activity, provided that the parent is also a registered user. This also applies to Xbox Live, where control tools are built into the console's software. Similarly, profile settings are easily found.

Principle 3 "Empower users through tools and technology"

In the Self-Declaration: The provider does indicate in the self-declaration that on Windows Live:

- the private profiles of users registered as under the age of 18 are not searchable on the service or via search engines
- full profiles are set to 'private' by default or to the user's approved contact list for those registering under the age of 18
- users have control over who can access their full profile by, for e.g., being able to block friends or 'reject' friend requests
- users have the option to allow only direct friends to post comments and content to their profiles
- users have the option to specify who can post and view comments from other users
- it provides easy-to-use tools for users to report inappropriate contact from another user
- it provides easy-to-use tools for users to report inappropriate conduct by another user
- it educates parents about available tools, both for wider internet access and the tools, information and advice provided to parents by SNS to help them protect young people

The self-declaration does *not* indicate:

- that users have the option to delete unwanted comments of other users
- how users can delete their profiles

For Xbox Live, the declaration says:

- the default settings for profiles are 'blocked' for the under 13s, and 'friends only' for those between 13 and 18
- Users can share profile with friends only, or block all access to profile
- users can complain about other users content or behavior
- Microsoft provides awareness-raising web sites

Not in the self-declaration:

- information on how to delete profiles

Since there is no system provision for posting comments on other user's profiles, related issues are not reported on in the self-declaration

On Windows Live:

It is easy to find information on how to report abuse or bullying, how to block other users from contacting you. Information on the possibility to specify who or which groups of users that could contact you (except form already confirmed "friends) was not found. After signing up information on restrictions of search options for profiles were found easily.

When signed into the profile it was not clear how much or if at all the user's personal information was visible to all other users, nor if the online status (if one is logged on or not) could be seen by others. But one has to explicitly change settings in order to make all personal information visible to other users.

Other users, or just friends, can post comments on the profile, but this requires that the user changes the settings to allow for publication of friends (private) or all users (public). No special warnings/tips or guidance where given regarding personal information when profile picture and personal information was uploaded. However, when re-signing into the site a general message appeared on the profile encouraging the user to learn more about privacy setting, options and managing permissions.

Information on how (or if at all possible) to delete/remove pictures and postings on other peoples profile was not found. However, one can revoke a general permission for anyone to tag you in a picture uploaded by others.

When wanting to delete the profile, information was not found on the profile site, and no information was given when searching for "delete profile" under the help section. After considerable searching some information was found under the "account" section. The information provided here was clear, and stated that one could deactivate ones profile, but not delete it completely as some information would be stored. The provided did give sufficient information regarding what personal information that would be retained/collected after the profile was deleted and how this might be used.

Finally, when signing out as a child and then logging onto a adult profile, the testing profile of an 11 –year old girl automatically came up as a friend suggestion for the adult profile, without having any common friends (or friends of friends). Here also information on the child profiles location, name and interests became available.[8]

One was able to find profiles of other 11-year olds when using the Windows Live search engine fairly easily by searching on e.g. "born in 1998".

On Xbox Live:

No information on how to report abuse or bullying could be found on the Xbox Live system. How to block others contact is easily found, as is the blocking mechanism itself.

Pictures you may have entered into your profile are easily removed.

As an above-18 user, the profile is by default accessible to all. Changing this is easy, as is the control over the profile's online status visibility. Safety tips are displayed when the profile is (attempted to be) updated.

No information on how to delete the profile could be found, nor could any information on what happens with the profile or its contents in case of a deletion. To get information on this one has to access an external website.

---

[8] After the test was performed Microsoft informs: "Without knowing if the default permissions were changed for the testing profile, or the permission setting on other user profiles, we'd assume the minor may have always had their birthdate correct representing themselves as 11. In addition, all minors across regions initially get default settings to My Network (…). However only Family Safety Settings (FSS) under 18 accounts are actively prevented from opening up those permissions to Public. Similarly, the account this minor is using may have been created with an adult birthdate initially, but then the birthdate was changed to that of a minor. Adult defaults are broader than those given to minors, and these are not reset if the birthdate changes". The tester notes: during the testing the permission settings were not changed (unless to restrict more) during testing, and the account was created initially for the child.

Principle 4"Provide easy-to-use mechanisms to report violations"

In the Self-Declaration:

All of Microsoft's online services are said to have a mechanism for reporting inappropriate content and/or contact. Generally, the mechanism is said to be easily accessible and understandable to all users, and that reports are acted upon quickly. The declaration does not indicated that the reporting procedure is age appropriate or that reports are acknowledged, or that the users are given indications on how such reports are typically handled. In addition, for the Xbox Live service, specific reporting mechanisms are said to be in place. No information is provided on their accessibility.

On the site:

When signed into the Windows LIVE profile, a link for reporting abuse or content that is violations of terms are visible on what is perceived to be the relevant sites, but is not visible all the time (e.g. could not be found when signed into the "account" and "home" sections of the profile), in contrast to the statement in the self-declaration: "*a 'report abuse' button appears at the bottom of every windows live social networking service window*".[9]

The button is easy to find, but is not considered easy to understand, especially for children, as the form to fill out is very technical. The form also does not allow for general safety enquiries, just report of specific incidents, as a URL to the specific incident must be provided and one cannot submit the form without filling out all the sections. Also a readymade list is provided for what type of incident one is reporting, not allowing for a potential "other" request or concern.

It took just under 24 hours to get feedback on the report sent asking for help. The reply from the Windows Live support team asked for more information regarding the specific incident, such as a clear description of the violation, profile or space name and a copy of the offensive message in order for it to be investigated further. No general information on safety issues or referral to other organizations that might help was given.

In Xbox Live, reporting violations is on a per-user basis, specifically during play or after receiving messages. The process involves pausing play and calling up the player list, thus requiring basic skills in using the Xbox system. For reasons described in the introduction, the reporting process was not fully tested in Xbox Live.

Blocking friends and/or requests is easy.

Principle 5 "Respond to notifications of illegal content or conduct"

In the Self-Declaration:

Microsoft states that for all their online properties they have robust, easy mechanisms for reporting abuse, and that they respond quickly to reports of abuse, including those involving potentially illegal content or behavior. This includes cooperation with law enforcement and government agencies. No information was provided regarding cooperation with other services such as Inhope.

---

[9] After the test was conducted Microsoft clarified that report abuse mechanism is requried ONLY on pages where user generated content is visible to the public (i.e. to others besides the poster of the content).

On the site:

The reporting mechanism was not tested for illegal content or contact. No information could be found regarding organizations such as Inhope on Windows LIVE or the general Microsoft Family Safety site.

The reporting mechanism in Xbox Live was not fully tested due to reasons described above. The initial procedure was however, easy to understand, once one could find the mechanism itself.

Principle 6 "Encourage users to safe use of personal info and privacy"

In the Self-Declaration:

According to the self declaration a range of privacy setting options are provided for users

- When users visit their profile, they see their own view of the profile, which always includes all of the information they have entered about themselves and a list of all of their activities
- the implications of automatically uploaded information provided during registration onto profiles have been considered
- users are notified when the information used to register is automatically uploaded onto their profile
- when information is automatically uploaded to profile users are able to edit and make public/private that information where appropriate
- indicate that privacy options are supported by information that encourage users to make informed decisions about the information they post online

The self declaration does not:

- address the issue of third party applications

On the site:

On Windows LIVE one can easily change one's privacy settings. Registering for the service one was asked to provide a wide range of personal information. Information like first and last name, year of birth, postal code and similar were required to register. All privacy settings can be changed once logged in. When searching for the testing profile of 11 years from the testing profile of an adult, information like name, picture, where one lived and interests came up with no restrictions.

Similarly, changing your privacy settings in Xbox Live is easy. Only date of birth and e-mail address is required. No statement is given as to whether these are inserted into the profile, they are however not visible. The self-declaration states that "Other than the username selected for the Windows Live ID, the pieces of information in a profile remain separate, with no automatic mapping taking place". This seems to be accurate.

A wide range of information could be registered/entered when logged onto the profiles, such as relationship status, hobbies, sense of humor, taste in music/films/movies etc. In Xbox Live, this is in the form of free text, and is not searchable.

No information was found on third party applications (nor was this addressed in the self-declaration report).

When trying to change settings for permissions in Windows Live, e.g. clicking the "permissions" under the blog post option under "invitations and communications preferences" column on the "permissions" site, only send you back to your own profile, giving a circular reference.

Principle 7 "means for reviewing illegal or prohibited content/conduct"

In the self-declaration it is generally declared (including both Windows LIVE and Xbox Live) that Microsoft employs human and automated forms of moderation, in addition to user generated reports. No details as to the type of technical tools are provided.

No information is provided regarding community alerts. No information is provided that steps are taken to minimize risk of employing candidates unsuitable to work with real-time contact with children for human moderators.- please see the other remarks sent via email

This principle was not tested on the services.

Conclusion

For Windows Live:

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	*Not Tested*				
6		x			
7	*Not Tested*				

For Xbox Live:

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	*Not Tested*				
6	x				
7	*Not Tested*				

MySpace

Bojana Lobe, University of Ljubljana

Introduction

MySpace.com is a social networking platform that allows users to create unique personal profiles online in order to find and communicate with old and new friends. The minimum age requirement to become a member is 13. The services offered by MySpace include any MySpace-branded URL (the "MySpace Website"), MySpace messaging services (including, without limitation, instant messaging, private messaging, and email services), MySpace music and video services, MySpace developer services, MySpace mobile services, and any other features, content, or applications offered from time to time by MySpace in connection with MySpace's business (collectively, the "MySpace Services").

The following is a report based on the testing of social networking service MySpace. It was tested at the main British English site (uk.MySpace.com).

Summary of findings:

- Safety information is available to all, also those not signed up.
- The safety information is extensive, targeted specifically to teens, parents, teachers and general users.
- Parental control tools are extensive and easy to understand.
- Report mechanisms are efficient and visible at all times.
- Users are provided with various tools to control their privacy settings.
- Minors are not searchable through search engines.
- A number of effective processes are in place to expeditiously review and remove offending content upon receipt of notification of alleged illegal content or conduct

Testing results:

Principle 1 "Raise Awareness"

In the Self-Declaration:

The self-declaration (even though under Principle 2) includes information on Terms of use. It also includes safety information.

The provider also indicates that the safety information is targeted. Amongst other, the provider states that users under 18 receive security warnings before posting content, users under 18 must review Safety tips before registering, they mention parental safety tips and MySpace Parent Brochure as well as School Administrator's Guide to Understand MySpace and Social networking Sites. Further, the provider has run

education campaign through MySpace and also through third party partners, such as National School Board Association, and are steering group member of Teach Today initiative.

The provider also states that there is a "safety tips" link on every page (that makes is accessible), which includes links to parent monitoring and blocking software. However, the provider does not specify whether the safety information is presented in a prominent way and a practical format nor whether it is easy understandable.

Also, the self-declaration does not state that the safety information provides guidance regarding inappropriate content and conduct and information on the consequences of breaching the Terms of Service.

On the site:

In **MySpace** both the Terms of use, Safety Policy and Privacy Policy are very easily found on the site. Safety Policy and Privacy Policy are visible when entering the site (at the bottom). It is also easy to find the Safety Policy and safety tips/information for children, parents and teachers as well as links to educational material or organizations active in child safety. Safety tips/information to parents, teachers and children is very easy to understand and to access. It is also very exhaustive. For example, the safety information for teens contains the instructions on how to use safety settings, safety tips, information on cyberbullying, links to get more information to help you stay safer online specifically targeted at teens and information on how to contact MySpace. The information for parents and educators includes the above information as well as the information on how to create and delete the account, how to talk to teens about Safer Internet Use and some basic information on MySpace.

The provided information is in textual and in audio/video format. It also provides concrete and anecdotic examples of use (e.g. why it is not smart to publish anything that can embarrass a teen later, why it is not wise they are older as they are etc.).

Beside specifically targeted information to the core three groups, MySpace also provides many external links to organizations that are working toward increasing awareness of Internet safety and teen health as well as links to Internet safety Experts (such as Wired Safety. Safe Kids, Safe Family etc.). All this information, together with ParentCare software (which was developed by MySpace itself) and some additional links to external software downloads s provided in the category "more resources".

The Terms of use clearly list content and conduct that are not allowed, as well as the consequences of engagement in prohibited behavior are listed. The minimum age required is \mentioned in terms of Use ad well as in the safety tips for teens.

In general, information on the following specific risks is found: hate speech, violence, bullying and divulging personal information. Even though the risks of seeing of being the subject of child abuse images or posting sexually provocative photographs are not explicitly mentioned on the site, they keep warning teens in the safety tips not to put photos that can embarrass them or expose to danger.

Principle 2"Ensuring Age Appropriate Services"

In the Self-Declaration:

The self-declaration provides information on how it is made clear to users where a minimum age applies (stated in their Terms of Use), it also outlines the steps taken to delete under-aged users (they employ search algorithm currently to seek and delete individuals misrepresenting their age and actively search out

underage users by hand) or to deny access and to prevent under-aged users to attempt and re-registering with a different account (the use of session cookies).

Further, the provider states they work closely with commercial content providers to ensure the users have information about the content to make informed choices. These might come in the form of warning messages, restricting content based on time of day. The provider also mentions application security steps they adopted and a number of steps taken to protect younger users from inappropriate content. Further, the provider mentions that inappropriate URLs are blocked and not being posted on the site. However, the self-declaration does not outline how it is made clear to users when services are not appropriate for children and young people.

The provider does also address in the self-declaration how uptake of parental controls is promoted on the service. They developed a software, ParentCare Beta, which is a free, simple software tool designed to help parents safeguard their teens. With ParentCare Beta, parents can determine if their teen has aMySpace profile and validate the age, user name, and location listed by the teen.

Also, they state there are safety tips link on every page, which include links to parent monitoring and blocking software.

On the site:

When signing up to the My Space, no age verification is needed, meaning one does not have to explicitly state (or tick a statement) that the user signing up is above a certain age. The service requires one to provide their full birth date. Also, email verification is needed. The attempt to sign up as a 11-years old failed as the users below 13 are considered under aged. The provider installs a cookie on the computer of the user to prevent them from trying to sign up with a different age. However, once the cookie was removed, the sign up as a 15-years old was successful.

On MySpace, the links to various parental control tools can be found. The software Parent Care can be downloaded from the site, and several FAQs are provided on how to install and handle the software as well as how to lock or delete the teens account. This makes the software easy to understand. The available parent control tools are considered efficient.

Principle 3 "Empower users through tools and technology"

In the Self-Declaration:

The provider lists a number of steps taken to protect younger users from inappropriate contact. Amongst many others, these can also be found:

- New profiles for under 18 are automatically set to private;
- No user can browse for under 16s;
- Adults can never add under 16s as a friend unless they know their name or email address;
- If under 16s override their privacy settings they are still only viewable by other under 18s;
- Under 18s can block all over 18s from contacting them or viewing their profiles;
- Under 16s are tagged to be un-searchable by age in search engines;
- Over 18 are limited to their ability to search in the School section.

The provider further lists a number of tools provided to all members. Amongst many others, they also state that all users can set their profiles to private and can pre-approve all comments before being posted. Users also have the chance to conceal their online status.

The provider does not mention how it educates parents about available tools.

The provider does not state whether the users have the option to allow only direct friends to post comments and content to their profiles or whether they have the option to delete unwanted comments of other users. But as mentioned above, the users have a chance to pre-approve which inherently include the possibility to delete even though the provider does not state that explicitly.

The provider also states that it provides tools to report inappropriate content or behaviour (more in Principle 4 as it is stated there).

On the site

The information on how to report abuse or bullying, how to block other users from contacting you, the information on the possibility to specify who or which groups of users that could contact you can easily be found on the site. However, the information on restrictions on search options for profiles was not found.

Once signed into the profile, the user is able to delete/remove posting and photos on their profile as well as those they put on other profiles.

Other users cannot post comments on the profile as only users' friends have this possibility, if the user account is set to private. Personal information (the one user decides to share) is visible to other users by default and one has to change privacy settings to make it only visible to friends. For under 18s the settings are set as default to private (which means friends only). Further, if under 16s decide to override their default privacy settings they are still only viewable by others under 18. In the safety tips for teens, the provider recommends and offers clear steps on how to set the profile visible to only friends.

The user also has the possibility between choosing online, hidden, or offline status when signed into MySpace. One can also decide to whom one wants to be available for IM (e.g. to only MySpace contacts or all under 18 etc.). The user is also notified when tagged in a photo by friends but does not have a chance to approve the photo before being published. One can remove a tag later.

Safety tips and/or guidance about publishing personal information or a photo on the profile is also provided every time the user wants to edit their profile. Also, when signing in, one gets the info about safety tips before posting any personal information of a photo. Also, on the photo upload page there is a link to the photo policy, which among other things it states: For security and privacy reasons, any image that contains personally identifiable information such as name, phone number, email address or web site URL is not permitted.

In case of attempt to cancel the profile, information can be found in the Privacy Policy page. There is also a clear link provided in the account-setting page that enables account cancelation. When cancelling the account, the user is asked for a reason as MySpace claims to collect this information in order to improve their service. The profile can be permanently deleted. The provider does not state any information about what personal information is collected/retained after cancelation of the account or how it is used.

The underage users can search for users their own age (16 and below) and are not searchable through search engines.

Principle 4"Provide easy-to-use mechanisms to report violations"

In the Self-Declaration:

The provider states in the self-declaration, that a report abuse procedure can be accessed from every MySpace webpage and whenever user generated content appears. Users can also report:

- Inappropriate content or behavior to MySpace;
- Spam email complaints to MySpace;
- Sexually explicit conduct directly to NCMEC's CyberTipLine;

The provider further states that the reports of abuse are acknowledged immediately and acted upon expediently by dedicated teams.

However, it does not say whether the mechanism is understandable to all users and age appropriate. The self-declaration does not indicate that the users are given indications on how such reports are typically handled.

On the site:

When signed into MySpace account, a link for reporting other users is visible at all times (at the bottom of the page of other users as well as friends). A clear link on the user page is provided to report abuse or block friends or any other users. The information on how to report a friend is found in "using safety settings' section. Also, one can decline a contact's request.

The link/tool where one can report abuse/violation of terms is also visible at all times. However, one can report photos or videos but not comments. The button to report photos or videos is easily found below them. The report mechanisms are in general easy to understand.

When the report is sent, one immediately receives the message: "MySpace Customer Care will review the reported content against our Terms of Use for violations and take any necessary action."

To report a user, a test was done. On Myspace, one can report a person, a photo, etc., but there is no general button for report in which one could include the general "Someone is sending me scary messages" report or at least it has not been found. To avoid falsely accusing a real person that is sending a scary message (not just someone, as planned in methodology), one of the profiles created for this exercise was reported for being underage (the reported profile was the underage profile used for registering to MySpace first as an 11-year-old and, when access was denied, as older). [10] A notification about the actions taken as a result of the report has been received within one day on the email address of the user but not in the inbox of the Myspace profile of the user. [11]

[10] The message from methodology was also sent at a later stage to report a grown up sending scary messages and there has also been the same response from the provider as in the first instance.

[11] Due to this, the reply did not reach the tester, but after consulting with the SNS it is clear that a reply was sent and was later found by the tester.

Principle 5 "Respond to notifications of illegal content or conduct"

In the Self-Declaration:

The provider states a number of effective processes are in place to expeditiously review and remove offending content upon receipt of notification of alleged illegal content or conduct:

- The Customer Care Team handles sensitive issues;
- The Content Assurance Team ensures integrity of safety systems and flags potential issues;
- The Security Incident Response Team has a dedicated security team that works to identify potential problems and takes immediate action when security issues occur;

The provider further lists arrangements in place to share reports of illegal content or conduct with the relevant law enforcement bodies and/or hotlines:

- The Parent Care Team provides a dedicated parent hotline;
- The School Care Team provides a dedicated educator hotline;
- The Law Enforcement Team provides a 24/7 dedicated hotline;
- They have established working procedures with NCMEC;
- They provide ongoing support to local, state, federal and international law enforcement;
- The Law Enforcement Guide and One Sheet have been created to help law enforcement
- Agencies understand MySpace and investigate cases.

On the site:

The reporting mechanism was not tested for illegal content or contact.

Principle 6 "Encourage users to safe use of personal info and privacy"

In the Self-Declaration:

Regarding encouraging users to employ a safe approach to personal information and privacy, the provider refers to Principle 3 where there is an extensive list of what user can do (please see the Principle 3 section in this report).

In the Principle 3 the provider also addresses Application Information and data collection, where amongst other things it states that all applications are governed by the same privacy controls that are in place for members. MySpace is also stated to take actions against the applications that violate safety and security requirements.

On the site:

On the site one can easily change one's privacy settings. At the registration, the user is asked to provide age, email, gender and real first and last name. Optional, user is asked to provide school or workplace information and a photo. A range of other information can be provided once registered by the user if wished so (political views, religion, relationship status, interests etc.). However user is notified with privacy warning before sharing any additional personal information on the profile.

From the provided information at the registration, the age, real name, and gender are automatically inserted into the profile. If user provided a country information at registration, that will also be inserted. Other information is inserted once the user provides it (if decides so). It is also clearly stated when a user signs up "your first and last name will be displayed publicly. One can hide one's real name after one sign up by clicking my account

Also, applications (3rd party, external or additional programs and/or services) need permission from the users to be installed and/or pull info from user's profile.

Principle 7 "Assess means for reviewing illegal or prohibited content/conduct"

In the Self-Declaration:

The provider refers to " Protecting Younger Users from inappropriate Content" and " Dedicated MySpace teams" in Principles 2 and Principle 5.

In " Protecting Younger Users from inappropriate Content" the provider also lists:

- All hosted images and videos are reviewed for compliance with Terms of Use, these images are
- then hashed to ensure they cannot be reuploaded.
- Inappropriate URLs are blocked from being posted on the site.
- User accounts are deleted for uploading pornographic videos.
- Alcohol related ads are not targeted to under 18s.
- Smoking/Drinking preferences are blocked for under 18's.
- Groups and classifieds are reviewed when inappropriate content is suspected.
- MySpace works closely with commercial content providers to ensure that users have the
- information necessary to make informed choices regarding content. This may come in a variety
- of forms for example, warning messages, restricting content based on time of day etc.

In " Dedicated MySpace teams" the provider also lists:

- The Customer Care Team handles sensitive issues;
- The Content Assurance Team ensures integrity of safety systems and flags potential issues;
- The Security Incident Response Team has a dedicated security team that works to identify
- potential problems and takes immediate action when security issues occur;
- The Parent Care Team provides a dedicated parent hotline;
- The School Care Team provides a dedicated educator hotline;
- The Law Enforcement Team provides a 24/7 dedicated hotline;

On the site: This principle is not tested on the site.

Summary of results

A. 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				

B. 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			*Not Tested*		
6	x				
7			*Not Tested*		

NASZA-KLASA.PL

Barbara Giza, Warsaw School of Social Sciences and Humanities

Nasza-klasa.pl (Our-class.pl) is a social networking site gathering Internet users who want to find their classmates form every level of education. It's aim is to enable and rebuild contacts with colleagues, from kindergarten to high school or college. It has been operating since November 11th 2006 and was created by four students. It's one of the most important and the biggest social networking services in Poland now with more than 20 milion profiles on it's website. As said in the self-declaration: "Nasza-klasa.pl offers many social features which help people "stay in touch". Users can create their own profiles, join school and class profiles, gather their friends, send internal messages, upload photos, leave comments on profiles and under photos and chat with friends via the forum".

The test was being done since October 28th till 30th by using two nicknames: Maria Kowalska aged 11 and Maria Nowakowska, aged 15. There's no minimum age to use the SNS in a Terms of Use.

The service is only three years old but it is very popular in Poland. Comparing to the self-declaration, it's still in process "of building" the area of safety for users under 18. It's not necessary for person under 18 to have any permission from any adult (e.i. parent) to set a profile on nasza-klasa.pl. It's not even asked on the website to give any contact e-mail to adult when setting the profile.

It's also necessary to accept the Terms of Use, of which some are for sure difficult to understand for children. In turn, they are repeated in some important places of the service, on the website and for example when publishing photos, with the information that obscene photos, which violate manners and morals will be removed from the gallery.

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

One can say that the provider create very clear or clear information about terms of use, safety policy, policy information and information for children and parents. It was difficult to find the information excusively for teachers, but there are links to organizations active in child safety. That information is placed on the website and easy to understand for parents, and for children and teenagers. This information is provided as general textual and video info, as concrete examples. There are also external links to professional safety organizations. The Terms of Use list content and behaviour which is forbidden and consequences of engagement in them, but it's not very easy to understand for children and young people.

Instead, there is a clear information on the website (not in Terms of Use) about specific risks regarding using online services, like hate speech, violence, bullying, no information was found about self-harm actions.

Principle 2, "Work towards ensuring that services are age – appropriate for the intended audience"

- it's necessary to say that the Use of Terms clearly state that a person under 18 must have adult permission to use nasza-klasa.pl. There's no other info provided in self – declaration about this. There was no problem to set up the profile as a 15 years old girl, because the provider does not ask for any adult's permission and does not delete persons under-age. The service allowed to sign up as 11 and 15 years old because it is not age restricted.

It was easy to find the information for parents on the SNS site about the problem of safety, how to contact the police, how to look for help in case of any danger.

When signing up as an adult the SNS requires to submit birthday data and e-mail for verification – it's impossible to sign up without clicking on a verification link sent over the e-mail.

Principle 3: "Empower users through tools and technology".

In self –declaration provider informs that children and young people are assisted in their experience on their service: they are provided with necessary tools which let them control relations they make through the service: they can hide their profiles and make them invisible for search engines, they can reject friends request, put unwanted guests an the "black list" (block them), remove unnecessary comments, quickly report photos that violate the Terms of Use. It's also possible to find the information on the social networking site on how to report abuse or bullying, how to block other users from contacting me and to specify who or which groups of users can contact me.

When using one's profile it's possible to delete or remove some postings and photos on the profile, and on other people's profiles, but it's necessary to have their permission. Not everyone can post comments on one's profile (only the friends).

When signed to the user profile: the personal information is not visible for all other users, but only to my friends, to change this it's necessary to change settings on one's personal information.

When about to upload a photo on my profile one gets safety tips about publishing photo, nothing when publish information.

It's not known (or it does not say) if you're notified when you're identified in pictures posted on other peoples' profiles when signed to my user profile.

It's easy to find information on how to delete or deactivate my profile, but it's not known (or it does not say) if possible to deactivate one's profile or delete it and there's no information what's going on with my personal information the sns collects after deleting or deactivating. The tester was told that the user is supposed to contact the Customer Service, but such information was not found for users on the site itself.

Principle 4: "Provide easy – to – use mechanisms to report conduct or content that violates the terms of service".

In self – declaration the provider indicate the information about Customer – service, working 24 hour per 7 days to resolve problems and abuses reported by users. There's no information on how that reports are ackowledged, are acted upon expeditiously. It also informs in self-declaration that the service co – operates closely with lawyers and police officers to develop their skills in legal matters.

When signed to profile, one can easily find information on where to report other users that bothers me, how to report bothering content, how to block a friend/ contact request and a link where to report abuse/violation of terms visible at all times when signed into the SNS. When one is signed into profile, can block a friend and decline a contact request.

There was information sent to the SNS asking for help because of being sent a "scary messages". The system immediately sent a notification to user when a report has been sent and how a report will be handled. After sending an e-mail with the sentence about "scary messages" as Maria Nowakowska, aged 15, one gets the answer that the message was received and it usually does not take more than 48 hours for the reaction. The message was sent on October 30th and the sns claims to have sent the response on November 3rd but it hasn't been received.

Principle 5: "Responding to notifications of illegal content or conduct",

is well described, easy to find (less than 15 seconds) and easy understand for children and young people.

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

is also well described in the self – declaration of the provider, which informs that there's a Privacy Policy of the service describing what data is collected, why and how it's collected and where and when users can manage it and that there are three main privacy settings: open profile, private profile and close profile with a possibility to customize individual privacy settings.

When signed to profile, one can easily change privacy settings. When registering to the sns one's asked to provide: real name (first and last) age and e-mail, without any other questions. Into profile there was automatically inserted real name, the age is hidden for people under 18. The adults can decide whether they want or not to insert their age.

When signed as an adult one can search for other profiles where one test as an 11/15 years old and is able to search for users profiles that are 16 years old or younger, but only when the name or nickname and place of living are known. When use search engine and search the nicknames one's able to find the profiles that he/she was registered as a minor in the SNS.

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

is well described in the self-declaration too. Nasza-klasa.pl is supposed to use human and automate forms of moderation, utilize technical tools such as filters to catch illegal comments, data and subtitles and employ user-generated reports which are made thanks to special buttons such a "report abuse".

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			Not Tested		
6		X			
7			Not Tested		

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 owner[12]. Although minors cannot choose to make their profile accessible to *everyone*, 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*[13]. 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

[12] 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).

[13] 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.

« 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 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 CAPTCHA[14]). 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.

[14] *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).

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 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	*Not Tested*				
6	X				
7	*Not Tested*				

ONE.LT

Rytis Rainys, Communications Regulatory Authority of the Republic of Lithuania

Introduction for the assessment

ONE.LT is a social networking site serving over one million internet users in Lithuania as well as a sizeable Lithuanian speaking internet user audience in other countries. It is the best known SNS among users under 18 years of age. ONE.LT offers a variety of social features helping people express themselves and stay in touch with their real-life and virtual friends. ONE.LT enables users to create and accessorize online profiles, establish friend connections with other users on the site, exchange private in-site messages, upload and showcase photos, post notes to forums attached to individual user profiles and user groups, rate user photos, join public online clubs dedicated to specific themes or topics, send virtual gifts to friends and participate in other online communication activities of similar nature. The possibility to use ONE.LT services exists only for the users over 14 years of age.

The test of ONE.LT that was performed on October 29th-30th, 2009. Observed that ONE.LT has various organizational and technical tools implemented that contribute to the privacy and safety of the users. Nevertheless, mismatches to the ONE.LT self-declaration pointing the areas where SNS service could be significantly improved were found as well.

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 signed by ONE.LT, SNS maintains a dedicated site section titled "Your Safety", accessible from every page of the site, providing practical instructions and advice to users on ensuring their safety online. During the test web site "Your Safety" was found and investigated. The web site is divided into separate parts where dedicated information is presented differently for children and parents. Basic information concerning personal data safety, privacy, reporting places, threats on Internet and advice how to safeguard is provided. It was observed that the web site is lacking information related for teachers and advice on protection and parental control tools. There is not clearly distinguished which information or parts of the content provided for children and which provided for teenagers.

In the self-declaration SNS provides that "Terms of use" are clearly defined and accessible. During the test "Terms of use" description was easy to find and access. It was found that text could be difficult to understand for children and young people.

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

In the self-declaration of ONE.LT is clearly stated that only users 14 years of age or above can register on the site. The test showed, that apart from the front page (login screen), no section of the site can be viewed by an unregistered user regardless of his/her age. When testing SNS, it was found that Terms of Use document provided in web site was also has restriction for service for users below 14 years of age. During the test, three users of age 11, 15 and 33 were successfully registered with detailed profiles. All three users were able to search and make connections with each other, including 33 years user contact to 11 years old child.

During the test it was observed that users are asked to use valid mobile phone number at account registration stage. By SNS self-declaration, it should limit the ability of young users to create multiple profiles and could make parental control easier. In practice it's not fully effective measure because of pre-paid mobile cards usage.

In a self-declaration of ONE.LT is mentioned that SNS has an image review process in place to ensure that attempts to upload inappropriate visual content are identified and infringing images are blocked before any minor users of the site could possibly be exposed to them. ONE.LT has implemented a collaborative peer review process and supporting site functionality that filters inappropriate images at the upload stage, before they can be displayed to the site audience. Images not passing collaborative peer review successfully are rejected and prevented from being displayed on the site pages. During the test, created profile got ONE.LT administrators offer to participate in the said collaborative peer review process, checking every profile image against a shortlist of approval/rejection criteria immediately after it is uploaded.

Principle 3: Empower users through tools and technology

According to the self-declaration, functionality has been implemented on ONE.LT enabling any user of the site to respond to unsolicited, inappropriate or otherwise unwanted contacts from any other site user by a) blocking the offending user entirely, thus preventing him/her from initiating any contact with the offended user in the future, or b) reporting any unsolicited message received as spam to the ONE.LT administrative team. During the test it was clear that user account can be "blocked" by any other user, preventing the blocked user from establishing any contact with the user who initiated the block. Also observed that any unwanted messages posted to a user's profile forum by other users can be removed by the user at will.

By the self-declaration, links to all user profiles can be discovered by using the internal profile search function, but the actual content of a given profile can only be viewed by people belonging to the user's extended circle of trust (friends, friends of friends). Test with different created profiles confirmed that information exchange was possible only between community members. Created profiles were searchable for other users with name and contact info information by default only. During the test it was clear that the user has full control over his personal profile data (age, phone number, email address), allowing or prohibiting it from being shown to his friends and/or other users of the site.

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

According to the self-declaration, any user-uploaded image on ONE.LT can be reported as inappropriate by any ONE.LT user, triggering a review of the image by ONE.LT administrative team. Additionally, all

ONE.LT users are encouraged to report suspected inappropriate behavior or content to ONE.LT administrative team by sending a message to the customer service with a link to such content. During the test, measures for reporting of inappropriate image or other content were available on site. Those measures were provided by e-mail contact to administrative team. For the test purposes, massage was sent to ONE.LT administrative team asking for the help regarding scary massage that user have got but no response and advice from SNS was provided during two days testing time.

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

By the self-declaration, responding to notifications of illegal content or conduct ONE.LT customer service is able to do permanent removal of user accounts, review and removal of inappropriate or illegal visual content, review and removal of inappropriate or illegal user groups or their components (photo albums, forum posts, etc.). In cases when potentially inappropriate or illegal conduct or content reported to ONE.LT customer service unit or found by the unit's staff independently is suspected to be in violation of criminal laws of the Republic of Lithuania, ONE.LT declare to follows internal procedures requiring such cases to be reported to respective law enforcement institutions. During the test, no illegal content was found on site on which reports to the ONE.LT customer service could have reason. Anyway, the measures to make a report concerning illegal content are accessible on site.

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

According to the self-declaration, ONE.LT user can change privacy settings for his/her profile data, including the user's age, phone number and email address, by indicating whether every specific bit of profile information should be shared with everyone. During the test persuaded that user privacy data can be changed at any time when the user is logged on. Also was observed, that ONE.LT site has advice on the importance of protecting the user's passwords and properly logging out of the site after finishing a usage session. During the process of creating profile only age was calculated and automatically included in profile.

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

According to the self-declaration, images reported to be inappropriate are reviewed by ONE.LT content moderators that are part of the ONE.LT administrative team. Additionally SNS has implemented site-wide filtering of inappropriate words and expressions in user messages and forum posts, preventing black-listed text strings from appearing on web site. ONE.LT customer service staff tasked with reviewing suspected illegal or prohibited content and conduct is undergoing periodic internal trainings to ensure they are able to identify actionable cases and have the knowledge required for taking appropriate action in every case. During the testing process, attempts to publish inappropriate content performed but their attempts was blocked by moderators.

Conclusions

Summarizing testing results, tester got general positive feeling of the testing object ONE.LT intentions to be socially responsible SNS. During the test of the ONE.LT conformity to the self-declaration, some positive and also weak points observed.

Positive remarks:

- dedicated site section “Your Safety” is a powerful awareness tool providing practical instructions and advice to users on ensuring their safety online;
- profile information is well protected and respond to notifications of illegal content or conduct is prepared.

Negative remarks:

- SNS self-declaration statement that only users 14 years of age or above can register on the site was not implemented at the time of testing and users under 14 years age is searchable by adults users;
- SNS do not have relevant information provided for users about parental control tools that allow them to manage their children's use of and how their can be used for benefit of parents and their children.

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			Not Tested		
6	X				
7			Not Tested		

PICZO

Simon Grehan, National Centre for Technology in Education, Ireland.

Introduction

Piczo, according to their self-declaration, allows members to "share their life stories with friends by designing their sites with multiple pages featuring photos, graphics, videos, music, comment boards, games, and more. Each site can be linked to other friends' sites and members can interact with them and their friends, and meet new people online".

I found that Piczo allows users to create professional looking websites without requiring technical skills. I was able to develop a personal websites using a user-friendly WYSIWYG (what you see is what you get) editor. I was able to create my own website and add items such as images, text content, videos, comments, and connections to other websites in the Piczo community.

Summary

The self-declaration provided by Piczo was largely in-line with the Safer Social Networking Principles. However, some discrepancies' arose during testing. The functionality of the site seems at variance with the description in the self-declaration. It seems that the self-declaration refers to a previous version of the website which was completely overhauled between the submission of the self-declaration and the testing of the site.

While it appears that the functionality of the site has been changed the safety advice and user documentation on the site has not been updated and still refers to the previous version of the site. For example, the self-declaration refers to parental controls for users under the age of 13, while the live site does not permit users in this age group and consequently there are no parental controls available.

The service appears to be more a blogging than a social networking platform. It features user-generated blogs and websites, in a twitter-style approach, allow users to update their feeds and follow other registered members. Each site or blog can be linked to other members' sites. While other social networking sites offer blog functionality as an additional feature, blogging is the main focus of Piczo.

Testing

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 their self-declaration, Piczo has developed a robust Safety education page which is located off the Homepage, linked in the footer, and called out during the Registration process. The footer containing links to Safety, Privacy and Terms of Service are available on all pages within the sites.

A hyperlink to a **Parents** page was found on the footer on the homepage. This link is in a font size larger than the text on the homepage. However this link is not immediately visible when the homepage loads. The user must scroll down twice in order to see the footer. On the **Parents** page prominent links to an FAQ for parents and a Parent's Guide from a third-party online safety organization were discovered.

The content on the **Safety** section of the site was found to be child-friendly. It has short safety tips accompanied by supporting graphics. There are prominent tips on the safety page encouraging users to respect others and never share personal information. It also has links to sections of the site with more information such as a **Safety FAQ**. This FAQ steps through how to report abuse and configure moderation and blocking settings on their profiles.

Both the **Parents FAQs** and **Safety FAQs** were obsolete at the time of testing. The content on the **Parents FAQ** and the **Safety FAQ** seemed to relate to a previous version of the site. In the Piczo self-declaration there is reference to the periodic safety and security campaigns run with partners and information regarding privacy options that are displayed before posting content; neither if these measures were in evidence on the site.

Piczo's claim to provide safety information for parents and young users was validated; however no material specifically targeting teachers was found. The general safety information is easy-to-find and easy-to-understand. The same can't be said of the privacy and terms of service information which is semantically dense and includes legal and technical jargon.

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

Piczo rely on self declaration of age by the user in the registration process as the key mechanism for ensuring that the services they provide are age-appropriate for their audience. If the date of birth entered by the user during registration indicates that they are below the permitted age, they are prohibited from registering. A cookie is place on the user's machine to prevent them from reregistering using a different date of birth.

Piczo claim to use content moderation solutions to identify and remove any content or members that break their terms of service and acceptable use policy (TOS). They claim to use image filtering solutions to flag images that might be pornographic and inappropriate URLs and HTML codes are blocked from being posted on member sites. They say they remove the accounts of users for excessive and/or repeat offences. Piczo says that images that break their TOS are hashed to ensure they cannot be uploaded again. No pornographic content was encountered during testing.

The Piczo submission states that users who declare themselves as younger than 13 must have parental approval via a confirmation email before being allowed to access the service. While testing, it became apparent that Piczo had changed their policy in this area since submitting the self declaration. Piczo made claims about segregating members into over 13 and under 13, with the under 13 service being Children's Online Privacy Protecton Act (COPPA) compliant. During testing, it was not possible to register as an under 13 and a cookie was placed on the machine preventing re-registering as older. Piczo also claimed to provide monitoring tools to parents of children under the age of 13 to monitor what their child is doing on the service. These tools were not found on the site during the testing period.

Principle 3: Empower users through tools and technology

Piczo claims to have taken measures that can help minimise the risk of unwanted or inappropriate contact between children and young people and adults. They claim that websites and profiles of members under the age of 16 cannot be found by searching for them using search engines.

All websites created on Piczo were found to be private in the sense that they are not locatable by other when they first register. Members must take deliberate steps to alert others of their website address. Piczo claims that users can set their websites to one of five types of privacy settings; the world, the Piczo

community, Friends Only, Password Protected, or only viewable by site owner. This feature was not found during testing, but only after comments from the SNS. It seems that the only restrictions on accessing websites or commenting on them are based on the assumption that only users with whom the url of your website is shared will be able to locate it. It wasn't possible using an adult account to access and comment on the website created using an under 16 account without any restrictions. In fact, it proved to be impossible to configure the website created by the under 16 to restrict who could access or comment on the site.

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

I found that Piczo provides prominent mechanisms for reporting inappropriate content, contact or behaviour. These mechanisms are, as they claim, easily accessible to users at all times and are easy to use. However users are not given information about how their reports are being handled nor are they given any feedback on how these reports were resolved.

Piczo has a prominent link to a **Report Abuse** page on the footer of all pages on the site. Links to information about how websites can be configured to deal with the abuse were found on the **Report Abuse** page. Piczo states that it provides an Abuse Hotline and a dedicated email address which parents and school official can use to contact Piczo.

The report abuse function was used to log the following report; "I am writing to you because someone is sending me scary messages. What should I do about this? Please help me." To do this a form was completed that allowed the reporter to provide personal details and details of the abuse. There was context specific advice in the comment field detailing what information should be included to make the report easier to act on. When the report was submitted, text was displayed on screen indicating a report has been sent. However, no specific communications in response to report indicating how the report would be handled was received. No feedback on the outcome of the report was provided. No reference number was provided that could be used to follow-up or track the report.

Principle 5: Respond to notifications of Illegal content or conduct

Piczo recognizes the importance of working with law enforcement in their declaration and outline the processes they have in place to review and remove offending content. They claim to have in place arrangements to share reports of illegal content or conduct with the relevant bodies.

Piczo mentions that it has established working reporting procedures in place with NCMEC and CEOP. They mention mechanisms they have in place to support law enforcement with investigations and prosecutions. Piczo has created a dedicated page on its service for law enforcement that includes a separate contact form and a guidebook on how to contact Piczo for information and relevant support inquires. Piczo also operates a hotline for law enforcement with a 24/7 answering service.

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

In the declaration, Piczo describe a range of awareness raising and technical measures they have taken to encourage users to make informed decisions about the information they post online. They claim the options outlined are prominent in the user experience and accessible at all times.

According to their declaration, "Members can set their websites to community only, friends only, password protected, or private. When contributing content to the community, members can do so privately. Members can set comments to pre-approve prior to being posted. Members can block other members from

contacting them or viewing their site. Members can hide their online status. Members can see the privacy setting for the site and any pages on theirs site in the page name list when editing. Members can quickly edit their privacy here as well. Members can enable right-click protection on images on their site. IM is set to Friends only. You must be a friend with a member before you can IM them." These measures were not encountered when using the Piczo website. The functionality of the site as described in the declaration was different to the functionality encountered during testing; some measures like the IM could not be tested as they are no longer part of the SNSs services. It proved impossible to configure access when contributing content to the community. Nor was it possible to set comments to pre-approve prior to being posted or block other members from contacting or viewing a site. It was not possible to edit privacy settings. The details relating to privacy seem to relate to a previous version of the site. User's privacy was only protected by the fact that you need to know the exact URL of a Piczo member in order to see their site.

Despite Piczo having few measures in place to protect user privacy, they request very little personal information during the registration process and visitors to Piczo cannot search and find any user sites. Only email and age details are mandatory during the registration process and gender, pictures and name fields were optional. Piczo members' sites don't show up on search engine websites.

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

Piczo did not detail in their submissions how they assess their service to identify potential risks to children and young people in order to determine appropriate procedures for reviewing reports of images, videos and text that may contain illegal and inappropriate/ unacceptable/prohibited content and/or conduct. Piczo don't use human moderators that interact in real-time with children. They do detail the measures they take to promote compliance with the TOS.

Piczo claim to use hybrid technical and human content moderation solutions to identify and remove any content or members that break their Terms of Service and Acceptable Use Policy (TOS). They say that images that break their TOS are hashed to ensure they cannot be uploaded again and that users who are found to be in breach of the Terms are either issued a conduct warning or have their accounts deleted depending on the severity of the breach.

Assessment of the Principles vs. the Self-declaration

Principle	Compliant	Partially Compliant	Not Compliant	Not Applicable	Comments/ Clarification
1		X			No material specifically targeting teachers was found.
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	Not Tested				
6		X			
7	Not Tested				

RATE.EE

Andra Siibak, University of Tartu

Introduction

The largest and most popular SNS in Estonia rate.ee has more than "300,000 active users comprising a one fifth of the population" (Self-Declaration, point 1). No information about the age restrictions is provided in the Self Declaration.

The site was „launched in 2002 offering a simple picture rating service it has since grown to a fully fledged online community featuring friends' lists, blogs, albums, and many other services"(Point 1). The website provides the users with additional opportunities e.g. rating the photos of others, sending messages to other users, chatting in forums, keeping a blog, reading horoscopes, converging among different communities, playing games, etc. Several other advantages (e.g. upload one's photos to the site before the others; get a VIP status in a chat room, use the Compatibility-Meter in order to test one's compatibility with certain users from the opposite sex, etc) are made available for the users who have purchased SOL's, the monetary unit only applicable on the *Rate* website. People in all age-groups can become users of the site, no minimum age is necessary.

Compared to some other SNS that are mostly focused on networking as such, most of the users of *Rate* are foremost interested in being rated and rating others. The majority of the users are hoping to gain positive comments and points for their profile images accompanying the textual parts of the profile in order to enlarge their fame inside the community (% of fame of every user is provided on their profile) as well as to gain a place in one of the numerous popularity charts created on the site (e.g. "TOP 100 of the most famous users", "TOP 100 of the most popular dates", etc.). Every user of the site is able to view profiles and profile images of others and rate and comment them according to their preference.

***Date of the test*:** Test was performed from 26. – 28. October, 2009

Main findings:

Rate has taken steps to ensure their users safety, foremost by providing the users with an opportunity to report about inappropriate content and behavior. Nevertheless, considerable gaps in the safety issues have remained e.g. without being a user of the site, one can access all the profile images and the majority of textual parts of the profiles of all the users; re-registering to the system is very easy; users can block their profiles altogether but not all information could be made "private" to friends only; no additional safety measures have been taken to ensure the safety of underage users

Rules of Conduct and Safety Rules can be found easily however, the quality of informative materials for adults and children is really poor.

No parental controls are provided

The process of looking through the reports is quite slow and the quality of feedback moderators give to the users is insufficient

Additional information: As main idea of the site is closely connected with the profile-image rating, there was a need to have live photos of real persons up on profile for the time of the test. The live-photos were provided by the leading experts. However, none of the photos provided could be published on the three fake-accounts created for the test. The profile images of 11 and 14 year old girls were rejected by the administrator as the "image is too small or in a bad quality" (message sent to the profile account by the administrator). In case of the photo of an adult woman, an "authorization code" was needed (message sent to the profile account by the administrator). In order to get the "authorization code" it was advised on the site to take the following actions: "In order to get the code you need, turn for help from some acquaintances who already have photos up on rate.ee. They can order an authorization code you need from their profile. The procedure will cost them 100 bonus points, thus you have to ask very nicely☺. If you do not have an acquaintance here, then send a message to some nice user from the opposite sex and ask them out for a coffee. Then you'll have a new acquaintance and may be also a code that you need. ;)" (http://www.rate.ee/confirm.php). After consulting with the leading experts, and making it sure that the test could be completed without having photos up on the site, it was decided not to pursue the authorization code and leave all the profiles without photos.

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

As suggested by the Principles, the site provider has stated in the Self-Declaration that "terms of Service are provided in a simple and easy-to-read format (http://www.rate.ee/rules.php) and are made available at the footer of every page." According to the Principles, the site provider should have provided "clear information about what constitutes inappropriate behavior", however, in the Self-declaration only "disclosing personal information of other people" is concretely stated to be prohibited. As recommended by the Principles, it is stated in the Self-declaration that additional educational materials are provided both for children as well as parents. No information about educational materials for the teachers is provided in the Self-Declaration. The information provided in the Self-Declaration is partially compliant with Principle 1.

In accordance with the Principle 1, the results of the test show that it is clearly indicated by the service provider in the Rules of Conduct what instances constitute as inappropriate behavior. Furthermore, a Report Abuse Button is provided under every photo, video, blog, comment, community, etc. up on the site. The system can be accessed and handled easily by all of the users. By clicking on the Report Abuse Button users can choose from a pre-given list of possible offences (e.g. inappropriate content, drugs and alcohol propagation, against Estonian law, etc). In addition a small additional report about inappropriate content found can be written which will then be forwarded to the administrators.

In accordance to the Self-Declaration, the site has provided an additional Safety page (http://www.rate.ee/safety.php). Although this page has two sections- for children and for parents- both of the sections have limited content and many safety aspects are left uncovered. No materials targeted to teachers can be found. In the section targeted to adults, it is advised that the parent should spend more time with their children in offline so that a trusty relationship is created with the child and thus, in case of problems in the virtual worlds, the child would ask from their parents for help. Parents are also advised to become users of the site, so that they could keep an eye on their child's activities on the platform.

However, no information is provided what the parents should do in case something bad has already happened to their child; no examples are given what kind of instances could be viewed as harassment or improper behavior online, and no links/additional materials are provided where people could turn for help or gain additional knowledge on the topic.

Majority of topics where Internet conduct or content risks are involved are left uncovered also in case of suggestions for a child (no difference is made between children or teenagers). In a simple language it is advised that children should not to insert information, e.g. contact information, they would not want other users to see, however, no reference about inserting the name of one's school or inserting inappropriate interests to one's age, etc. is made. It is advised how children should proceed when wanting to meet with online acquaintances in offline settings. Nevertheless, no information is provided where children could turn for help; what kind of photos and personal data (e.g. school, home address, etc) would be safer not to upload; what kind of contacts to block or reject, etc.

Under most Frequently Asked Questions, an answer is provided to the question "Is it safe to use rate.ee?" In answer to that question it was reminded to the users that they should be careful about their nickname and password selection, so that there would be no occurrence of identity theft on the site. Nevertheless, all other dangers were left uncovered.

Raising awareness about safety measures taken by the service provider are partially compliant with the information provided in the Self-declaration.

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

According to Principle 2 in the Self-Declaration: "when registering for the service, all users are asked to enter their date of birth". It is also stated that "all profile pictures need the approval by site's moderators". In several aspects, however, the suggestions provided in Principle 2 have not been included in the Self-Declaration. For example, no information is provided about the steps taken to re-register as users; no information about age-restrictions or about the possible uptake of parental controls could be found either in the Self-Declaration or on the site. Although the provider has taken some steps in the Self-Declaration to ensure that the services are age-appropriate, the aspects stated are partially compliant to the Principle 2.

Based on the test results, when registering for the service on the site, it is stated by the provider that users need to activate their profile from their e-mail account. However, the need to active one's account only rose when wanting to make changes in the profile information. Without an interest to change one's profile information, a person could start using the site without actually activating their profile.

Furthermore, one does not need to be a user of the site in order to access and search all the textual and visual information available on the site. Both textual and visual information on the profiles, e.g. profile images, blogs, etc. could be accessed and viewed without the need to register as a user of the site. All the information (except the contact information and real name information i.e. parts of the profile which might have been made private on some accounts) can be found freely available about all the users, including under-age users.

On the site, it is declared by the provider that moderators work in order to find and delete fake-profiles. Nevertheless three fake-profiles were created on the same day from the same laptop, without any problems or a necessity to delete cookies. However, as declared in the Self-Declaration, none of the profile images uploaded on the site was approved by the moderators (cf. additional information).

Hence, the measures taken by the service provider to ensure the services are age-appropriate are partially compliant with the statements in the Self-Declaration.

Principle 3: Empower users through tools and technology

The service provider has not followed several important suggestions in Principle 3. For example, no indication has been made in the Self-Declaration about how to ensure privacy of under-age users; giving control to the users, about who can access their accounts; giving users an opportunity to have just their direct friends posting comments on their profiles; or providing additional educative materials for the parents. According to the Principle 3 of the Self-Declaration „Users have an option to delete unwanted comments on their profile page, users can block other users and reject friend request, users are able to report inappropriate contact„. Nevertheless, the Self-declaration is only partially compliant with the suggestions in the Principle 3.

The test results indicate that adult users of the site are able to search for information or contact under-age users. Profiles of children who are 7 years old or older (http://www.rate.ee/search.php) can be easily searched by adult users who are logged in to the site. Furthermore, besides the in exhaustive safety information targeted to parents, no additional tools for educating the adults as well as filtering or parental control tools could be found.

As promised in the Self-declaration users can block other users, reject friends' requests, delete unwanted comments and report inappropriate content. All of these options are provided as well as easily-accessible.

According to the test results, it cannot be specified by the users who or what type of people can contact them. Furthermore, although users can delete the comments they have received, no opportunity is provided to specify who are allowed to comment their profiles altogether. Thus total strangers, including users without a profile image, can post comments on the profiles of all the users, including under-age children.

Individual "ignore-list" can be created by every user of the site. The nicknames of users whom one has blocked as well as those users who have blocked the profile owner are made visible in the "ignore-list". In order to "block" other users' one has to visit the profile of the person one wants to block and click on the button "block the user". The user needs to provide a reason for blocking which is said to be visible for the person doing the blocking as well as the user who is being blocked.

Users can also block their profiles when clicking on a link on the profile edit page: "Yes, you can block your account from the page "your profile". By doing so, your profile will be made invisible to the users (it will not appear in search results, etc.). In case you block your account and will not log in anymore, your account will be automatically deleted in two months time. During this period, you still have a chance to change your mind"(http://www.rate.ee/faq.php). Nevertheless, the above-mentioned wording suggests that blocking one's profile is something a person does mainly before deciding to quit using the service and less for the reasons of keeping one's profile "private". Furthermore, users cannot make all the information available on their profile available to friends only.

Although additional improvements could be made, Rate has taken steps to empower users through tools and technology, and the measures taken are compliant with the ones stated in the Self-Declaration.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the terms of service

According to the Self-Declaration users can report about "any picture that is inappropriate by using a Report Abuse button" and "report any received e-mail that violates the terms of service". Users are "instructed to write at webmaster@rate.ee to report any violation of the terms of service". The Self-Declaration does not provide any information how to make the reporting most efficient or how the report is acknowledged. As the abovementioned information could be found from the site itself (the service provider had described the aspects which needed to be specified in order the report to be processed by the moderators (i.e. stating the problem, nickname of the abuser, time of occurrence, copy of the content (e.g. abusive comment)), the Self-Declaration is compliant with the Principle 4.

The test results confirm that in accordance with the Self-Declaration, an easily accessible and age-appropriate reporting system, i.e. the Report Abuse button, is available in all different parts of the profile. In addition, a forum where users can post their questions and comments as well as a Customer Service Mechanism, are provided for the users. On both of the platforms, the problems and questions of users are answered by the moderators of the site. However, no information about webmaster@rate.ee could be found on the site and thus it was difficult to find a place where the message in Annex 2 could be posted.

Feedback to the problem "Someone is sending me scary messages" (Annex 2) was received on the next day through a forum. Feedback consisted of a response by a moderator advising: "block the person". A response from the Customer Service Mechanism was received nine days later. First a message was sent to the profile saying "you've got a message from Customer Service". On the Customer Service page the following reply was found: "Hallo! And who is this someone, include some of the messages. Regards, rate.ee team". The reply was created 6. November, 16:16 o'clock.

Although Rate has taken steps to provide easy-to-use mechanisms to report conduct or content that violates the terms of service, the measures taken are partially compliant with statements in the Self-Declaration.

Principle 5: Respond to notifications of Illegal content or conduct

According to the Self-Declaration rate.ee moderator responds to complaints daily. It is also stated that the site cooperates with law enforcement agency provided with the complaint is filed with the police.

Users are informed on the site that the site cooperates with law enforcement agency; however no additional links to law enforcement agencies or other relevant services is provided.

As provided in the Self-declaration, the steps taken to respond to notifications of illegal content or conduct are compliant with Principle 5.

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

According to the Principle 6 a range of privacy settings should be provided and made prominent and accessible at all times. Furthermore, the provider should encourage the users to make informed decisions about their privacy settings and thus, the users should be able to view their privacy settings at any given time. The provider has stated in the Self-declaration that user privacy settings are prominently made available on the site and "contextual warnings are displayed throughout the site and confirmations are asked before user submissions". Hence, the Self-Declaration is compliant with the Principle 6.

Based on the test results it could be claimed that privacy settings apply for certain textual parts in the profile e.g. e-mail, phone, additional contact information and one's full name. In all the other parts of the profile, including profile images, no information is provided how these aspects could be made "private" or available

to "friends" only. The rule is applicable to all the users, i.e. no additional safety measures are used for under-age users. No safety information or reminders appear when choosing which applications to publish. A list of technical reminders but no safety reminders is provided when uploading one's profile images.

One's full name, date of birth, email, gender, location and a photo of oneself need to be provided when registering for the services. All the aspects, except an e-mail and full name which are only available to friends, are apparent on the site when logging in. Although users can block the profiles so that they would be inaccessible for the others, the wording provided on one's profile edit page suggests that blocking one's profile is something a person does mainly before deciding to quit using the service and less for the reasons of keeping one's profile "private". Profiles of 7-99 year old users can be searched for without any age restrictions. When logged in as an adult, an in-depth search was necessary in order to find the under-age fake-accounts as the search engine automatically starts looking for people with photos (cf. additional information). Without that restriction, one of the fake accounts (11-year old girl) was found. It was stated on the site that in case the account name consists of a first name and a surname, it is more difficult for the search-engine finds to find the matching person. Furthermore, all information (except "private" information) is accessible also to non-users of the site.

When registering as a user of the site automatic permission is granted to the provider to use the information provided on the profile for their own purposes (not concretely specified). No information is provided about 3rd party users. Thus, measures taken are non compliant with statements in the Self-declaration.

Principle 7: Assess the means for reviewing illegal or prohibited content/conduct SNS Rate mainly use human moderation and user-generated reports in order to ensure community's adherence to rules. The Self-Declaration states that "hundreds of moderators are monitored by a handful of carefully selected super-moderators. Unsuitable moderators are replaced. Super-moderators are selected and monitored by the site administrator." Moderators help to keep discipline on the site, advise the users, provide information, etc. (http://www.rate.ee/moderators.php). Moderator's approval is needed for all the profile images uploaded on the site. Moderators are responsible for giving feedback to the user-generated reports and removing all inappropriate content. Based on the assessment of the Self-declaration, the measures taken are compliant with Principle 7.

Summary of Results and Conclusion

Although rate.ee has taken several steps to ensure the safety and privacy of its users, additional improvement is needed in order to be able to state that the measures taken are compliant with the "Safer SNS Principles for the EU".

Assessment of the Principles vs. the Self-declaration

Principle	Compliant	Partially Compliant	Not Compliant	Not Applicable	Comments/ Clarification
1		X			
2		X			Several suggestions has not been adhered to
3		X			Several suggestions has not been adhered to
4	X				Information about how to make an effective report is provided on the site
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	*Not Tested*				
6			X		One need not be a user of the site to have access to all the content provided by the users (except parts of the profiles made “private”)
7	*Not Tested*				

SKYROCK.COM

Cédric Fluckiger, University of Lille 3.

Introduction

Skyrock is a SNS specifically dedicated to teenagers and young adults. It offers a blogging service very popular among teenagers in France. Users can create a blog, where articles are mainly based on pictures and short texts. Teenagers use Skyrock blogs to create kinds of "profiles", and communicate with friends. Users can comment other user's articles. One of the important features, that made this blogging plateform become one of the most popular SNS among teenagers, is the possibility to set up a list of friends and friend's blogs. The minimum age is 12 to create an account.

Conduct of the testing

The testing was conducted from october 25th to october 30th 2009. For the testing, the screen resolution was set to 1024*768. Note that the accessibility of information and readibility is lower at that resolution than at a higher resolution. Skyrock was tested in French.

Summary of findings

- Information is sufficient, adapted to adults and children. The only concern one might have is that this information is somewhat "hidden" in the terms of use page and not more directly accessible.
- Children under 12 cannot create a profile on Skyrock. However, when rejected for being too young, a user can immediately change his/her age and register as an older teenager (according to Skyrock, this problem is dealt in backoffice).

Reporting the results

Principle 1: Raise awareness of safety education…

In the self declaration

In its self declaration, skyrock.com states a large number of safety measures, which can be roughly summarized in sending security warnings before posting; providing a "flag this content" button on every page; providing minors and parents with guidance, education information, tips and context-specific warnings; displaying the Insafe national campaign about bulliying; participating in EU Safer Social Networking Task Force, having relationship with the Minors brigade in Paris and in "Alerte Enlevement" (French Amber Alert aquivalent).

Information provided

The self-declaration says that "Skyrock provides since April 2009, clear targeted guidance to minors and parents in a prominent accessible and easy to understand format (cf http://www.skyrock.com/safety/index.php)." Indeed, the "Terms of use" page is easily accessible form a link at the bottom of the page. However, one could regret that the link displayed is "Conditions", which

stands for the french usual "Conditions d'utilisation", but could be rather difficult to understand for youngers.

On the "terms of use" page, the terms are presented in both extended or summarized way. This allow to have a full "legal style" terms of use on one hand, and easy-to-understand language, relevant for teenagers on the other hand. The summarized version of the terms of use gives safety information and lists age requirement, contents and conducts that are not allowed on the site. It also indicates the consequences of engagment in prohibited behavior. There is a "sécurité" (safety) link beside the terms of use that leads to the terms of use.

Indeed, the terms of use page provides also users with other useful and clear information. However, these pages are not very visible in the terms of use page.

The safety information is devided into: help - terms of use – parents – minors. The "Help" page gives information on registration and login access, but gives also useful security/privacy/report information. For instance, it explains what to do in different situations: "Someone hijacked my account! What do I do?"; "What do you do with my personal information?" or "How do I delete my account?"; etc. The "Minors" (under 18) page (http://fr.skyrock.com/safety/minors.php) gives 10 pieces of advice to young users in an easy-to-undestand and age-appropriate language, such as: "warn your parents that you want to open an account on Skyrock.com and get their authorization"; "when registering give your real age"; "the blog and profile are public spaces accessible to everyone"; etc.

Information for parents or teachers

As stated in the self-declaration, information is given to parents. The "parents" page gives information to parents (http://fr.skyrock.com/safety/parents.php). It gives parents advices on what to do when they discover inappropriate content, on how they can close any account their child has created, and so on. No information is given to teachers.

Links to association and help services

As announced in the self-declaration, Skyrock.com provides links to: Internet sans crainte (Insafe programme in France) ; E-enfance (association implied in the insafe program); Safer Internet page; and Net ecoute (a phone help line, operated by e-enfance).

Specific information and tips

The self-declaration also states that ", before accepting the Terms of use, a short summary of users major engagements", which is verified in the testing.

The self-declaration states that "All users receive security warnings before posting content on the platform", and that "Skyrock.com provides education and tips about online safety and privacy", when posting content, safety and privacy tips are given. Though the message is not very visible, it is complete and adapted to children.

Principle 2: Work toward ensuring that services are age-appropriate…

The self-delcaration says that "The Skyrock.com service is mainly designed for young people (12 or older). Skyrock.com does not host any "adult" content or does not have any specific sections or services for adults". Indeed, the testing confirms that the Skyrock service is designed for children and teenagers: there is no specific service or content not suitable for them. Therefore, there is no parental control device, restricting the access to some parts of the content to adults.

Creating a profile

"Skyrock's Terms of Use clearly indicates a minimum age to use, and moreover to register on Skyrock.com". However, in the self-declaration, no reference is made on how it is made clear. It only says that one cannot register when too young.

In the testing, it was confirmed that a child under 12 cannot create a profile: a message is displayed in the form: "registration is only authorized to 12 years-old or older".

The self-declaration says that "Skyrock uses cookies session, permanent cookies, email and IP addresses on its registration page to flag users who will change their age if the initial age was below the one specified in our Terms of Use". However, during the test, it appeared that one can change his date of birth and log-in without a problem once this message has been displayed. When a child (older than 12 years-old) creates an account, he or she receives an e-mail.

The user is also asked if he/she wants to receive promotional offers from partners, though teenagers might not be fully aware this means advertising. Users can also decide wether they can be found by their e-mail, first or last name, or not (all in one).

The self-declaration states that "Skyrock uses filtering algorithm especially in French, Dutch and English, to seek and delete individuals misrepresenting their age." The test could not validate or invalidate this statement. It could not be tested either that "Skyrock moderation staff actively searches out underage users manually. Upon discovery that a user is not 12 years or older, Skyrock.com deletes the user's account, blog and profile."

The self-declaration states that "skyrock uses cookies session, permatent cookies, email and IP addresses on its registration page". However, it is possible to log as an adult after being logged as a child, without having to remove a cookie.

Means to limiting exposure to potentially inappropriate content

Skyrock says that "All hosted images are hashed when uploaded and are all reviewed by the Skyrock.com moderation team for compliance with Terms of Use. All deleted images are then hashed to ensure they cannot be re-uploaded."- "Skyrock.com filters automatically thousands of inappropriate terms and urls every day". In the conditions of the testing, it was not possible to test these statements.

Principle 3: Empower users through tools and technology…

Skyrock provides users with some tools to manage their contacts and choose some privacy and safety options. In this section, are detailed the main features mentionned in the self-declaration. Age-based search restrictions are detailed in the principle 2 section above.

Accepting or blocking friends requests

A user can accept other users as "best friends" (meilleur ami), accept as friend, refuse or wait. On the profile settings, one can decide who can write a comment on its blog: all users - all registered users - only friends - only best friends

Controlling comments on the blog

A user also has the possibility to validate comments before they are displayed (the comment says that "this option allows you to check comments on your blog before they are published").

Contact options

Skyrock states in the self-declaration that "Minors or majors cannot contact members who are not in the same age group". Search options are detailed above. The testing shows that an adult can send an invitation to a 15 years-old girl and be added on it's friend's list. However, when those users are "friends", they cannot send messages to each other

The black list

One important feature cited in the self-declaration is the black list. Evey user can black-list another user. When a user is black-listed, he/she appears in the black list. The user has the option to unblock any user in its black-list. Surprinsingly enough, a user in the black-list still appears in the list "My complete list". From that list, one still can add him as best friend! This means that this user will appear *at the same time* in 3 lists: My complete list - My best friends - My black list

Note that a user is not warned that he/she is black-listed: when he clicks on "add a comment", nothing happens.

Deleting a profile

Information about deleting a profile can be found in the FAQ section, and is therefore not so easy to find for a child. Information is quite complete and understandable for children "if you delete your account, you will lose information on your blog, your profile", etc.

In order to delete his/her profile, a user has to find the "delete" button, just below the advestisment. This button is not easy to find in the page. It leads to a specific page where one can delete his/her profile.

Regarding the conservation of personnal data, the terms of use explains that data are either erased or anonymised.

Principle 4: Provide easy-to-use report mechanisms…

As stated in the self declaration, there is a button to "report an abuse" on every blog. When a user click on the button, a window appears, where the user is asked to enter a valid e-mail ; choose a category of the abuse; write an additional comment; precise if the report concerns : the entire blog – pictures – messages - the blog's prestentation – videos – comments – other. When the user clicks on "send", the following message appears: "WARNING: it is not advised to report an abuse on a blog if it does not violate the General Conditions of Use of the service. For your information, if your request proves to be unjustified, it shall be sent to PROPER AUTHORITES (police or tribunal). Therefore are you sure you want to report an abuse on this blog? "

It is not possible to send the message "someone is sending me scary messages…" as Skyrock only provides a mechanism to report a specific blog.

A few minutes after sending a report, an email is sent from the "skyrock team"s saying : "Hello, Skyrock.com received your report regarding – lucasmartinssnpt09 – Pornography. It will be treated by our teams as soon as possible. If you wish to complete your report, thanks for answering to this email without changing the subject. Thanks for contacting Skyrock.com." However, 3 days later, the reporter was not informed if the report was taken into account, and if the reported blog was compliant with the terms of use.

Principle 5: Respond to notifications of illegal content or conduct

According to the self-declaration: "Extremely inappropriate contents or behaviors such as paedo-criminality, racial hate, inciting or advocating crimes against humanity are reported to the French Interior Minister centralized platform (PHAROS)."

Principle 6: enable and encourage users to employ a safe approach…

In the self-declaration, the only information provided is that "Skyrock.com allows users to manage their personal information and privacy in an all-in-one URL". These options where tested during the testing and are detailed in section 3.

Information added onto the profile is: age, gender, home town and a picture if the user uploaded one.

Concerning age restrictions, only one functionality is mentioned: which category of contact is allowed: "The age registered by the user will determine which categories of age groups the user will be able to contact or be contacted by".

Indeed, the test showed that searchable profiles depend on the age of the user: unregistered users cannot search under the age of 16; users registered as adults cannot search minors under 18; when connected as a 15 years-old girl, searchable profiles are categories from 12 to 16.

Principle 7 : assess the means for reviewing illegal…

In the principle 3 of the self-declaration, Skyrock states that it uses both human and automated forms of moderation:

- Skyrock.com moderators are experienced and trained". Also in Principle 5: "The moderation staff works 24/7 and is seized to handle the thousands of reports or millions of images, texts or other contents and behaviors that are illegal are removed immediately by the Skyrock.com team upon notice and saved for possible police investigations
- Skyrock.com uses a series of tools and algorithms to identify anomalies in how a user might be using Skyrock.com. Users' behaviors are then rated and Users can be excluded from the website". In principle 2: "Skyrock.com filters automatically thousands of inappropriate terms and urls every day

Skyrock also states that reasonable steps are taken to minimize the risk of employing candidates who may be unsuited for work which involves real-time contact with children or young people: "Skyrock.com moderators are experienced and trained. All moderators' backgrounds are checked when hired."

Conclusion: global assessment of compliance

Assessment of the Principles vs. the Self-declaration

Principle	Compliant	Partially Compliant	Not Compliant	Not Applicable	Comments/ Clarification
1	X				
2	X				Nothing is said about parents being able to "manage their children's use of service"
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			- No measures are taken to "prevent users from attempting to re-register"
3	X				
4		X			- Notification possible only on content (one specific blog), not on conduct
5			Not Tested		
6	X				
7			Not Tested		

SULAKE

Mika Rantakokko, Center for Internet Excellence

Introduction

This evaluation of social networking services concerns Sulake Corporation and its two services, Habbo Hotel and IRC-Galleria. Tests were done to the Finnish language versions. The tests were performed on 28.-30.10.2009. Sulake Corporation, founded in 2000, is an online entertainment company focused on virtual worlds and social networking.

Currently Sulake operates three services:

Habbo Hotel: The world's largest virtual world for teenagers. Habbo is a multi-dimensional virtual world and community for teens. Users join by creating a fully customized online character called a Habbo. From there, they can explore many public hang-outs, participate in a variety of activities, connect with friends, decorate their own rooms, and have fun through creativity and self expression. Currently there are Habbo communities in 33 countries on six continents. To date, 151 million Habbo characters have been created and 14.6 million unique users worldwide visit Habbo each month (source: Quantcast and Sulake statistics). Minimum age of the service user in Finland is 10 years; though recommended minimum age by service producer is 13.

IRC-Galleria: IRC-Galleria is currently the most used social networking service in Finland with over 500 000 active registered members. The average age of the users is currently over 20 years. IRC-Galleria is an interactive service where users can e.g. post and share their photos and music on their own customized site, join different communities and communicate with people in many ways. In addition to Finland, IRC-Galleria is currently available as a local service in Germany. Minimum age of the service user is 12 years.

Bobba Bar: Recently established virtual networking service for people older than 16 (not part of self-declaration or this assessment).

The assessed services, Habbo Hotel and IRC-Galleria are fulfilling the Safer Social Networking Principles for the EU quite well. Self-declarations concerning both Habbo Hotel and IRC-Galleria are informative and clear, as well as in line with the EU principles.

Habbo Hotel with main focus on service for teenagers the main point is the anonymity of the service, which is also main point concerning the safety. In the guidance on how to use the Habbo Hotel service it is underlined that you are not allowed to give any personal information where you could be identified. Concerning IRC-Galleria the main focus is being more identifiable; including for example that picture in the profile must be clear enough so person can be recognized from the picture. Security guidance in both services is informative and easy to find.

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

1. To which extent the actions mentioned in the self-declaration are in line with the Principles?

Actions concerning both services which are mentioned in self-declaration are well in line with the Principles. In both services the only exceptions are teachers, which are neglected as actors promoting safe use of SNSs. *This shortage results that the services provided by Sulake are only partially compliant with the Principles.*

2. Have the measures reported in the self-declaration report been implemented?

Reported measures have been implemented. There are clear instructions for users as well as clear information concerning the situation when the rules are not followed.

3. Do the implemented measures work?

Instruction and rules presented in self-declaration works as presented. Sulake also co-operates with governmental organizations and campaigns like Insafe / Safer Internet Day and many other organisations. These collaborators play an important role especially in the case of Habbo Hotel in the services giving guidance about safe use of SNS's.

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

1. To which extent the actions mentioned in the self-declarations are in line with the Principles?

There are age limits both in Habbo (recommended 13 years, minimum 10 years – limits are mentioned in the service, though different ages have no visible effect on how does the service work) and in IRC Galleria (12 years). Minimum age of 10 to access Habbo is not mentioned in self declaration as it is done from international perspective. The self-declaration states that there are no reliable technical tools to guarantee the age. According to the service guidelines moderators monitor user behavior and remove clearly under-age users.

2. Have the measures reported by the signatories in their self-declaration reports been implemented?

Age limits are clearly mentioned in the services. When trying to register as under age person both services deny the access. This feature in both services was tested by ages 7, 9, 9 years 10 months and 11 years 6 months. The registration was denied while confirming the registration. It was possible to register from the same computer, with the same name and email address, only by changing the date of birth.

3. Do the implemented measures work?

There are age limits both in Habbo (10 years) and IRC Galleria (12 years). If trying to register as under age services don't give access. Though, it was easy to register to both services by attempting again with identical information by only changing the age.

Principle 3: Empower users through tools and technology

1. To which extent the actions mentioned in the self-declarations are in line with the Principles?

In Habbo there are no public profiles; and it is also possible to limit others to contact your profile. Default setting in Habbo is that the profile name and character are visible. Also in IRC Galleria it is possible to customize your visible profile and for example put unwanted profiles to black list, so they cannot send comments to you or see your private pictures. Default setting in IRC Galleria is that the profile picture and name are visible. There are no parental tools in Sulake services, excluding the guidelines for parents.

2. Have the measures reported by the signatories in their self-declaration reports been implemented?

Reported measures are been implemented in respective services. There are easy-to-use tools to control which information is visible in the profiles. The Habbo feature of being anonymous was tested by putting imaginative telephone number and name to the profile. This information was removed by moderators. In IRC Galleria the focus is in being identifiable; if you put there a picture from which you cannot be identified you will be asked to send another picture. This feature was tested with the artificial picture provided to the test; there was feedback from moderator to change the picture to something more identifiable.

3. Do the implemented measures work?

The technical tools like filters and automatic monitoring tools are mentioned but not presented in detail. This makes it difficult to evaluate how they work. Personal tools like limiting the access by other users of the service to your profile works well.

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

1. To which extent the actions mentioned in the self-declarations are in line with the Principles?

Reporting tools for illegal/harmful content are very well in line with the Principles. Almost in every view there is a possibility to report conduct or content. In Habbo there is a question mark which you can push if you feel any kind of threat or would like to report something. In IRC Galleria there is a similar button "inform maintenance".

2. Have the measures reported by the signatories in their self-declaration reports been implemented?

Easy-to-use reporting tools are available all the time, in every situation. You can report all kind of content, and also send report via various ways, including telephone line and e-mail.

3. Do the implemented measures work?

Reporting mechanisms about harmful/illegal content were tested asking for help because someone is sending a scary message. Reporting was easy to be done and fulfilling the Safer Social Networking Principles in both services. In Habbo Hotel there is a help tool which can be used for this purpose. In IRC Galleria there is a report-button in every view. In both services you got feedback to your registered e-mail. When sending in a report there was an immediate reply to the e-mail concerning the report with information that the report/request will be handled within next three days. In the more detailed reply which came later was additional questions and guidance on how to react to scary messages. Concerning the reply from IRC Galleria the moderator requested information about which nickname sent the scary messages so they could check it and take the necessary actions.

In IRC Galleria FAQ it has been described that you will not get detailed reply about what will be done with the report concerning other profiles in the service. Concerning the reply from Habbo there was also a question to send additional information.

Principle 5: Respond to notifications of Illegal content or conduct

1. To which extent the actions mentioned in the self-declarations are in line with the Principles?

Self-declaration is fully in line with the Principles. According to the self-declaration the reports referring to illegal content and conduct are top priority of Sulake SNS's. Reports are handled according to that approach, as urgently as possible. There is also good collaboration with authorities, and illegal content is reported to them if there appears such.

2. Have the measures reported by the signatories in their self-declaration reports been implemented?

The measures are described in the rules and regulations as well as concerning the use of the services. Also the close collaboration with the authorities is mentioned both in Habbo and IRC Galleria case.

3. Do the implemented measures work?

These measures were not tested in this assessment.

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

1. To which extent the actions mentioned in the self-declarations are in line with the Principles?

Actions are in line with the Principles. Concerning Habbo there is even more secure situation, than with ordinary service because in that service the participants are anonymous; Habbo users are not allowed to give any identifiable information like real-life photos, videos or share any personal information. This principle is informed and followed very strictly contributing centrally to the safety of the service.. Though it is also possible to limit who can access your Habbo profile.

IRC Galleria is based on certain publicity; ia. you must appear there with your own face. At the same time you can still customize the user experience and privacy settings according to your wishes.

2. Have the measures reported by the signatories in their self-declaration reports been implemented?

Measures mentioned in self declaration have been implemented in the services.

3. Do the implemented measures work?

The measures can prevent unwanted contacts and visibility.

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

1. To which extent the actions mentioned in the self-declarations are in line with the Principles?

Self declaration is in line with the Principles. There are both human moderated reviews complemented with technical automatic filtering.

2. Have the measures reported by the signatories in their self-declaration reports been implemented?

There is limited information about moderation and automatic tools to follow up the services and content there. This limited information is understandable due to the nature of the guardian role.

3. Do the implemented measures work?

These measures were not tested in this assessment. There are some statistics giving a view to the success of used tools; according to the SNS the amount of pictures against the service rules in IRC Galleria have gone down from 1/500 to 1/1000 during the last three years.

Summary of results and Conclusion

Awareness raising of safe use principles are clear covering all the main points to guarantee safe activities within the services, taking also into account different age groups. Teachers as a target of safety education messages are the only groups which have been forgotten.

Habbo Hotel has the minimum age of 10 years, while recommended minimum age is 13 years; though there is no different treatment for those youngest users. IRC Galleria has an age limit of 12. Registration with under-age profile is not possible, though you can register after using under-age just by changing the date of birth and keeping the rest of the registration information the same as before. Age limits are difficult to control, but the services are doing quite well by combining techniques with human moderation for that purpose. Especially in Habbo Hotel the users are also receiving lot of education about safe use of internet, partly due to the age structure.

Users of both Habbo Hotel and IRC Galleria can control the public information ia. by blocking the information which is not wanted to be public as well as by blocking unwanted people contacting them. According to the tests both services provide easy access to report content or conduct that violates the terms of service; reporting possibility is available all the time. These reports are the top priority of the maintenance. Notifications are taken very seriously, and if needed handled in collaboration with authorities. Habbo Hotel service is based on anonymity with no pictures and real contact names while IRC Galleria requires certain public profile.

Sulake Corporation and its SNS's Habbo and IRC Galleria are well functioning services complying quite well with the Safer Social Networking Principles for the EU and self-declaration.

Assessment of the Principles vs. the Self-declaration

Principle	Compliant	Partially Compliant	Not Compliant	Not Applicable	Comments/ Clarification
1		X			Teachers are not taken into account concerning the awareness raising.
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			It was possible to register with the same information by just changing the date of birth from under-age to sufficient age.
3	X				
4	X				
5	*Not Tested*				
6	X				
7	*Not Tested*				

TUENTI

Charo Sádaba, School of Communication of the University of Navarra

Introduction

Tuenti is the most popular social network amongst Spanish teenagers. It is a private network, as a *by existing member invitation only* system is established to add new users. Every member of the SNS has several invitations, usually 10, to send to friends or relatives. Minors under 14 are not allowed to open an account.

According to the SNS self-declaration, this system allows users' control over the network and constitutes the main security mechanism that is built on users' confidence. In fact, only personal users are allowed to open an account: companies or institutions cannot have profiles. Commercial presence is limited to organizing events that users are invited to take part. In its self-declaration Tuenti declares to work with public and private institutions with educational goals in order to increase users' security online. Besides that it also mentions that users profiles are not indexed on search engines, as Google, in order to protect their privacy.

As other SNSs Tuenti offers the most common utilities: personal profile pages, photo and video uploads, personal messaging and chat.

The test was performed October 27th 2009.

Self-declaration does not refer to any specific educational resource provided by Tuenti for parents or educators and relies very much on the by invitation and self-controlled model that Tuenti proposes. The SNS seems to rely too much on users and does not describe the proactive attitude it could take to make this principles a reality. Most of the relevant information is included in the Terms of Use, a document available only to users.

In general, Tuenti's self-declaration could be improved in order to get a closer accomplishment of the Safer Social Networking Principles. Besides that, what Tuenti declares on its self-declaration is only partially present on its website.

Reporting on testing results:

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

Tuenti does not include any reference to its terms of use on the self-declaration, that appeals to confidence as the best tool for security. The SNS does not explain how it is going to assure that users confidence drives to real security.

Most of the relevant information regarding this principle is included on the Conditions and Terms of Use, but this information is available only for users. The terms of use are more than 8 pages of text that combines some sentences that use an age-adapted language with others using legal and not so easy to understand expressions.

Regarding the information for parents or educators, Tuenti does not provide any information on its website for these groups. It is stated on the self declaration that "*Tuenti works in permanent collaboration with educational institutions in order to disseminate online security policies by using a series of tools made available by Tuenti, along with specific education on our general privacy principles. Furthermore, Tuenti collaborates with institutions that protect minors to develop promotional campaigns to foster online safety for minors on the Internet*". But this collaboration is not presented in the website.

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

In the self-declaration Tuenti states that "*is a network platform for users aged 14 and over and complies with this standard by upholding a very clear-cut Privacy Policy*". This Privacy Policy is fully explained in the Conditions and Terms of Use, using a not very easy to understand language.

"*In addition, we have signed an agreement with the Spanish Data Protection Agency, whereby our public commitment to prevent minors from creating and maintaining accounts in our network is formally laid out*."

During registration process the system does not allow to select a birth date before 1995 (under 14). But users could chose any other data if they want a personal profile. In fact, as registration as a 11 years old girl was not possible, a new attempt was successfully made under a 15 years old fake profile during the same session an through the same computer.

Under principle 1, the SNS states that "*members do not allow unknown people or fake profiles in their networks and report questionable profiles to our staff as a safety precaution*", what is not a SNS proactive measure towards security rather a presumption that users will do that thing.

Despite the *by invitation only* system, it is easy to find, through Google search, i.e., someone who gives away some invitations. Introducing "invitation for Tuenti" on Google more than 66,000 results are obtained. There are pages as www.tuentiadictos.es, www.invitacionestuenti.net or www.eltuenti.org where users can obtain an invitation from unknown members.

Again, most of relevant items for this principle are only available at the Conditions and Terms of Use.

Principle 3: Empower users through tools and technology.

As it is stated on its self-declaration, "*Tuenti provides its users with user-friendly tools that ensure a high level of privacy. We offer our users a wide range of very secure functionalities that, for instance, allow them to block messages sent by unknown senders and to decide which of their contacts can or cannot view and/or download their pictures*". Most of the functionalities offered to users are not mentioned on this document (self declaration) but are exhaustively detailed on the Conditions and Terms of Use.

No reference to parents or educators is made in this point, and the self-regulation model is presented as the best security system.

Inside the SNS, the availability of tools to report abuse or bullying is not clear: those are under the Frequently Asked Questions, covering all kind of subjects (from how to use tools, to more serious issues).

Users are provided with tools to control their own information: they can block users, remove postings or pictures.

Profiles are opened under real names, nor nicknames, including as mandatory fields, information as name of school (selected from a list, fake names are not possible), university (the same applies) or company where user is working (it is the only option not using an existing list).

Besides that, school/university options are linked, as mandatory information, to expected graduation year. The school or university name is presented with the place where the educational center is located. Users can change the privacy options of their profiles (open to everyone, only friends or friends of friends), but basic mandatory information (name, school or university, and city) is public and searchable. It is possible, i.e., to find where a particular person lives (city), or which school is attending.

Under principle 1, in self-declaration, Tuenti recognises that it "*does not index any user data in online search engines, and nobody can join Tuenti without a prior invitation from a current member*".

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the terms of service

Self declaration relies on users as the main factor to report conduct or content that violates the terms of service. Self declaration does not identify a proactive attitude towards these issues. It also recognizes that it is improving the Conditions and Terms of Use in order to create a safer environment.

Although it is easy to report an abusive picture/video, there is no quick way to report an abusive situation: user is redirected to the FAQs, or, if he has read the Terms of Use, he knows he can write an email to the SNS, and an email address is provided.

In the FAQs it is not a direct tool to chat with some responsible of the network. It is possible to send a message through the help page inside the SNS, but limited options are offered: it just could be tagged as an "error" or a "suggestion".

A message was sent to soporte@tuenti.com, the email provided by the SNS, asking for help to deal with an uncomfortable situation (receiving scary messages from other user). An automatically generated email was received from SNS with the advice of checking again the FAQs looking for an answer and, in case it was not found, sending a new message.

Later, other email, with a more personalized answer, was received where some extra information was provided explaining how to report a user or an illegal content. In both cases, a technical procedure was explained, and it was remarked that in order to evaluate the reporting, appropriate problem classification was needed.

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

Inside the network, and coherently with self declaration, users are provided with quick and efficient tools to block content or users with inappropriate behavior. Users could report an illegal or abusive picture, video with really simple tools.

It is also mentioned that the SNS offers its Support team with ongoing training on legal and privacy issues to answer quickly to users demands, reports and questions.

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

It is interesting that in this principle, where Tuenti is doing its best, is not well described in the self-declaration: it is just mentioned, the by invitation only system, but not explained.

Users are allowed to invite friends to join the network. Those friends only could open an account under the email provided by *current members*: when opening a new account, email information is system provided as non-removable field.

Besides that, some personal information is included in the profile: name and last name, sex, birth date, province, school or university attended and expected graduation year. Filling in these fields is mandatory, and all of them are automatically uploaded to the profile.

And again, Tuenti assures that profiles are not indexed on search engines.

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

In its self-declaration Tuenti does not mention anything about that. It says it works with several institutions, mentioned in the self-declaration, in this field. But it is not explained how collaboration works, and no links to this institutions are provided at the homepage, nor inside the network.

Again, most of relevant information is provided in the Conditions and Terms of Use.

A. 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		

B. 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			Not Tested		
6		X			
7			Not Tested		

VZNET NETZWERKE LTD.

Jan-Hinrik Schmidt, Hans-Bredow-Institute for Media Research, Hamburg

Introduction

The VZnet Netzwerke Ltd. provides three social network sites for the German market: *schülerVZ* (http://www.schuelervz.net) is a platform aimed at pupils from 12 to 21 years, while *studiVZ* (http://www.studivz.net) and *meinVZ* (http://www.meinvz.net) are both open to users above 18 years only. The general design and most of the functionalities of all three platforms are very similar: Registered users are represented by a profile site where they publish certain personal information like hobbies, favorite music or popular movies as well as pictures. They can add other users as their "friends", create or join groups where they can engage in discussions about topics they are interested in, and use channels for interpersonal communication such as direct messages or chat. In this respect, studiVZ and meinVZ are completely interconnected, so users can contact each other or transfer their profile from studiVZ to meinVZ. schülerVZ, on the other hand, is a stand-alone platform, that is not open for general registration and allows no interaction (e.g. no messages or friend requests) with users of studiVZ or meinVZ.

All three platforms are among the most popular social network sites in Germany and combined a total of 13.5 million registered users in April 2009. VZnet Netzwerke Ltd. claims that 75% of all Germans between 14 and 29 years own an account at one of the three networks.

Summary

The evaluation shows that all three platforms provide extensive and age-appropriate information about reasonable conduct, possible privacy risks and other problematic aspects of use. There is no external check for age, so users might open fake accounts, posing either as a teenager (schülerVZ) or as an adult (studiVZ and meinVZ). The platforms offer options to modify various aspects regarding privacy and disclosure of personal information to other users, and also provide options to report offensive users, groups, and pictures. However, there is no way to report offensive messages or postings as such.

2. Testing results

The following discussion of the testing results is focused mainly on schülerVZ, since this platform is targeted specifically at adolescent users. The platforms studiVZ and meinVZ are open to adult users of 18 years and older only. They are similar in design, but in some instances do provide some different mechanisms of applying the "Safer Social Networking Principles for the EU". These differences are also mentioned in the following paragraphs.

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

Although VZnet Netzwerke Ltd. does not specifially mention all aspects that relate to safety awareness in their self-declaration, schülerVZ provides a wide range of information about safe and reasonable conduct that is targeted at different groups. Because the platform itself is only open to 12- to 21-year-olds (although one cannot rule out that parents, teachers and other older adults might have fake profiles on the site), most of the safety information is targeted at teenagers and young adults. It is easy to understand as well as exhaustive and includes not only text, but also videos. In addition, schülerVZ provides information end educational material targeted specifically at teachers and parents, but no specific information for children of 12 years and younger.

The information and educational material (e.g. teaching units on topics such as privacy or self-disclosure) is easy to understand and accessible. The links to the material, as well as to organizations providing additional help, are featured in the bottom navigation on each page. Information is not only textual, but also provided in a couple of short videos. Some of these (dealing with the Code of Conduct which is complementing the Terms of Service) resulted from a competition and have been produced by users of the platform themselves (http://www.schuelervz.net/l/rules/).

Both the Code of Conduct and the Terms of Service prohibit various forms of content (e.g. hate speech or pornographic images) and of conduct (e.g. bullying or mobbing). The safety information also mentions other aspects such as the prohibition of fake accounts, the possibility of 'surveillance' by prospective employers and the copyright users possess in their own photos or messages. It does not mention the possibility of inappropriate contact from adults or information on self-harm actions.

studiVZ and mein VZ do also provide links to the Terms of Use, the Code of Conduct and general safety advice within the bottom navigation of every page. Due to the different age group targeted (18 years and older), there is no additional information for particular groups such as teachers or parents. The information is primarily textual, with no user-generated advice videos as in schülerVZ. Although some of language and the topics of the safety and privacy advice differs from schülerVZ, the Code of Conduct on all three platforms is very similar and prohibits offensive content or behaviour.

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

VZnet Netzwerke Ltd. states that they address the principle of age-appropriateness by targetting their platforms to different age groups: schülerVZ is restricted to users between 12 and 21 years; studiVZ and meinVZ are open only to users older than 18 years.

Registration at schülerVZ is not generally open, but only possible via an E-Mail invitation from already registered users.[15] After receiving the invitation link (which also serves as a confirmation of the E-Mail address), new users have to give their birthday date. They are denied from registration if they are younger than 12 years or older than 21 years. After receiving the warning, however, they can easily change the birthday date at the registration form. Since there is no external check of the users' age, it is possible for younger or older users to get an invitation code through already registered friends, then give a false birthday date and create a fake account. The platform relies on reports from the community to identify these fake accounts. It states in the self-declaration that these profiles will be deleted and the corresponding E-Mail addresses will be locked so no future attempt to register can be made through them.

schülerVZ is intentionally targeted at adolescents and young adults. Specific parental control tools are not mentioned in the self-declaration nor implemented on the platform, as well as no specific functionalities for

[15] For testing purposes, an invitation gained during a previous research project was used.

labelling content or for restricting access to particular times of the day. VZnet Netzwerke Ltd states that they employ educationists who are evaluating the communication and safety education on the schülerVZ platform.

Contrary to schülerVZ, registration on studiVZ and meinVZ is open to anyone, but in their Terms of Use they restrict their service to users of 18 years and older. If the age given at registration is under this limit, a warning appears. The age can then be changed without problems and without an external check, so it is generally possible for adolescents to create a fake profile on these sites.

Principle 3: Empower users through tools and technology

VZnet Netzwerke Ltd. states that profiles on all three platforms are not searchable for outside crawlers or search engines. The self-declaration does not give any information about options for managing or pre-moderating comments, nor on how to delete one's profile. The platform gives information on how to modify their privacy settings and how to report abuse or bullying in their general safety tips. It does provide no option to limit the range of users that can send contact requests or messages to specific age groups etc..

Within the schülerVZ platform, users can modify privacy settings which make it possible to, for example, restrict access to profile information (or parts of it) to their friends only. There is no option, however, to define sub-groups of one's friends list (e.g. "close friends", "my football teeam" etc.) and then use these groups to restrict or open access to personal information in a more differentiated way.

As a default, only friends (confirmed contacts) can access one's profile and post comments there, but these settings can be changed. Users can remove both comments others have made on their profile as well as own comments they have posted on other peoples' profile. Users can also block/ignore or report other users (see below).

It is not possible to post pictures directly to other peoples' profile, but users can include picture folders on their own profile and can identify (tag) other users on the pictures. While the default privacy setting prohibits this tagging of others, users can set the option to "my friends can tag me" and "my friends can tag me but I have to approve it". Users can not be tagged by people who are not on their friends list; this information is also stated in the privacy setting section. When uploading a picture, users receive information about copyright issues and a link to the code of conduct.

The link to delete one's account is not given on the profile itself, but under "my account". The provider states the deletion (which is said to be complete, not a mere deactivation) might take up to 48 hours. Users are also informed that they should check if they want to have comments, pictures or postings on other profiles or in groups deleted as well. Contacting schülerVZ to ask for deletion of pictures AFTER deleting one's own profile is possible, but will take more time.

With respect to privacy and control over one's profile (including deletion), the "architecture" of studiVZ and meinVZ is almost identical to schülerVZ. Users can open or restrict access to their profiles and other information through the privacy settings.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the terms of service

VZnet Netzwerke Ltd. states in the self-declaration that mechanisms for reporting inappropriate conduct or content are accessible from every page. If the reported content breaches the internal code of conduct, it will

be deleted. Users breaching the code of conduct will be reprimanded, temporally locked or deleted from the platform.

On schülerVZ, there is no general "report button", but links to report offensive content or conduct are placed on every profile, group and picture, thus being easy to find and use. Other users can be blocked, and contact requests can be declined. The information about the criteria and procedures is somewhat less accessible and part of the general safety advice, needing two or three clicks.

schülerVZ provides no direct way to report a particular message that is sent within the internal message system. For the purpose of this test, an internal personal message was sent to one of the members of the community team, asking for help about a scary message. This required some effort (following links through "about us" and "schülerVZ-Team", then clicking on the profile of one of the team members. The team member responded about one week later, asking about the content of the message.

A different way to report an inappropriate message would be to click on the sender's profile and then choose "report user". Testing this mechanism, however, was not part of this evaluation.

Again, there are no huge differences between schülerVZ and both studiVZ and meinVZ. The options for reporting offensive content or users are identical to schülerVZ, so there is also no option to report specific messages or postings as such, but only to report users, groups and pictures.

Principle 5: Respond to notifications of illegal content or conduct

VZnet Netzwerke Ltd. states that, in addition to the above-mentioned reporting mechanisms, it provides special teams assigned to deal with teachers' or parents' requests in respect to schülerVZ. It also cooperates with public authorities or law enforcement agencies especially in cases of political extremism and child pornography.

Information on the reporting mechanisms and the way of contacting the provider are accessible from every page. StudiVZ and meinVZ provide no specific support teams for parents or teachers, but include similar information on every page.

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

For this principle, VZnet Netzwerke Ltd. does not give separate statements but refers to previous statements on the principles 1 and 3 where they mention privacy settings and control of personal data. They provide no statements on particular aspects such as transfer of data from registration process to the profile. None of the three platforms is open for third-party applications.

As mentioned above, registration to schülerVZ requires a previous invitation by another user. In addition to the E-Mail address used in this process, users have to provide their age, their gender, their school and their real name (first and last) in the registration form. Of this, gender, age and real name are automatically transferred to the profile.

Adult users (between 18 and 21 years within the platform; 18 and above from outside) cannot search for profiles of younger users, since they are per default closed, not visible in internal searches and external search engines.

studiVZ and meinVZ require similar information upon registration. In addition to age, e-mail, gender and real name, users have to provide their university (studiVZ) or region (meinVZ). This information is then transferred to the profile, together with name and gender (but not age).

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

For this principle, VZnet Netzwerke Ltd. does not give separate statements but refers to previous statements on the principles 2, 4 and 5 where they mention their support/screening team and the options to report offensive content and conduct. They do not mention aspects such as automated technical control or community alerts. StudiVZ and meinVZ do not differ from schülerVZ in this respect.

Summary of results

VZnet Netzwerke Ltd. addressed three platforms in their self-declarations. While they are very similar with respect to design and functionalities, an important distinction exists: schülerVZ is open for adolescents and young adults only, while studiVZ and meinVZ are targeted at users over 18 years. Accordingly, the main focus of this evaluation has been on schülerVZ.

schülerVZ provides various accessible, age-appropriate and understandable information which is targeted at the main "stakeholders" of the platform: adolescent users, parents, and teachers. Thus, it assists in raising awareness about the communicative mechanisms, acceptable uses and possible risks. By restricting the platform to users between 12 and 21 years, schülerVZ aims to minimize risks that might arise through age-inappropriate content and conduct. Since it does not externally check users' age, the platform cannot prevent, however, that older users will use fake accounts to gain access.

schülerVZ provides various options to modify privacy settings, to manage comments and content, and to delete one's profile. Default settings are more strict on schülerVZ than on studiVZ and meinVZ. All three platforms provide options to report offensive users, groups and pictures. However, there is no way to report offensive messages and postings directly; users always have to visit the offending user's profile page first. A message to a member of the community team of schülerVZ asking for help about a scary message was answered six days later.

Upon registering as a new user, only some personal information is required and even less is included in the starting profile automatically. The information and safety advice deal with the topic of data protection and privacy; schülerVZ even includes user-generated videos in their educational outreach.

Regarding the review of illegal or prohibited content and conduct, all three platforms rely on a combination of user reports and support/moderation. There seem to be no mechanisms for automated control of content installed.

schülerVZ

A. 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				

B. 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			Not Tested		
6	x				
7			Not Tested		

studiVZ/meinVZ

A. 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				

B. 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			Not Tested		
6	x				
7			Not Tested		

YAHOO!EUROPE

Leslie Haddon, London School of Economics and Political Sciences

Introduction

Yahoo! has two services that were evaluated. Flickr is primarily a picture-sharing service i.e. a site for posting one's own pictures and viewing other people's pictures. Users can make their pictures visible to everyone, or just to certain social networks, they can search for their friends' photos and there are various other functionalities. In Yahoo! Answers, users post their own questions about any topic, they may supply answers for other people's questions, they may search for question topics to see what has been covered in the past, they can vote on other people's answers, or, for example, read an Answer's blog.

The reason why both services are included in this test is that both services have some SNS elements, mainly user profiles, but also the opportunity for other users to communicate e.g. in terms of comments regarding pictures posted in the case of Flickr. For both Flickr and Yahoo! Answers the minimum age of users is 13 years old.

This declaration covers the two different services and it is not always specified exactly how issues are handled for each of the services. That said, there were areas in the principles which the self-declaration did not address. As regards tests, Flickr did not have all the elements claimed in the self-declaration (principles 3 and 4), whereas Yahoo! Answers was compliant with its self-declaration.

The principles

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

In the self-declaration, the provider includes information about the terms of use as well as the additional *Community Guidelines* for its different services. Safety information is noted at various places in the document, while the *Privacy Centre*, amongst other locations, provides privacy guidance. The declaration says that because young people gain an understanding of safety issues from peers, the priority is to target information at children. The document notes that this information is shown in a prominent fashion, widely available (typically at the bottom of the page), and presented in a systematic way and easy to understand language. Guidance regarding inappropriate content and conduct is provided, with an indication of the consequences of breaching the terms of service. The provider has also created targeted advice to educate and support parents and carers, although there are no comments that explicitly mention teachers.

Flickr: All the policy statements (terms of use, safety, privacy, code of conduct) are easy to find through links at the bottom of the page. Safety tips aimed at children and parents took a little longer, found via FAQs. There was nothing explicitly addressed to teachers. The advice was always easy to understand for children of various ages and adults, and certainly sufficient in terms of raising a range of issues. Clear examples of the types of content and conduct that will not be tolerated are provided, as is an indication of

the consequences of breaching the terms of conduct (e.g. pictures deleted, account suspended). Of the risky material tested, the Flickr site only explicitly mentions bullying, someone doing something to make me feel uncomfortable (the nearest item to stranger danger) and no nude pictures (the nearest item to porn and sexually provocative photos) – there is nothing explicitly on hate speech (maybe less relevant for a picture site), violence, divulging personal information and images of child abuse: at best, more general comments are contained in the community guidelines.

Overall, since the principle explicitly mentions that providers 'should' supply teachers with material, and there is nothing in the self-declaration (nor anything on the site) explicitly for teachers (only the wider concept of 'carers' who receive the same material as parents), the self-declaration has to be judged partially compliant with the principle. On the other hand, in testing, in general the site does what it claims to do in the self-declaration – e.g. guidance is provided.

Yahoo! Answers: All the policy statements (terms of use, safety, privacy, code of conduct) are easy to find through links at the bottom of the page. Safety tips could also be found there, addressed to children and to parents 'and carers' but not explicitly to teachers. The advice was always easy to understand for children of various ages and adults, and certainly sufficient in terms of raising a range of issues. Clear examples of the types of content and conduct that will not be tolerated are provided, as is an indication of the consequences of breaching the terms of conduct (e.g. account terminated). The declaration mentions most of the items listed in the test (hate speech, porn, violence, bullying, stranger danger, divulging personal information and posting sexually provocative photos), but not self-harm.

Overall, since the principle mentions that providers 'should' supply teachers with material, and there is nothing explicitly for teachers (nor anything on the site distinct from the material for parents), the self-declaration has to be judged partially compliant with the principles. On the other hand, in testing, in general the site does what it claims to do in the self-declaration.

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

It is made clear in the self-declaration that community services (such as Yahoo! Answers and Flickr) are not appropriate for children under 13, but since the declaration covers different services, it is not specified how the minimum age is made clear to users (given that this detail varies by service). The self-declaration states that there are steps to deny access to under-age users (although it does not say what the steps are – but again, this may vary by service). It does, however, state that the profile of anyone discovered to be under-age (i.e. who lied about there age) will be deleted. One mechanism to support compliance with the minimum age requirement is that the date of birth originally provided cannot be modified, although there is no mention of further steps to prevent those users re-registering. We are told in the self-declaration that advice and material for parents is provided and where ('help pages'). The provider indicates the user flagging system (as well a company reviewers and technical solutions) to counter inappropriate content. As regards contact, the provider notes the profiles are not, in any case, as developed as in dedicated SNSs and not searchable, but there are a number of other mechanisms in place to make these private, safety messages about posting content and the ability to block contact.

Flickr: It is clear on the Flickr site that the minimum age is 13, and when registering for a Yahoo! account applicants have to give date of birth (although there is no email verification system). At the next stage,

correctly, Flickr rejected the attempt to sign on as an 11 year old, with the message that the applicant was under 13. Since the 11 year old Yahoo! details could not be changed, as noted in the declaration, a different age and name for a new Yahoo! account was submitted, and the user was able to go onto Flickr as a 15 year old – so the user could have been an 11 year old pretending to be a 15 year old.

Overall, the provider has reacted to some suggestions in the principle, and so the declaration has to be judged complaint with the principles. In terms of testing, the mechanism for blocking under-age age access could be better, but since it did what was claimed in the self-declaration to must be judged compliant.

Yahoo! Answers: As in Flickr, it is clear on the Yahoo! Answers site that the minimum age is 13, and when registering for a Yahoo! account applicants have to give a date of birth. Even a person registered as an 11 year old can view questions, but when such a user tries to react to them, correctly, Yahoo! Answers did not allow this saying the person was not old enough. Since the 11 year old Yahoo! details could not be changed as noted in the declaration, as in the test for Flickr, a different age and name for a new Yahoo! account was submitted, and the user was able to go onto Yahoo! Answers as a 15 year old – so the user could have been an 11 year old pretending to be a 15 year old.

Overall, while the provider has reacted to some suggestions in the principle, and so the declaration has to be judged complaint with the principle. In terms of testing, the mechanism for blocking under-age age access could be better, but since it did what was claimed in the self-declaration to must be judged compliant.

Principle 3: Empower users through tools and technology

The document states that under 18 profiles are not searchable and default to private. There are safety messages about connection invitations, and means to block (or advice to ignore) such requests. The declaration says nothing about posting comments on profiles because on neither service can you do this, nor about posting comments on photos (applicable on Flickr). The document notes that there is an easily identifiable (and in practice easy to use) '*report abuse*' flag for dealing with inappropriate contact (and conduct is implied). The declaration indicates that it has developed advice and guidelines for parents/carers.

Flickr: As specified in the self-declaration, under 18 profiles are not searchable. Users can block others (or rather 'specific others', not defining which groups - e.g. age groups - can make contact). Some, limited, parts of the profile appear to be visible to all by default (user name, when he/she joined), while others are by default only visible to my friends (email and IM names). The default is to show posted photos, including photos posted by minors, to everyone and allow all comments, although users can change this setting, while notes and tags are by default allowed only by one's contacts. Comments are about photos rather than profiles. Reporting is discussed under the next principle. There does not seem to be advice for parents on the Flickr site (even if there is advice on the Yahoo! site the information is not replicated on or easily accessed from Flickr), and the provider notes that Flickr does not offer tools for parental controls.

In sum, various steps have been taken to address principle 3 and so the provider must be judged compliant with the principle. In testing, the advice for parents noted in the declaration that relates to the Yahoo! Help pages is missing from the Flickr site and so the site must be judged partially compliant with the self-declaration

Yahoo! Answers: As specified in the self-declaration, under 18 profiles are not searchable. Users can block others (though it is rather 'specific others', it is not clear if they can define which groups can make contact). The profile is by default visible to my friends, though it can be changed to be visible to all. If the users wants to add to his/her profile the system suggests using a nickname to protect your privacy. Information about parental controls was easy to find via *Safety Tips* at the bottom of the pages where there are questions.

In sum, various steps have been taken to address principle 3 and so the provider must be judged compliant with the principle. In testing, the site provided what was claimed in the self-declaration and so is compliant.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the terms of service

The self-declaration notes that there is a 'report abuse' button to report inappropriate content, contact or behaviour, a button that is always accessible by virtue of being on every page. It does not specifically add that the mechanism is easily understandable (although it is in practice) or age appropriate. The declaration says that that reports receive an automated response and are acted upon in a timely way, typically being resolved within 48 hours. It does not say that the users are provided with the information they need to make an effective report (but there is no need since the options are clear in practice). It does say how, in general, reports are handled.

Flickr: Users can report inappropriate contact and conduct via the *Report Abuse* link at the bottom of the page, which leads to various options about what to report. The reporting tool is easy to understand, including for children, but the user has first to realise that the mechanism is at the bottom of the page. The user is offered various options – the user does not write a message, but picks from choices (which means that the actual wording of the test could not be used). When clicking on the report *'behaviour of another Flickr member is making me feel uncomfortable'* option, for example, the system suggests that you block anyone who is troubling you and tells you the consequences of doing so – but it did offer the option to send off an actual report and there was no feedback from the system that any report had been sent. However, if the user reports the content of a picture, the system notes the page details and provides a message that this report is in a queue to be reviewed.

Overall, the self-declaration is compliant with the principles (even if it does not explicitly mention that all questions will get an answer). In testing, there is a clearly worded reporting mechanism that does report problematic content. But since the system does not actually send off a report if you try to report contact this service must be judged to be partially compliant as regards this issue.

Yahoo! Answers: Users can report both inappropriate contact and conduct via the *Report Abuse* link that appears when the users look at particular questions. The information seems more geared up to reporting any content within the questions that infringe rules, but you can report contact if the person answering is ranting, insulting, threatening or harassing you, for example. It is clearly worded, visible and easy to understand. The system offers the person making the report various options, including the reporting of unwanted contact – the user does not write a message, but instead picks from choices (which means that the actual wording of the test could not be used). There is notification when a report has been sent (the system thanks you for reporting) and there is information about general next steps (e.g. under what conditions the question might be removed).

Overall, the self-declaration is compliant with the principles (even if it does not explicitly mention that all questions will get an answer). In testing, Yahoo! Answers is partially compliant, since "acting upon" a

complaint needs to include some form of feedback to the person making the complaint. In the present case, that could include a request for further information from the complainant, a reference to a help page or a response stating that the complaint was not being taken further. Here there was only an acknowledgement and general information.

Principle 5: Respond to notifications of Illegal content or conduct

The self-declaration does not explicitly say that processes are in place to review and remove content - but it does say that that reports are '*acted upon*'. It does indicate arrangements are in place to share reports of illegal content with law enforcement bodies and that there are links with hotlines (e.g. Inhope).

These measures were not tested in Flickr or Yahoo! answers, but if they are in place then the provider has to be judged compliant to the principle for both services.

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

Yahoo! makes it clear that the profile pages on its services are not the same as standard SNS ones, but are more like 'user cards' containing limited information that 'does not prompt the sharing of personal details'. The self-declaration says nothing about providing users with information to make informed decisions about what they post online, but users may change their privacy settings at all times. While there are no comments on the implications of automatically uploaded registration information for profiles, notification to users that this information is used in profiles and the ability of users to edit this information, to put this into perspective, the initial profiles on Flickr and Yahoo! Answers are very limited

Flickr: A user can check and change the privacy setting in *Your Account* at any time. On registering for a Yahoo! account, the user provides information about age (birthday), gender, postcode (which almost identifies address), first and last real names and an alternative email address. The user is not warned at this point how information might be used in the profile. When signed up for Flickr the profile automatically reveals just the user name and when they joined. Any extra information later volunteered (e.g. real name, gender, hometown, description of yourself, email address) is also revealed.

In sum, the provider has to be judged compliant with the principles, given that the initial profiles generated are very limited. From the tests, while it would be better if the user were informed about what information would appear on the profile when registering, it is subsequently clear that very little information about the user is provided on the profile by default. And since in privacy settings can also be easily viewed and changed, the provider is in compliance with the self-declaration.

Yahoo! Answers: As in Flickr, the users can check and change the privacy setting in *Your Account* at any time. As noted above, on registering for a Yahoo! account, the user provides information about age (birthday), gender, postcode (which almost identifies address), first and last real names and an alternative email address. The user is not warned at this point how information might be used in the profile. When signed up for Yahoo! Answers the profile automatically reveals just the user name, when the user joined the service and some other data about questions asked and answered. Users can volunteer descriptions of themselves and photos if they wish.

In sum, the provider has to be judged complaint with the principles, given that the initial profiles generated are very limited. From the tests, while it would be better if the user were informed about what information would appear on the profile when registering, it is subsequently clear that very little information about the user is provided on the profile by default. And since in privacy settings can also be easily viewed and changed, the provider is in compliance with the self-declaration.

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

The provider states that it employs automated solutions to check content as well as human review (e.g. on Flickr). Users receive automated responses confirming the receipt of a complaint. There is no comment on the steps taken to vet any human moderators but this reflects the fact that staff do not have real time one-to-one contact with children.

Based on the limited information in the declaration that there are multiple systems in place, both services must be judged compliant to the principle.

Summary of results and conclusion

Since one declaration covers two services sometimes it can be difficult to be too specific in the self-declaration because an issue is handled slightly differently in each service. That said, there were areas in the principles which the self-declaration did not address. As regards tests, Flickr did not have all the elements claimed in the self-declaration (principles 3 and 4), whereas Yahoo! Answers was compliant with its self-declaration.

Flickr

A. 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				

B. 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			*Not Tested*		
6	X				
7			*Not Tested*		

Yahoo! Answers

A. 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				

B. 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			*Not Tested*		
6	X				
7			*Not Tested*		

ZAP.LU

André Melzer, Université du Luxembourg

Introduction

ZAP is a free-access social networking website (*"community platform"*) in Luxembourg for people aged 13 and above. Due to the three main languages that are spoken in the country, ZAP offers a Luxembourgish, German, and French version of the site. It provides information on event schedules, nightlife reports, user profiles, homepages, and photos. ZAP users may present and describe themselves for social purposes using public messages, friend lists, a mailing system, and picture and video upload functions.

The implementation of the Safer Social Networking Principles was tested on October 26th, 27th, and 30th 2009. Tests were conducted using the Luxembourgish version of ZAP. Testing revealed that ZAP implemented Principles either partially of fully. Some aspects that were announced in the self-declaration as being in preparation are still awaiting implementation (e.g., guidelines for parents and carers). Other important aspects of the self-declaration were found not to work properly (e.g., age-control system, feedback to reported harassment).

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

The self-declaration contains several details on measures that the SNS provider is taking in order to comply with Principle 1 on raising awareness of safety education messages. The self-declaration contains information on Terms of use, but not on privacy. With regard to safety information the SNS provider claims *"ZAP is actually working out a guide for school personnel and parents"*. Collaborations of the SNS provider and several youth services ("Service national de la jeunesse"), as well as Internet safety organizations ("LISA Stop Line"), are also mentioned.

The SNS website itself provides a mixed picture, though. Information like Terms of use, safety policy and privacy policy is easily accessible. Surprisingly, and unlike safety policy and privacy policy, Terms of use is available in German and French only, but not in Luxembourgish. The website provides users with a link to the *National Commission for Data protection*. In addition, there is explicit information on both content and conduct that is not allowed on the social network. Likewise, the consequences of engaging in prohibited behaviour and/or actions are clearly stated. Neither the aforementioned guide for teachers (see also Principle 3) nor any web link to the organizations that were mentioned in the self-declaration form may be found on the website. General information for parents is not available separately, but included in the guidelines for teenagers. Also, there is no information on specific risks while using the social network. This is also true for the PDF files containing safety-relevant tips that were mentioned in the self-declaration. However, these tips are available as online information.

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

In the self-declaration the SNS provider states that only people aged 13 and older may fully access the social networking community. It is also mentioned that age-appropriateness of advertising will be ensured through the use of cookies. However, the self-declaration does not provide information on what kind of information on the website is age-inappropriate, how under-age users are prevented from accessing the SNS, or if parental controls are promoted. In addition, although the self-declaration outlines that exposure to potentially inappropriate content will be limited through the use of buzz word filters, there is no indication of how inappropriate contact may be prevented.

When signing up as an adult on the SNS website, ticking a box that indicated accepting the Terms of use is required. Entering the birth data of an 11-year old child leads to a rejection of the user during registration. However, simply changing the year of birth from 1998 to 1994 leads to successful signing up. The age control system appears to be largely ineffective, because it may easily be outmanoeuvred even without having to delete cookies or using a different e-mail address. Younger children are thus not prevented from having access to large parts of ZAP. Hence, they may become exposed to information that is either inappropriate, or that parents may find offensive. In addition, parental control tools are missing on the SNS.

Principle 3: Empower users through tools and technology

With regard to empowering users, the self-declaration lists numerous ways how the SNS provider supports this. Users may put unwanted other users to an *"Ignore List"* and manage their own profile and homepage by restricting access to certain sections. They may also delete unwanted comments, prevent posting of public messages on their profile, and report unsuitable behaviour. There are no comments on how users may report unwanted contact or how profiles may be deleted. There is also no information on how parents may be educated about available tools on the website that help them to protect young people (see also Principle 1). With regard to age restriction, profiles and homepages of registered users under the age of 16 are not searchable on ZAP. This is also true for browsing user pages, which is not possible for users aged 13 to 16.

During testing, it was observed that the ZAP website offers many tools that empower users. This includes specifying user groups that may or may not contact the user (i.e., blocking function), as well as specifying actions with regard to individual profile availability or accessibility. When signing in to the test user profile, Zap's "greeting message", which is displayed in the user profile (but not send as a separate email) includes information on safety tips and/or guidance about publishing personal information or photos to the profile. However, it was observed that default settings render personal information visible to all other users, such that restricting the visibility depended on the account owner's activity. In contrast, deleting a profile is supported by a dedicated web link together with easy-to-understand "how-to" information. No information was found what personal information the SNS provider will store once the profile is deleted.

Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the terms of service

In the self-declaration form, the SNS provider indicates that there is a *"Report"* button on the top of every page. However, there is no information on age-appropriateness or understandability of the reporting procedure. In addition, there is no indication how to make an effective report, how reports are typically handled, or that reports are acted upon expeditiously.

Testing revealed that the *"Report"* button is not located on the top of every ZAP page, but only on the top of non static pages like, for example, personal pages. The *"Report"* mechanism is difficult to understand for children and young people, but may be found easily and quickly. Most importantly, however, asking for

help with the standard message *"Someone is sending me scary messages (…)"* remained without consequences; there was no notification/receipt that the report was sent to the SNS provider, and no information on how the report will be dealt with. Therefore, a second report with the same help-seeking message was sent two days later. Again, there was no feedback from the provider.

Principle 5: Respond to notifications of illegal content or conduct

The self-declaration of the SNS provider indicates that illegal contents and conducts will always be reported to the law enforcement. The reader is also informed about consequences of rule infractions (i.e., warnings or exclusion of the profile from the ZAP website). Yet, the self-declaration does not indicate which particular processes will take place when the provider is informed about alleged illegal content or conduct.

When using the SNS after signing in to an individual user profile, clear information is given on where to report other users or bothering content. This is also true for blocking functions (e.g., blocking a friend or a contact request) and the so-called *"Report"* button (see also Principle 4).

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

According to the self-declaration the SNS provider clearly states that users will be provided with a range of privacy setting options. In particular, users can manage themselves how many details they want to publish about their own person. In addition, they are also encouraged not to reveal any private information. On the other hand, the self-declaration does not contain any practical information like, for example, that privacy options are accessible at any time, or that users are able to view their privacy status or settings at any time.

When signed in to the test user profile (as a 15-year old user), changing privacy settings is easy and always possible. Also, third-party applications will be installed only after previous permission of the test user. For the initial step of the first-time registration process, entering E-mail address and individual password is sufficient. Next, a so-called *"profile configuration"* window appears. Mandatory personal information comprises first and last name, date of birth, as well as the user's hometown and land/region, but not home address or nationality. Other information is either optional (e.g., gender, nickname, picture of the user), or not mentioned at all (e.g., school/workplace, phone number, personal security number, religious orientation). The initial profile configuration also includes checkboxes on adult-relevant information like, for example, user's sexual orientation, marital status, name of the partner, and main interests of using the SNS. Providing this information is surprising, because the self-declaration indicated that users are encouraged not to reveal any private information. Following registration, real name or nickname is automatically inserted into the user profile, depending on the user's previous decision, together with information on age, gender, and user's hometown. E-mail is not visible, though. Sexual orientation, marital status and main interests are also displayed on the profile page. A look at privacy settings reveals that by default all information is visible to "everyone" unless the user restricts visibility. Again, this is in contrast to Principle 6 that only the name and the age will be shown per default. After signing in as an adult user, searching for profiles of users aged 16 is possible, but not for the 15-year old user. Also, no search results are rendered for profiles of users who are 12 years old or younger. These observations are in line with the self-declaration of the SNS provider.

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

In the self-declaration form the SNS provider indicates that it employs some form of moderation, namely a daily check of all uploads performed by the SNS administrators. A content that does not correspond to the Terms of use will be immediately removed. In addition, buzzword filters (see Principle 2) serve as technical tools to control for potentially illegal or prohibited content. With regard to real-time contact with

children/younger user the SNS provider indicates in the self-declaration that they count the frequency with which adults contact minors. Great age differences between corresponding users as well as suspicious behaviour are supposed to lead to investigations of the profiles in question. There is no indication through which kind of technology or service this will be achieved. Finally, there is no indication in the self-declaration whether or not ZAP uses human moderators, or if attempts will be made to avoid real-time contacts between children or young people and candidates, who are unsuited for this kind of work. As was already mentioned with Principle 5, there is no indication in the self-declaration that the SNS provider responds to user-generated reports. Also, there is no indication whether ZAP includes a "community alert function".

Summary of results and Conclusion

Testing revealed that there was full compliance between three Principles (i.e., 1, 3, and 6) and the self-declaration from the SNS provider of ZAP. In contrast, only partial compliance was observed with Principles 2, 4, 5, and 7. With regard to ensuring that services are age-appropriate (Principle 2), the self-declaration lacks information on parental controls and preventing under-age users from accessing the SNS. In addition, the self-declaration does not contain information on how to make an effective report of inappropriate conduct or content, and how reports are typically handled (Principle 4). There is also no information on how the provider will respond to notifications of illegal content or conduct (Principle 5), and how reviewing illegal or prohibited content/conduct will be done (Principle 7).

Testing also showed that, except for Principle 3, not all aspects of the self-declaration have been fully implemented on the SNS website yet (Principles 1, 2, 4, and 6). For example, the currently built-in functions in ZAP appear to be insufficient to prevent minors (i.e., children younger than 13) from accessing information on SNS websites (Principle 2). Testing also revealed that even without having to delete cookies simply changing the year of birth was sufficient to outmanoeuvre the registration barrier. In addition, the SNS website is currently lacking information for children and carers, as well as links to educational material. Finally, it is important to note that there was no feedback at all following two reports on harassment sent to the SNS provider, casting serious doubts on the belief that such reports will be treated timely and adequately by the provider of ZAP (Principle 4).

In sum, testing leads to the impression that the ZAP website is currently predominantly focusing on adult, or at least "older", users, which are given many options. With regard to minors, but also parents and teachers, however, testing revealed that several shortcomings need to be addressed to make the ZAP website fully compliant with the Safer Social Networking Principles for the EU.

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			Insufficient age control system
3	X				
4		X			No feedback to reported harassment
5	*Not Tested*				
6		X			
7	*Not Tested*				

For further information:
Directorate-General
Information Society and Media
European Commission
Safer Internet Programme
E-mail:
saferinternet@ec.europa.eu
Fax: + 4301 34079
Office: EUFO 1194
European Commission
L-2920 Luxembourg

http://ec.europa.eu/saferinternet