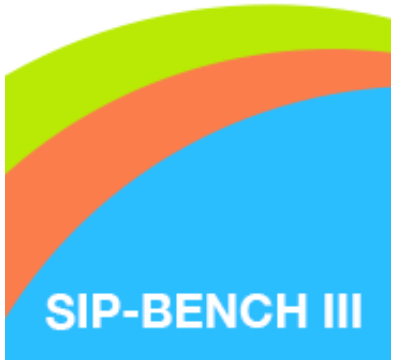


Benchmarking of parental control tools for the online protection of children

SIP-Bench III

3rd CYCLE STUDY REPORT

Assessment results and methodology

SAFER INTERNET PROGRAMME

Empowering and Protecting Children Online

The Study Report has been prepared by Cybion Srl and Stiftung Digitale Chancen, coordinated by INNOVA Srl for the European Commission Directorate General for Communications Networks, Content and Technology in the framework of the SIP-BENCH III project (**Benchmarking of parental control tools for the online protection of children)**, funded by the European Union, through the "Safer Internet Programme" http://ec.europa.eu/saferinternet.

The document reports the results of the 3rd testing cycle carried out during the year 2014. At this stage, some of the findings of this report may be outdated. However, after a long interruption of project activities, due to a suspension required by the European Commission, the project has been re-opened and a new testing cycle is now on-going on an updated list of tools. The main results of this 4th testing cycle will be released in early 2017 to the European Commission and published online by April 2017.

Main contact for the project and the study:

Antonella Vulcano
a.vulcano@innova-eu.net
INNOVA Srl
Via Giacomo Peroni, 386
00131 Rome - Italy

Table of content

INTRODUCTION

Objectives

The present report is the 3rd out of four reports that will be published in the framework of the *SIP-Bench III* – "*Benchmarking of parental control tools for the online protection of children"* project, funded by the European Commission in the framework of the Safer Internet Programme in the period 2013-2017.

The study is a vendor/supplier-independent comparative expert assessment of 'parental control tools' with the objective:

- To provide the end-users (notably PARENTS) with a detailed overview of the existing parental control tools benchmarked according to the identified needs.
- To support the end-users (notably PARENTS) to choose the most appropriate parental control tools best matching their specific needs.
- To raise awareness about tools that help protecting children and teenagers from Internet threats.

The report aims at guiding the end-users in a simple way through the assorted panorama of parental control tools available on the market.

The Internet has grown quickly in recent years: young people and children are today amongst the biggest user groups of online and mobile technologies in Europe.

The Safer Internet Programme aims at empowering and protecting children and young people online by awareness raising initiatives and by fighting illegal and harmful online content and conduct.

Parental control tools allow parents to manage and restrict the content that their children may access while surfing the Net through PC or mobile devices. They can block or filter content, or simply offer control over a child's activity on the Internet.

The results of the study will also be available online through a downloadable report and a searchable database that allows extracting ranking lists of tools to help and guide users in the decision making process according to their specific needs.

SIP-BENCH III TESTING CONTEXT

What are parental control tools?

One of the biggest concerns parents have about the internet is the kind of websites their children are browsing and the content they may be viewing. It is therefore important to empower children and young people to use online media safely and responsibly. In addition, there are software and other instruments that can be used to help protect children.

Apart from the clear advantages and opportunities, the Internet carries also threats to CHILDREN and TEENAGERS: from access to inappropriate content (e.g. pornography, violence, self-harm and illicit act incitement) to exposition to online predators and to dangerous behaviours of which they can be victims or authors (e.g., sexting, cyberbullying, pedophilia).

Today the market provides PARENTS with numerous instruments to support protection of their CHILDREN/TEENAGERS from such threats. They are known as '*PARENTAL CONTROL TOOLS*'.

It is possible to use a parental control tool in three different ways:

- ☞ Install software on the PC or download an app on the mobile devices;
- ☞ Subscribe to an online filtering service. In this case, there is no need to install it on the PC. It is offered by many ISPs (Internet Service Providers);
- ☞ Combine both solutions.

Once the tool is operative, PARENTS can:

- ✓ Customise Web content filtering: PARENTS may ask the tool to block or to show content indicating the topic, a list of URLs or some specific keywords. PARENTS may also set a level of filtering (low, medium, high)
- ✓ Block the usage: PARENTS may block the usage of some applications (for instance, Skype or Peer to Peer applications)
- ✓ Monitor: PARENTS may receive reports on the activity of CHILDREN/TEENAGERS in the Internet, getting information about the sites that have been accessed or blocked, which applications have been used, etc.

The first element PARENTS should consider is the device used by the CHILDREN/TEENAGERS to access the Internet. Apart from PC/Mac, which is still the most common device, mobile devices and game consoles are increasingly used by youngsters to access the Internet.

SIP-BENCH III has conducted a third cycle of vendor/supplier independent benchmarking tests on selected tools differentiated by access device as it follows:

- 10 PC/MAC parental control tools
- 10 parental control tools for mobile devices
- 5 so called “Alternative” parental control tools.

Due to the lack of updates, game console tools were not tested in the third cycle.

During the tests, content sent or received by the CHILDREN/TEENAGERS (e.g.: the content of e-mails received, or the information published by TEENAGERS on Facebook) was not taken into consideration. Filtering of such content would violate privacy rights.

What are the main criteria for choosing a tool and type of tests carried out?

The criteria guiding the selection of the most appropriate tool are different according to the parents' specific concerns that may be grouped into the following main categories:

- Viewing/producing **inappropriate content.**
- Being a victim/author of a **harmful communication.**
- Spending too much time on the Internet or using certain **applications/protocols.**

SIP-BENCH III has identified the following four main categories of users' needs:

One unique perfect tool does not exist: every PARENT should look for the tool that best matches his/her needs, by finding the balance among functionalities offered, effectiveness, security and usability performance.

Table 1 – USERS' NEEDS

Test Type	What it consists in	Where the results are synthesized
FUNCTIONALITY	It assesses which functionalities the tool provides - Does the tool offer the functionality you need? For instance, is there a functionality to block the access to social networks? Is it possible to have a different level of filtering for your 7-year-old daughter and your 16-year-old son?	Functionality tables
SECURITY	It assesses the tools resistance to the users' attempts to by-pass it by means of specific actions. Is it easy or difficult for your CHILD to uninstall or by-pass the tools and access the Internet freely?	Functionality tables dedicated column
EFFECTIVENESS	It measures how each tool blocks harmful content and allows non-harmful content. Does the tool block 50%, 75% or 90% of pornographic/violent websites? Does the tool allow your CHILD to visit acceptable websites?	Effectiveness tables
USABILITY	It assesses if it can be easily installed, configured, used and maintained by average user. Will it be easy/difficult/almost impossible to install and configure the tool?	Usability tables

In order to have more details of the needs and related testing criteria users may also read:

- Tools specific and **detailed fiches** (more detailed information is available, especially for functionalities and security at http://sipbench.eu/results)
- The **Methodology Key Issues** section at the end of this report.

In the following tables in relation to the four users' needs a certain number of areas of needs have been identified and briefly described.

Table 2 - FUNCTIONALITY NEEDS

Area of Need	Description
COMPATIBILITY	If you already have the device, you have to check whether the tool is compatible with the related operating system (e.g., Windows, Mac OS, Linux) and the related version (for instance Vista, 7, 8).
DIFFERENT USERS	If the access to the device is open to more than one CHILD/TEENAGER with different filtering needs, you need to create and manage more than one user with specific and customized features.
CUSTOMIZATION OF FILTERING	If you have specific needs with regards to content to be filtered (topics, specific URLs white and black list). This might be useful when you are particularly concerned by certain topics, wish to restrict your CHILDREN/TEENAGERS navigation to safe websites and block the others.
KEYWORDS	If you are particularly concerned with some words that your CHILDREN/TEENAGERS may find in content (webpages and communication messages).
TIME RESTRICTION	If you are worried about the time your child spends in the Internet (whether browsing, playing or communicating).
USAGE RESTRICTIONS	If you are interested in deciding which actions the CHILDREN/TEENAGERS can perform on the Web and when. The main actions are available due to specific protocols/applications. That is why it is important to understand if the tool enables you to control such protocols/applications. The type of control considered within the test is the following: block/monitor. You might want to block the access to the Web (thus leaving the access to other device functionalities open to the CHILDREN/TEENAGERS) or to specific applications/protocols that allow: o Surfing the Web (WEB ACCESS). o Watching/listening to video/images/music in streaming (STREAMING through the Web). o Sharing content by uploading or downloading (P2P).
USAGE RESTRICTIONS RELATED TO COMMUNICATION ACTIVITIES	The **inward/outward communication activity** constitutes one of the PARENTS increasing concerns. The communication/networking tools are an opportunity to make CHILDREN/TEENAGERS share their opinions and find new friends but there is also a risk: CHILDREN/TEENAGERS could easily come into contact with malicious or potentially dangerous people that profit from the anonymity granted by the username or they could **be the actors of bullying, sexting or** performing malicious actions **themselves**. In this case you could wish to block or monitor the access to the following applications/protocols that allow: chatting and sending instant messaging or email to specific contacts – e.g. **Skype, Live Messenger** (Instant Messaging), email client e.g. Outlook, Thunderbird or webmail provider, e.g. Yahoo!, Gmail.

Table 3 - SECURITY NEEDS

Area of Need	Description
SECURITY	Today, especially TEENAGERS could be able to by-pass or uninstall the tool. Depending on your CHILD´s computer skills, you should choose the tool also considering its resistance to various type of violations, such as: o By-pass the tool accessing the prohibited pages through: using the IP address, proxy websites, online translation service (e.g., Google Translate), the Google Cache, an alternative browser. o By-pass the tool: changing the time settings (if time limit usage restriction is applied).

Table 4 - EFFECTIVENESS NEEDS

Area of Need	Description
TOPIC of CONTENT	You might have different needs in terms of topics to be filtered and should choose the most effective tools accordingly.
UNDERBLOCKING/OVERBLOCKING	Each tool faces two problems: 1) blocking non-harmful pages (overblocking); 2) allowing harmful pages (underblocking). You may decide to give more importance to overblocking or underblocking. For instance, for a child you may prefer to ensure a good filtering of harmful content even if many non-harmful content is blocked, while for a teenager you could prefer to give him/her a wider access to Internet even if more harmful content is not blocked.
AGE	According to their age, children and teenagers have different needs in terms of content to be filtered. Some tools may have a different efficiency according to these needs. The tool effectiveness was verified according to two different classes of **age: ≤ 12 and ≥ 13 years old.** (more details in the section *Methodology key issues*).
LANGUAGE	The interface of the tool needs to be available in a language you are confident with. The tool should also be able to accurately filter the content in the language children and teenagers use most.
WEB 2.0 and WEB	With growing Web 2.0 (blog, forum, YouTube/daily motion, social networking), the risk for CHILDREN/TEENAGERS to come into contact with inappropriate material produced by “unchecked” sources has increased. You should be aware of the kind of content mostly accessed by your children when configuring the tool.

Table 5 - USABILITY NEEDS

Area of Need	Description
INSTALLATION	You might want a short installation process or no installation at all. You should be able to understand and manage the installation process quite well, i.e. choose between installation for beginners or advanced users.
CONFIGURATION	You might want to set up different degrees of strength of filtering. Also, you might have different sensibility regarding different types of content. You might want to transfer filter configuration between different users or devices. The overall process should be comprehensible, conform with your expectations and be easy to learn.
USAGE	The alert message in case of blocking should be understandable for children as well as for their parents. You might want to have an option to choose between different reactions in case the tool blocks a website. You might want the tool to support you in your education and help your children understand why the parental control tool is in operation. Not every tool offers a reporting function. Nonetheless, reporting should be easy to handle and understand.

PARENTAL CONTROL TOOLS FOR PERSONAL COMPUTERS

FINDINGS FOR
FUNCTIONALITY, SECURITY, EFFECTIVENESS, USABILITY

PCs and the Internet

The PCs are the most common way to access the Internet. They enable CHILDREN/TEENAGERS to access Web pages, share experiences and contents through social networks and communicate with people.

PC PARENTAL CONTROL TOOLS: Functionality key findings

- ➔ **None of the 10 tested tools[1] reaches the complete functionality coverage. The most complete one covers 80 %.**
- ➔ **Seven tools reached 77 % functionality coverage.**
- ➔ **Six tools are rated under 50 %.**

The **3 highest scoring products** are:

- PURESIGHT OWL (77 %)
- Norton Online Family, OPTENET PC and QUSTODIO (53 %), and
- TREND MICRO ONLINE GUARDIAN (47 %)

Customisation of Web content filtering

- Most of the tools provide the parent with the complete set of customisation functionalities (topic and URL black/white lists)
- Keywords filtering option is uncommon: only 3 tools offer this option. 9 tools give the possibility to block access to social networks, and
- 7 tools give the possibility to force the user to use the Safe Search functionality of the most common search engines.

[1] Functionality results for NetNanny are not available as it was not possible to install the tool.

Protocols and Applications The tools rarely provide the option to block an **entire protocol** whereas blocking **applications** is more common.

Management of users' profiles Most of the tools enable the parent to create and manage different profiles for users with different needs. One tool can be used only with one profile. Remote Management is possible in 5 tools.

Restricting Web access All tools enable parents to block the access specifically to the Internet (whether using a specific functionality or using the "time restrictions").

Streaming The majority of the tools are able to block Web based streaming provided by YouTube, if not with a specific option, at least by adding it to a black list. Blocking the specific application which allows streaming such as Windows Media Player is possible for seven tools.

Communication activities One tool is able to block Windows Live Messenger and two are able to block Skype. If tools are able to block Skype and/or MSN, they block it with respect to the whole application and it is not possible to limit the blocking to Voice Over IP (VoIP) or Video chat only.

Monitoring Most of the tools are able to provide the parent with at least a basic report on the user's web activity (visited websites or violations). Four tools allow remote access to monitoring.

Language Interface English is the most frequent language whereas the choice of tools is limited for many other European languages.

Security Some tools present some security weaknesses. The most common is allowing access to a prohibited page through translation sites or Google Cache. Few tools can be uninstalled without a password.

Table 6 - PC Tools FUNCTIONALITY results and overall functionality and security score

Area of need	Usage Restriction															
Functionality	Email	P2P		Personal data Provision	Safe search	Skype		Social Networks		Streaming		Web		Windows Life Messenger		
Specific Issue	Block email client and/ or webmail access	Block the appli-cation	Monitor Downloads	Block	Avail-ability	Block chat	Block video chat	Block Access	Monitor Usage	Block Access	Monitor Access	Block Access	Monitor Access	Block chat	Block video chat	Monitor
F-Secure Internet Security	N	N	N	N	Y	N	N	Y	N	N	N	Y	N	N	N	N
K9 Web Protection	Y	Y	N	N	Y	N	N	Y	N	Y	N	Y	Y	N	N	N
Mac Os X Parental Controls	Y	N	N	N	N	Y	Y	N	N	N	N	Y	Y	N	N	N
McAfee All Access	N	N	N	N	N	N	N	Y	N	Y	N	Y	Y	N	N	N
Norton Online Family	Y	N	N	Y	Y	N	N	Y	N	Y	N	Y	Y	N	N	N
Optenet PC	Y	Y	N	N	Y	N	N	Y	N	Y	N	Y	Y	Y	Y	N
Panda	Y	Y	N	N	N	N	N	Y	N	N	N	Y	Y	N	N	N
Puresight Owl	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N
Qustodio	Y	N	N	N	Y	N	N	Y	Y	Y	N	Y	Y	N	N	N
Trend Micro Online Guardian	Y	Y	N	Y	Y	N	N	Y	N	Y	N	Y	N	N	N	N
% of tools with function	80 %	50 %	10 %	30 %	70 %	20 %	20 %	90 %	20 %	70 %	10 %	100 %	80 %	10 %	10 %	0 %

Table 7 - PC Tools FUNCTIONALITY results and overall functionality and security score

Area of need	Management			Filtering Customisation					Keywords			Time	Blocking Message			Security
Functionality	Management of User profiles	Monitoring	Remote Management	Topics	URLs Black List	URLs White List			Keywords			Time Limit Settings	Type			Score
Specific Issue	Create several profiles	Remote access to monitoring	Manage on various devices	Customisation of Filtering Topics	Creation of User's own Black List	Default White List	Modification OR Creation	Restrict Browsing to White List	Creation of a User's Black List	Creation of a User's White List	Default Black List	Set a specific time frame or web access duration	Ask for un-blocking by parents	Redirect to safe re-sources	% function coverage	
F-Secure Internet Security	Y	N	N	Y	Y	N	Y	Y	N	N	N	Y	N	Y	33 %	1
K9 Web Protection	N	N	N	Y	Y	N	Y	N	Y	N	N	Y	N	N	40 %	3
Mac Os X Parental Controls	Y	N	N	N	Y	Y	Y	Y	N	N	N	Y	N	Y	40 %	2
McAfee All Access	Y	N	Y	Y	Y	N	Y	N	N	N	N	Y	N	N	33 %	0
Norton Online	Y	Y	Y	Y	Y	N	Y	N	N	N	N	Y	Y	Y	53 %	1
Optenet PC	Y	Y	N	Y	Y	N	Y	N	Y	N	N	Y	N	N	53 %	3
Panda	Y	N	N	Y	Y	N	Y	N	N	N	N	N	N	N	30 %	0
Puresight Owl	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	N	N	77 %	4
Qustodio	Y	Y	Y	Y	Y	N	Y	Y	N	N	N	Y	N	Y	53 %	4
Trend Micro Online Guardian	Y	N	Y	Y	Y	Y	Y	N	N	N	N	Y	N	N	47 %	0
% of tools with function	90 %	40 %	50 %	90 %	100 %	20 %	100 %	40 %	30 %	10 %	0 %	90 %	10 %	40 %		

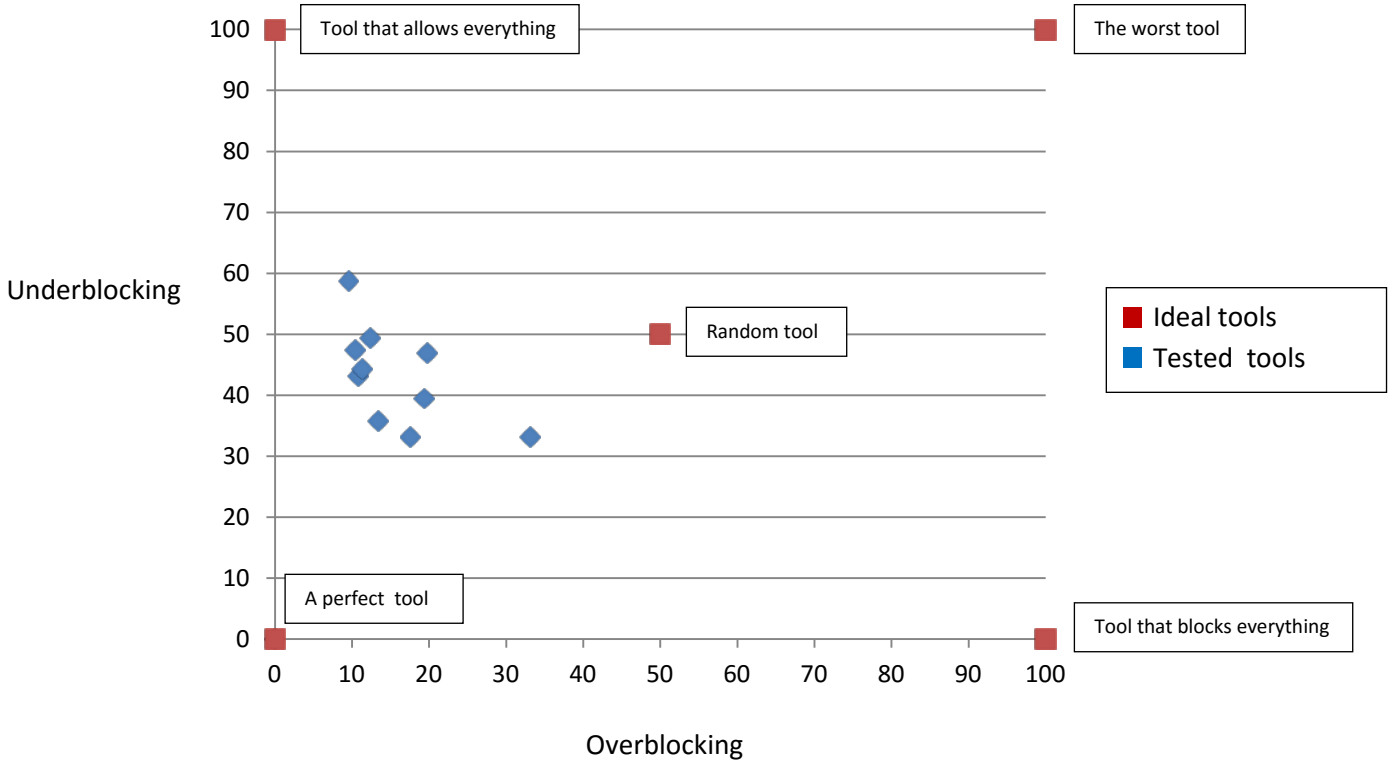
PC PARENTAL CONTROL TOOLS: Effectiveness key findings

Table 8 - Effectiveness key findings

In general, tools have low effectiveness	
Underblocking/Overblocking	The underblocking rate is higher than 30 % for all tested tools. The overblocking rate is low for some tools but, in these cases, the underblocking rate is very high. Overblocking and underblocking rates are linked: tools with a low underblocking rate have a high overblocking rate. It might be assumed that the tools rely mainly on black lists and keywords URL analysis, having the well-known limits associated with these techniques, in particular the difficulty to analyse user-generated content. Less than 20 % of the data test set used belongs to the existing black lists and the data test set consists of 4,000 items. This may explain why effectiveness results may be lower than the ones proposed by other similar tests.
Age classes	The tools perform quite similarly with a configuration for the two age classes (≤12 and ≥ 13). Part of the explanation lies in the fact that many tools do not give a real possibility to create personalised profiles according to the age: • No level of filtering available • Personalisation by content categories that both applies to children and teenagers. In most of the cases, the tools perform better for the ≥ 13 age class, as the scoring gives less importance to underblocking for teenagers, than for children.
Web and Web 2.0	The tools present lower effectiveness on Web 2.0 content. In particular, the tools which achieve better results than the others have generally higher discrepancy between the underblocking rate on Web and Web 2.0. It is an indicator of the difficulties of tools to deal with user-generated and Web 2.0 content. The web 2.0 is more difficult to filter for several reasons: the content is produced mainly by users and not by

	identified subjects like companies or institutions. On the website you can find content published by different users, both harmful and not harmful. The content is changing very quickly: a web page that is not harmful could become harmful because of uploaded image. The content may vary according to the user: for instance, each Facebook user's home page is different. Concerning the qualitative tests on web 2.0, all the tools fail.
Topics	The adult content is better filtered than the "other" content categories. On adult content some tools achieve an underblocking lower than 10 % which is almost good. On the "other" content categories (except of gambling) only a few tools have an underblocking close to 30 %. Most of them have very low effectiveness (more than 70 % of underblocking).
Languages	Tools work better in English than in other languages. Even considering only English content, all the tools have an underblocking rate higher than 20 %.

Figure 1 - PC PARENTAL CONTROL TOOLS Effectiveness performance



Each point in the above graph represents the overblocking and underblocking performance of the tested tools compared with ipothetic performance of ideal tools.

PC PARENTAL CONTROL TOOLS: Effectiveness (score view)

Effectiveness assessed according to topic and age

Table 9 - PC Tools EFFECTIVENESS results: score view

TOOL NAME	Adult		Other		Overall Score	
	≤12	≥13	≤12	≥13	≤12	≥13
F-SECURE INTERNET SECURITY	3,0	3,0	0,0	0,0	1,5	1,5
K9 WEB PROTECTION	2,2	2,4	0,0	0,0	1,1	1,2
MAC OS X PARENTAL CONTROLS	2,0	2,0	0,0	0,0	1,0	1,0
MCAFEE ALL ACCESS	2,0	2,0	0,0	0,0	1,0	1,0
NORTON ONLINE FAMILY	3,6	3,2	0,0	0,0	1,8	1,6
OPTENET PC	2,2	2,4	0,0	0,0	1,1	1,2
PANDA	2,6	2,2	0,0	0,0	1,3	1,1
PURESIGHT OWL	3,0	3,0	1,4	1,8	2,2	2,4
QUSTODIO	2,2	2,4	0,0	0,0	1,1	1,2
TREND MICRO ONLINE GUARDIAN	2,2	2,4	0,0	0,0	1,1	1,2

How to read the table
The table shows how effective the tools are in filtering harmful content. The tool was scored both with reference to the “adult” content and to the “other harmful” content (drugs, violence, racism, etc.) taking into account two different class of age (≤12 years old and ≥13 years old). An overall score was assigned to each age class as **the result of the average performance of the two content topic types.** The scoring scale considers both the underblocking (harmful pages which are not blocked) and overblocking (non-harmful pages which are blocked). For a comprehensive understanding of the assessment, please read the ‘Methodology key issues’.

Effectiveness Score. The tool was scored from 0 to 4 according to the number of the tested functionalities covered (see ‘Methodology key issues’):
0 Very weak - The tool is less effective than a random tool
1 Weak - The tool has a low effectiveness and answers very partially to parents needs
2 Fair - The tool has a fair lever of filtering, nonetheless a non-small part of the content is not correctly filtered
3 Good - The tool offers a good level of filtering but a part of the content is not correctly filtered.
4 Excellent - The tool offers a very good level of filtering and satisfies the parents’ needs in terms of effectiveness.

Note: The overall effectiveness score only provides a synthetic view of the results. The reader should check all the results (overblocking, underblocking...) before choosing a software. A tool could have a good overall score having a very good result on other contents.

PC PARENTAL CONTROL TOOLS: Effectiveness (over/underblocking)

Underblocking and overblocking

The tools' effectiveness was assessed in terms of their performance in blocking harmful content and allowing non-harmful content. When a tool is not able to perform perfectly, two situations may occur: underblocking and overblocking. Underblocking occurs when the tool allows harmful content; overblocking occurs when the tool blocks non-harmful content.

Therefore, each tool's performance was measured and shown in terms of both underblocking and overblocking (in the final ranking the two situations will be weighed differently according to the user's age).

In the following tables the outcomes are provided in percentage (%):

- Underblocking measures how much harmful content is not filtered. **A good tool will have a low underblocking**, and your child will be rarely exposed to harmful content.
- Overblocking measures how much non-harmful content is blocked. **A good tool will have a low overblocking**, and non-harmful content will be rarely blocked.

The lower the level of both underblocking and overblocking, the better the tool is.

PC PARENTAL CONTROL TOOLS: Effectiveness related to topic (over/underblocking)

Table 10 – PC Tools EFFECTIVENESS results for topics: % of over/underblocked content

Topic	Adult content		Violence and Crime		Racist		Drugs & Self-Damage		Gambling	
	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking
F-SECURE INTERNET SECURITY	13	15	7	74	9	79	19	46	21	28
K9 WEB PROTECTION	12	27	7	80	13	74	8	55	11	29
MAC OS X PARENTAL CONTROLS	27	21	18	80	7	80	10	72	15	60
MCAFEE ALL ACCESS	23	22	16	60	14	62	12	62	21	44
NORTON ONLINE FAMILY	22	9	6	87	2	89	3	90	0	93
OPTENET PC	13	24	8	79	9	80	7	70	8	54
PANDA	31	13	27	72	13	77	53	42	48	22
PURESIGHT OWL	18	19	1	53	12	60	35	38	21	38
QUSTODIO	12	26	4	97	0	98	6	96	19	75
TREND MICRO ONLINE GUARDIAN	11	23	11	60	9	64	14	79	13	60

How to read the table

The table shows how effective the tools are in blocking content according to the topic.

PARENTS can verify how effective is each tool for the categories they assume are more threatening for their children.

Results are provided in % of overblocked or underblocked content.

PC PARENTAL CONTROL TOOLS: Effectiveness related to language (over/underblocking)

Table 11 – PC Tools EFFECTIVENESS results for languages: % of over/underblocked content

Language	English		German		Italian		Spanish		French		Polish	
	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking
F-SECURE INTERNET SECURITY	14	24	16	25	12	56	17	47	15	48	10	64
K9 WEB PROTECTION	12	38	11	44	11	50	9	48	9	48	10	50
MAC OS X PARENTAL CONTROLS	21	27	15	53	17	67	15	70	21	73	27	72
MCAFEE ALL ACCESS	19	22	14	48	17	60	17	64	17	59	30	59
NORTON ONLINE FAMILY	11	42	15	54	14	53	12	52	13	51	11	70
OPTENET PC	13	39	7	48	9	66	12	49	9	53	8	59
PANDA	35	28	32	32	29	38	30	41	30	35	34	44
PURESIGHT OWL	17	26	18	43	19	51	20	43	20	35	18	28
QUSTODIO	11	52	8	63	10	64	9	67	10	65	8	71
TREND MICRO ONLINE GUARDIAN	12	33	7	54	15	59	9	51	12	54	7	57

How to read the table

The table shows how effective the tools are in blocking content in six different languages.

PARENTS can verify how effective each tool is for their language/s of interest. Results are provided as % of overblocked or underblocked content.

PC PARENTAL CONTROL TOOLS: Effectiveness related to age (over/underblocking)

Table 12 – PC Tools EFFECTIVENESS results for users' age: % of over/underblocked content

Age	≤12		≥13	
	Overblocking	Underblocking	Overblocking	Underblocking
F-SECURE INTERNET SECURITY	14	34	14	37
K9 WEB PROTECTION	12	44	10	42
MAC OS X PARENTAL CONTROLS	24	55	16	39
MCAFEE ALL ACCESS	9	40	29	40
NORTON ONLINE FAMILY	16	53	8	45
OPTENET PC	12	56	10	38
PANDA	33	30	33	36
PURESIGHT OWL	17	32	19	34
QUSTODIO	10	59	10	59
TREND MICRO ONLINE GUARDIAN	13	46	9	42

How to read the table

The table shows how effective the tools are according to the age of the children. Each tool has been configured for each category and tested. PARENTS can verify how effective each tool is, considering the age of their children. Results are provided in % of overblocked or underblocked content.

PC PARENTAL CONTROL TOOLS: Effectiveness related to Web type: Web/Web 2.0

Table 13 - PC Tools EFFECTIVENESS results for Web types: % of over/underblocked content

Web Type	Web		Web 2.0	
	Overblocking	Underblocking	Overblocking	Underblocking
F-SECURE INTERNET SECURITY	16	21	11	51
K9 WEB PROTECTION	8	41	14	45
MAC OS X PARENTAL CONTROLS	12	37	26	57
MCAFEE ALL ACCESS	20	42	18	37
NORTON ONLINE FAMILY	14	33	10	64
OPTENET PC	13	31	8	65
PANDA	43	19	22	46
PURESIGHT OWL	14	27	22	39
QUSTODIO	12	32	8	85
TREND MICRO ONLINE GUARDIAN	10	30	11	57

How to read the table

The table shows how effective the tools are according to the typology of content, whether it is part of the traditional Web or Web 2.0.

The tools were tested both on user generated content or web 2.0 (blogs, social networks, forums) and traditional Web content (pages of website).

PARENTS can verify how effective each software is, considering the kind of content most accessed by their children. Results are provided in % of overblocked or underblocked content.

PC PARENTAL CONTROL TOOLS: Effectiveness related to social Media

Table 14 - PC Tools EFFECTIVENESS results for social Media content: % of underblocked content

	Tumblr	YouTube	Vine	Pinterest	Twitter	Facebook
F-SECURE INTERNET SECURITY	100	100	100	100	100	100
K9 WEB PROTECTION	15	99,5	100	97,2	100	99
MAC OS X PARENTAL CONTROLS	90	97	100	100	100	99
MCAFEE ALL ACCESS	86	100	100	45	100	99
NORTON ONLINE FAMILY	79	99	100	100	100	99
OPTENET PC	95	100	100	96	100	99
PANDA	82	99,5	100	100	100	100
PURESIGHT OWL	75	95	100	90	97	98
QUSTODIO	70	100	100	87	100	100
TREND MICRO ONLINE GUARDIAN	88	99	100	58	100	100

How to read the table

The table shows how effective the tools are according on the main social media platforms.

PARENTS can verify how effective each software is, considering the kind of content most accessed by their children. Results are provided in % of underblocked content.

The tools have huge difficulties to handle the contents present on the main social media platforms and mostly do not filter them. The only exception is Tumblr which is well filtered by K9. In this case further tests have shown that this tool has a very high overblocking score. In other words, K9 blocks almost all content present on Tumblr, whether it is harmful or not.

PC PARENTAL CONTROL TOOLS: Usability key findings

9 out of 10 tools gain better scores for installation and/or configuration than for usage.

Overall, no tools score less than 2 points, thus not reaching the threshold of 50 % of 4 points, two tools range between 2 and 2.50, three tools from 2.50 up to 3. **Five tools score in the top area and gain 3 points or more**.

General findings	Some of the tools keep the installation and configuration procedures very simple. However, possibilities to customise the tool to one's own needs are poor. Other tools have very extended options to configure the software but then the risk of unwished configuration effects and bad filtering results is high. Only a few tools provide additional information about filtering in general and about limitations and restrictions of the filtering procedures. About one third of the tools provide a web- or server-based configuration. Web-based or remote management allows the parents to reconfigure and monitor their children's use from another device, but might consume more time for navigation and storage. But server based configuration has also risks: one product (Net Nanny) was not installable due to bad server connections.
Findings on the installation process	A high percentage of tools keep the installation process very simple. In some cases, the installation process runs nearly automatically and is similar to the installation of an App on a smart phone or other mobile device. Some tools merge the installation and first configuration steps into one single process.
Findings on the configuration process	The configuration process is key for the product because of its relevance for an effective use of the filter. For several tools there are very few configuration options. For other tools, configuration is very exhaustive and comprises a lot of functionalities. Some products compensate complexity by good explanations and a well-structured user interface. The range of customisation options is broad. For some tools there can be set only one degree of strength of filtering for all content categories, while others allow to differentiate the strength of filtering between different content categories. Several tools do not explain their filter categories, although some categories are quite unusual with regards to youth protection, i.e. sports or humour.

Findings on the usage of the tools	As most parental control tools work 'in the background', there is less “usage” than with other computer software. Nonetheless, it is important that parents can easily handle the alert messages and the reporting to keep them involved with the products. Testing of the usage of traditional parental controls refers mainly to the usability of alert messages for blocked web sites. Most tools do not address the alert message to children and youth but to adults only. Most tools do not allow appropriate reaction to the alert message for a blocked web site. Monitoring and reporting functionalities were tested as usage of the tools where applicable. Reporting ranges from mere log file data to detailed and colourful diagrams. For alternative tools testing of usage covers also the usability for children as they are the user target group of those products.

PC PARENTAL CONTROL TOOLS: Usability table

Table 15 - PC Tools USABILITY result

PC / Mac	F-Secure Internet Security	K9 Web Protection	Mac Os X Parental Controls	McAfee All Access	Norton Online Family	Optenet PC	Panda	Puresight Owl	Qustodio	Trend Micro Online Guardian
I	3,05	2,28		3,22	2,98	2,78	2,4	2,96	3,01	2,69
C	2,87	3,31	3,09	3,21	3,43	2,47	2,66	3,01	3,43	3,63
U	2,96	2,65	2,69	2,52	3,22	2,14	1,44	3,33	2,63	2,9
overall	**2,93**	**2,90**	**2,94**	**3,00**	**3,28**	**2,44**	**2,24**	**3,09**	**3,11**	**3,22**

How to read the table

The table shows the results for three different processes: Installation, Configuration/Re-configuration and Usage.

The scores are scaled from 0 to 4 points.

For each process a set of criteria was applied to the product. The detailed test results are available in a tool fiche for each product and also in a database available online.

I = Installation

C = Configuration /Re-configuration

U = Usage

PARENTAL CONTROL TOOLS FOR MOBILE DEVICES

FINDINGS FOR
FUNCTIONALITY, SECURITY, EFFECTIVENESS, USABILITY

Mobile phones and the Internet

Smart phones are one of the most trendy devices used by CHILDREN /TEENAGERS, with a majority of teens, to access the Internet, to watch video streaming and to communicate with other people using specific applications such as Instant Messaging (e.g. Skype).

MOBILE PHONES PARENTAL CONTROL TOOLS: Functionality key findings

Tools able to filter the web-pages content have limited functionalities compared to the tools available for PCs.

iPhone are equipped with an OS-embedded parental control tool which is able to restrict the usage of some protocols/applications such as accessing Internet, browsing YouTube or sending/receiving e-mails.

Apple provides also content filtering function as out-of-the-box feature based on the OS.

The other operating systems do not provide embedded parental control tools for mobile phones as comprehensive as the ones provided by Apple. Actually, the only way to filter the Internet is to use an external tool.

Web Content Filtering

8 out of the 10 selected tools give parents the opportunity to personalise the filtering process by choosing filtered topics.

Some tools give parents the possibility to manage the tool online (from a PC or another mobile device). For some tools - Norton for example - it is possible to manage both the mobile tool and the PC tool (provided that user instal both tools on the children/teenager's device).

Applications/Protocols and other issues

As for the usage restriction and monitoring, the selected tools offer very limited functionalities, in particular for Skype or streaming which are very popular among teenagers.

Security

Many tools can be easily uninstalled. Many tools consist of a browser with Internet access; often it is easy to use another browser and in this way by-pass the tool. In many cases mobile devices tools are useless.

Table 16 - MOBILE PHONES Tools FUNCTIONALITY results and overall functionality and security score

Area of need	Usage Restriction															
Functionality	Email	P2P		Personal data Provision	Safe search	Skype		Social Networks		Streaming		Web		Windows Life Messenger		
Specific Issue	Block email client and/or webmail access	Block the application	Monitor Downloads	Block	Availability	Block chat	Block video chat	Block Access	Monitor Usage	Block Access	Monitor Access	Block Access	Monitor Access	Block chat	Block video chat	Monitor
AVG Family Safety	N	N	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N
F-Secure Mobile Security	Y	N	N	N	Y	Y	N	Y	N	N	N	Y	N	N	N	N
K9 Web Protection Browser (Mobile)	N	N	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N
Mobicip Safe Browser	Y	N	N	N	N	N	N	Y	N	Y	N	Y	N	N	N	N
Mobiflock	Y	N	N	N	Y	N	N	Y	N	Y	N	Y	Y	N	N	N
Mobile Parental Filter	Y	N	N	N	N	N	N	Y	N	N	N	Y	N	N	N	N
Net Nanny For Android	N	N	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N
Norton Online Family (Mobile)	Y	N	N	N	Y	N	N	Y	N	N	N	Y	Y	N	N	N
Parentsaround (Mobile)	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N
Xooloo (Mobile)	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
% of tools with function	50 %	0 %	0 %	0 %	70 %	10 %	0 %	50 %	0 %	20 %	0 %	80 %	20 %	0 %	0 %	0 %

Table 17 - MOBILE PHONES Tools FUNCTIONALITY results and overall functionality and security score

Area of need	Management			Filtering Customisation					Keywords			Time	Blocking Message			Security
Functionality	Management of User profiles	Monitoring	Remote Management	Topics	URLs Black List	URLs White List			Keywords			Time Limit Settings	Type			Score
Specific Issue	Create several profiles	Remote access to monitoring	Manage on various devices	Customisation of Filtering Topics	Creation of User's own Black List	Default White List	Modification OR Creation	Restrict Browsing to White List	Creation of a User's Black List	Creation of a User's White List	Default Black List	Set a specific time frame or web access duration	Ask for unblocking by parents	Redirect to safe resources	% function coverage	
AVG Family Safety	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	10 %	0
F-Secure Mobile Security	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	20 %	1
K9 Web Protection Browser (Mobile)	N	N	N	N	N	N	N	N	N	N	N	N	N	N	7 %	1
Mobicip Safe Browser	Y	N	Y	Y	N	N	N	N	N	N	N	N	N	N	23 %	1
Mobiflock	N	Y	Y	Y	Y	N	Y	Y	N	N	N	Y	N	N	43 %	0
Mobile Parental Filter	Y	Y	Y	N	Y	N	Y	N	N	N	N	Y	Y	N	33 %	4
Net Nanny For Android	Y	N	Y	Y	Y	N	Y	N	N	N	N	Y	N	Y	30 %	4
Norton Online Family (Mobile)	Y	Y	Y	N	Y	Y	Y	N	N	N	N	Y	N	N	40 %	0
Parentsaround (Mobile)	Y	N	Y	N	Y	N	Y	N	N	N	N	Y	Y	N	23 %	4
Xooloo (Mobile)	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	3 %	4
% of tools with function	50 %	30 %	60 %	30 %	60 %	10 %	50 %	10 %	0 %	0 %	0 %	60 %	20 %	20 %		

MOBILE PHONES PARENTAL CONTROL TOOLS: Effectiveness key findings

Table 18 - MOBILE PHONES PARENTAL CONTROL TOOLS – Effectiveness key findings

Many of the solutions tested are also offered on PC with different interfaces and functionalities. The effectiveness of the mobile solutions is slightly lower than the one assessed for the similar PC products	
Age classes	The tools have similar results for CHILDREN and TEENAGERS. Indeed, the results of underblocking are almost the same for the two age categories.
Web and Web 2.0	All tools perform better on web than on web 2.0. As for the qualitative tests on web 2.0, all tools fail.
Topics	Other categories are badly filtered, with a very high underblocking for both tools. The tools perform better on adult content.
Languages	The tools are more positively assessed with reference to English content than with reference to other languages.

MOBILE PHONES PARENTAL CONTROL TOOLS: Effectiveness

Table 19 - MOBILE PHONES Tools EFFECTIVENESS results – Score view

	Adult		Other		Overall Score	
	≤12	≥13	≤12	≥13	≤12	≥13
AVG FAMILY SECURITY	3,0	3,0	0,0	0,0	1,5	1,5
F-SECURE MOBILE SECURITY	3,0	3,0	0,0	0,0	1,5	1,5
K9 WEB PROTECTION BROWSER	2,2	2,4	0,0	0,0	1,1	1,2
MOBICIP SAFE BROWSER	2,2	2,4	0,0	0,0	1,1	1,2
MOBIFLOCK	0,8	1,6	0,0	0,0	0,4	0,8
MOBILE PARENTAL FILTER	2,4	2,8	0,0	0,0	1,2	1,4
NET NANNY FOR ANDROID	1,4	1,8	0,0	0,0	0,7	0,9
NORTON ONLINE FAMILY	3,6	3,2	0,0	0,0	1,8	1,6
PARENTSAROUND	1,4	1,8	0,0	0,0	0,7	0,9
XOOLOO (mobile)	2,8	2,6	0,0	0,0	1,4	1,3

How to read the table

The table shows how effective the tools are in filtering harmful content. The tool is scored both with reference to the "adult" content and to the "other harmful" content (drugs, violence, racism, etc.) taking into account two different classes of age (≤12 years old and ≥13 years old). An overall score is assigned to each age class as **the results of the average performance of the two content topic types.** The scoring scale considers both the underblocking (harmful pages which are not blocked) and overblocking (non-harmful pages which are blocked). For a comprehensive understanding of the assessment, please read the 'Methodology key issues'.

Effectiveness Score. The score ranges from 0 to 4 according to the number of the tested functionalities covered (see 'Methodology key issues'):

0 Very weak - The tool is less effective than a random tool.

1 Weak - The tool has a low effectiveness and answers very partially to parents needs.

2 Fair - The tool has a fair lever of filtering, nonetheless a non small part of the content is not correctly filtered.

3 Good - The tool offers a good level of filtering but a part of the content is not correctly filtered.

4 Excellent - The tool offers a very good level of filtering and satisfy the parents' needs in terms of effectiveness.

Note: The overall effectiveness score provides only a synthetic view of the results. The reader should check all the results (overblocking, underblocking) before choosing a software. A tool may have a good overall score with very good results on adult contents, but bad results on other contents.

MOBILE PHONES PARENTAL CONTROL TOOLS:
Effectiveness (overblocking/underblocking)

Underblocking and overblocking

The tools' effectiveness was assessed in terms of their performance in blocking harmful content and allowing non-harmful content. When a tool is not able to perform perfectly, two situations may occur: underblocking or overblocking.

Underblocking occurs when the tool allows harmful content; overblocking occurs when the tool blocks non-harmful content.

Therefore, each tool's performance has been measured and shown both in terms of underblocking and overblocking (in the final ranking the two situations are weighed differently according to the user's age).

In the following tables the outcomes are provided in percentage (%):

- Underblocking measures: how much of the harmful content is not filtered. **A good tool will have a low underblocking** and the CHILD/TEENAGER will be rarely exposed to harmful content.
- Overblocking measures: how much of the non-harmful content is blocked. **A good tool will have a low overblocking** and non-harmful content will be rarely blocked.

The lower the level of both underblocking and overblocking, the better is the tool.

MOBILE PHONES PARENTAL CONTROL TOOLS:

Effectiveness (overbloking/underblocking)

Table 20 - MOBILE Tools EFFECTIVENESS results for topics: % of overbloked/underblocked content

Topic	Adult content		Violence and Crime		Racist		Drugs & Self-Damage		Gambling	
	Over-blocking	Under-blocking	Over-blocking	Under-blocking	Over-blocking	Under-blocking	Over-blocking	Under blocking	Over blocking	Under blocking
AVG FAMILY SECURITY	15	13	20	75	14	55	13	50	21	36
F-SECURE MOBILE SECURITY	13	17	9	75	10	76	20	47	22	30
K9 WEB PROTECTION BROWSER	12	29	7	79	13	76	8	56	11	33
MOBICIP SAFE BROWSER	11	26	7	74	10	73	10	64	18	53
MOBIFLOCK	1	60	9	67	12	63	9	71	10	74
MOBILE PARENTAL FILTER	9	20	15	53	14	72	17	62	20	54
NET NANNY FOR ANDROID	16	38	10	81	11	79	41	54	35	50
NORTON ONLINE FAMILY	23	9	6	85	2	92	4	90	2	94
PARENTSAROUND	15	40	14	70	13	72	15	75	20	45
XOOLOO (mobile)	21	13	13	72	10	80	10	60	21	35

MOBILE PHONES PARENTAL CONTROL TOOLS:

Effectiveness (overbloking/underblocking)

Table 21 – MOBILE Tools EFFECTIVENESS results for languages: % of over -/underblocked content

Language	English		German		Italian		Spanish		French		Polish	
	Over blocking	Under blocking	Over blocking	Under blocking	Over blocking	Under blocking	Over blocking	Under blocking	Over blocking	Under blocking	Over blocking	Under blocking
AVG FAMILY SECURITY	18	24	20	46	21	35	12	43	9	38	8	58
F-SECURE MOBILE SECURITY	14	26	14	25	14	57	15	47	16	49	11	62
K9 WEB PROTECTION BROWSER	14	37	10	48	12	58	8	56	11	46	7	57
MOBICIP SAFE BROWSER	9	39	13	52	17	50	12	53	14	48	9	62
MOBIFLOCK	5	59	6	67	6	71	10	72	6	80	7	55
MOBILE PARENTAL FILTER	13	36	17	45	12	45	10	46	14	32	12	52
NET NANNY FOR ANDROID	26	41	17	61	13	68	20	54	8	62	12	70
NORTON ONLINE FAMILY	12	43	15	54	12	55	13	53	18	53	12	70
PARENTSAROUND	16	47	16	55	15	58	15	57	14	56	10	69
XOOLOO (mobile)	9	29	8	44	30	50	12	58	59	29	16	44

MOBILE PHONES PARENTAL CONTROL TOOLS:

Effectiveness (over/underblocking)

Table 21 – MOBILE Tools EFFECTIVENESS results for Web types: % of over -/underblocked content

Web Type	Web		Web 2.0	
	Overblocking	Underblocking	Overblocking	Underblocking
AVG FAMILY SECURITY	10	25	22	42
F-SECURE MOBILE SECURITY	16	32	11	42
K9 WEB PROTECTION BROWSER	8	42	14	48
MOBICIP SAFE BROWSER	12	47	10	45
MOBIFLOCK	6	60	6	67
MOBILE PARENTAL FILTER	13	35	12	45
NET NANNY FOR ANDROID	21	50	19	54
NORTON ONLINE FAMILY	14	33	10	64
PARENTSAROUND	16	40	14	65
XOOLOO (mobile)	15	33	18	41

MOBILE PHONES PARENTAL CONTROL TOOLS:

Effectiveness (over/underblocking)

Table 22 - MOBILE Tools EFFECTIVENESS results for users' age: % of over -/underblocked content

Age	≤12		≥13	
	Overblocking	Underblocking	Overblocking	Underblocking
AVG FAMILY SECURITY	12	38	20	30
F-SECURE MOBILE SECURITY	14	34	14	40
K9 WEB PROTECTION BROWSER	13	46	12	42
MOBICIP SAFE BROWSER	15	48	7	44
MOBIFLOCK	7	66	5	62
MOBILE PARENTAL FILTER	12	41	14	39
NET NANNY FOR ANDROID	20	50	20	54
NORTON ONLINE FAMILY	18	53	8	47
PARENTSAROUND	14	50	16	56
XOOLOO	17	34	11	40

MOBILE PHONES PARENTAL CONTROL TOOLS: Usability key findings

The overall score for the mobile tools range between 1.96 and 3.19

General findings	The issue that most children consider their mobile phone as a very personal item is not sufficiently reflected in the tools' functionalities, i.e. parents need to take the device from their children for monitoring their usage and to access the reporting. Although most tools provide web-based configuration and reporting mechanisms, most of the tools lack the opportunity to address the children appropriately and communicate the objectives of the parental control tool to them.
Findings on the installation process	The tools tested come as an application that is installed nearly automatically with the download. Therefore, there is no installation process to be handled by the user.
Findings on the configuration process	The complexity of the configuration process differs: most tools provide a web-based configuration. Some tools provide a configuration on the tool and additionally a web based configuration. Tools with application-based configuration have less opportunities to offer a wide spectrum of functions. The configuration on the device also might be challenging for parents not familiar with mobilesmart phones. Information about how to proceed after the installation is sometimes missing or badly linked within the smartphone application.
Findings on usage	As most parental control tools work 'in the background' of the mobile phones, there is less usage than with other computer software. Nonetheless, it is important that parents can easily handle the alert messages and the reporting to keep them involved with the products. Few tools address the alert message for a blocked web site to children but alert messages are mostly comprehensible to youth and adults. Reporting function is comprehensible for most products, and the amount of information is adequate.

MOBILE PHONES PARENTAL CONTROL TOOLS:

Usability key findings

Table 23 - MOBILE PHONES Tools USABILITY results

	AVG Family Safety	F-Secure Mobile Security	K9 Web Protection Browser	Mobicip Safe Browser	Mobiflock	Mobile Parental Filter	Net Nanny For Android	Norton Online Family (Mobile)	Parentsaround (Mobile)	Xooloo (Mobile)
I										
C	2,44	3,28	2,45	2,84	3,43	2,89	3,38	3,46	3,13	2,84
U	1,61	2,11	1,15	1,2	2,09	2,93	2,87	2,5	2,24	0,75
overall	**2,13**	**2,84**	**1,96**	**2,22**	**2,93**	**2,9**	**3,19**	**3,1**	**2,8**	**2,06**

How to read the table

The table shows the results for three different processes: Installation, Configuration/Re-Configuration and Usage. The scores are scaled from 0 to 4 points. For each process a set of criteria has been applied to the product. The detailed test results are available in a tool fiche for each product and also in a database available online.

I = Installation

C = Configuration /Re-configuration

U = Usage

ALTERNATIVE TOOLS

FINDINGS FOR
FUNCTIONALITY, SECURITY, EFFECTIVENESS, USABILITY

Alternative tools

Alternative tools refer for example to tools based entirely on white lists (so called "walled gardens") or child safe browsers which are usually designed to create a safe environment for very young children.

ALTERNATIVE TOOLS: Functionality key findings

The alternative tools tested in the 3rd cycle were the following:

- for Win7 Care4teen, KidZui and Magic Desktop) and
- for Android (Famigo and Xooloo_Mobile)

Care4teen is a very basic parental control tool and is supported by common web browsers. The tool can be managed on various devices and offers a remote access to monitoring.

KidZui and Magic Desktop are similar. They are browser applications. The offered websites, online games and videos in KidZui are all approved by KidZui's staff. Compared to Magic Desktop, with KidZui it is not possible to edit the default white list.

Care4teen, KidZui and Magic Desktop allow browsing by white list only, but their white lists differ as for their quality and quantity (please see under "Security and effectiveness" section].

Famigo and Xooloo (Mobile) are also similar. They are closed systems with their own entertainment choices to buy. It is not possible to search the internet like with a web browser. It differs from the intended purpose to protect children's activities on the internet and to learn how to use the computer.

ALTERNATIVE TOOLS: Functionality key findings

Table 24 - ALTERNATIVE Tools FUNCTIONALITY results and overall functionality

Area of need	Usage Restriction															
Functionality	Email	P2P		Personal data Provision	Safe search	Skype		Social Networks		Streaming		Web		Windows Life Messenger		
Specific Issue	Block email client and/or webmail access	Block the application	Monitor Downloads	Block	Availability	Block chat	Block video chat	Block Access	Monitor Usage	Block Access	Monitor Access	Block Access	Monitor Access	Block chat	Block video chat	Monitor
Care4teen	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
Famigo	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Kidzui	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N
Magic Desktop	N	N	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N
Xooloo (Mobile) [younger age group]	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
% of tools with function	0 %	0 %	0 %	0 %	40 %	0 %	0 %	0 %	0 %	0 %	0 %	40 %	0 %	0 %	0 %	0 %

ALTERNATIVE TOOLS: Functionality key findings

Table 25 - ALTERNATIVE Tools FUNCTIONALITY results and overall functionality

Area of need	Management			Filtering Customisation					Keywords			Time	Blocking Message		
Functionality	Management of User profiles	Monitoring	Remote Management	Topics	URLs Black List	URLs White List			Keywords			Time Limit Settings	Type		
Specific Issue	Create several profiles	Remote access to monitoring	Manage on various devices	Custom-isation of Filtering Topics	Creation of User's own Black List	Default White List	Modification OR Creation	Restrict Browsing to White List	Creation of a User's Black List	Creation of a User's White List	Default Black List	Set a specific time frame or web access duration	Ask for unblocking by parents	Redirect to safe resources	% function coverage
Care4teen	N	Y	Y	N	N	Y	N	N	N	N	N	N	N	N	13 %
Famigo	Y	Y	Y	N	N	Y	N	N	N	N	N	N	N	N	13 %
Kidzui	Y	N	Y	N	N	Y	N	N	N	N	N	N	N	N	13 %
Magic Desktop	Y	N	Y	N	N	Y	N	Y	N	N	N	Y	N	N	23 %
Xooloo (Mobile) [younger age	N	N	N	N	N	N	N	N	N	N	N	N	N	N	0 %
% of tools with function	60 %	40 %	80 %	0 %	0 %	80 %	0 %	20 %	0 %	0 %	0 %	20 %	0 %	0 %	

ALTERNATIVE TOOLS: Security and Effectiveness

Care4teen

It has not been possible to complete the installation of Care4teen during the effectiveness tests. So effectiveness has not been tested.

Famigo

Famigo is an app for mobile devices. Parents can select the apps installed on the device used by the children/teenagers. The children/teenagers can also access some selected resources on Internet through a white list. As the tool offers only access to a white list it is not possible to calculate the effectiveness of the tool.

The tool offers a good level of security. It is necessary to insert the parent password to exit the tool. The mobile is used by the children/teenagers only through the tool interface so he/she can access only some limited functionalities.

KidZui (LeapSearch)

KidZui is an easy web browser for children. All the offered websites, online games and videos are approved by KidZui. The software only allows to browse on a predefined white list and there is no possibility to edit the list. The configuration process and the general handling is very easy.

The content of the white list is accessible both by an internal search engine and some lists. It is to be noted that the accessible content is in English. Therefore, a non-English speaking child would not be able to use the internal search engine.

The tool offers a good level of security. It is necessary to insert the parent password to exit the tool. The parent may activate an option that launches the tool when starting the computer. In this case the child cannot access the Internet but only the website is accessible through the KidZui browser.

As the tool offers only access to a white list or a full access to the Internet, there is no filtering.

Magic Desktop

Magic Desktop is not a typical parental control. It provides a full environment to the children substituting Windows with a specific desktop layout and specific educational software. It offers two tools that provide a limited access to the Internet:

- A web browser which offers by default access to a limited list of websites or to websites chosen by the parents. Alternatively, the child can have full access to the Internet if the parent provides the administrator password.
- A mail client which enables the child to write ad receive messages from a limited list of contacts supervised by the parent.

Parent can switch to Windows and use it normally.

Easy Magic Desktop offers a good level of **security**. Easy Magic Desktop is launched automatically when starting the computer and the administrator password is required in order to switch to Windows. The security tests (closing the tool through the Task Manager starting the computer in safe mode) had a positive result. As the tool offers only an access to a white list or full access to the Internet, there is no filtering and it is not possible to calculate the effectiveness score.

Concerning the access to the Internet, the white list is very short (42 sites in English, 8 in Italian, 11 in German). The fact that the full access to Internet is provided through the software interface, specially designed for children, and not with Internet Explorer or Firefox could be misleading for the parent. Ideally the tool should alert the parent that full access to the Internet equals to no protection.

Xooloo

Xooloo App Kids is an application that provides an environment for children. The child can only access some limited resources and functionalities of the mobile device (apps selected by the parent), apps and web content selected by the software provider. The software only allows to surf through a predefined white list and there is no possibility to edit the list. The content of the white list is accessible by an internal search engine. There is no direct access to Internet and so it is not possible to calculate the effectiveness score.

The tool offers a good level of security. It is protected by a password and cannot be easily by-passed.

ALTERNATIVE TOOLS: Usability key findings

In the “classical” usabilitiy rating the alternative tools achieve quite close scores. Care4teen reached the highest score (2.4) closely followed by Magic Desktop (2.3), Kidzui and Famigo with the same score (2.2) and Xooloo (Mobile) (2.1).

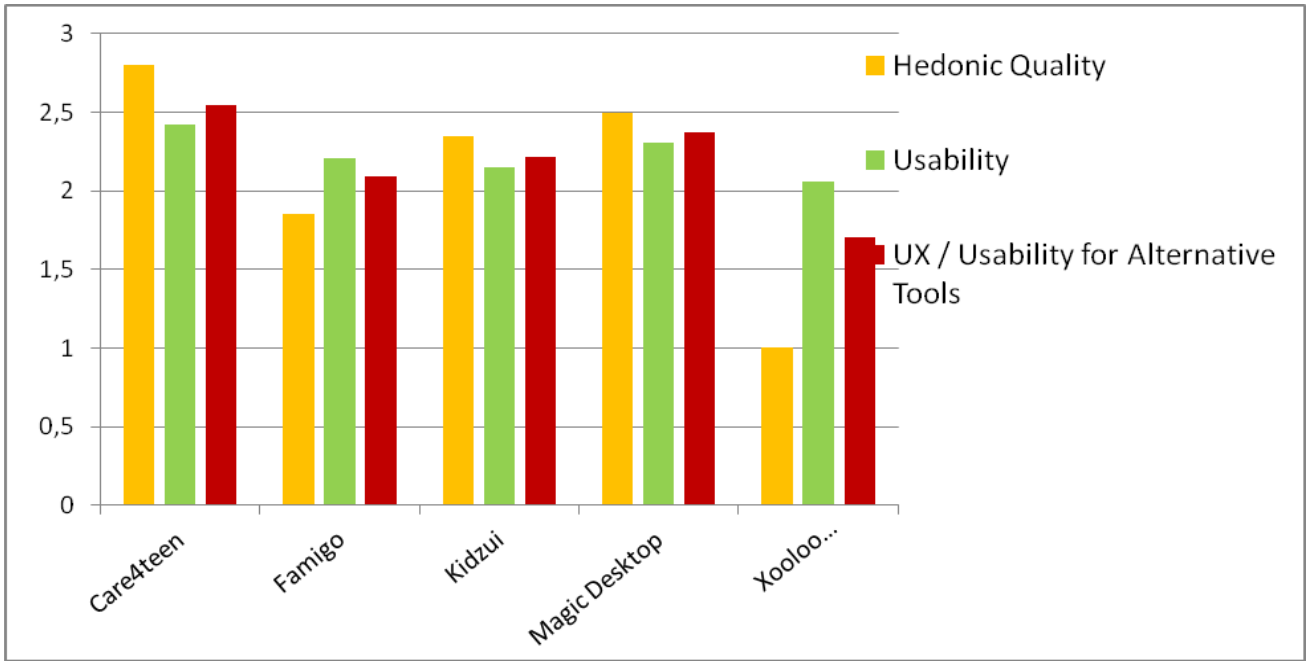
Table 26 - ALTERNATIVE TOOLS USABILITY results

Usability Alternative	Care4teen	Famigo	Kidzui	Magic Desktop	Xooloo (Mobile) [younger age
I	2,97				
C	2,53	2,56	2,59	2,85	2,84
U	1,86	1,63	1,42	1,4	0,75
Usability	2,4	2,2	2,2	2,3	2,1
Hedonic Quality	2,8	1,9	2,4	2,5	1,0
overall UX / Usability	**2,5**	**2,1**	**2,2**	**2,4**	**1,7**

In the overall usability Care4teen reaches the highest score (2.5) followed by Magic Desktop (2.4) that benefits from the high hedonic quality, and by KidZui (2.2) and Famigo (2.1). Xooloo (Mobile) reached the worst rating with the lowest hedonic quality score.

The below figure shows the performance of the five tools according to the Usability criterium, the hedonic quality and the overall UX/Usability.

Figure 2 - ALTERNATIVE TOOLS USABILITY scoring



PARENTAL CONTROL TOOLS FOR GAME CONSOLES

Game consoles and the Internet

Game consoles are meant for gaming and they are not widely used to access the Internet. They are mainly used for online gaming, chatting with other players and downloading content.

Game consoles were not tested in the 3nd cycle due to the fact that there were no major updates available at the stage of the testing phase.

The most recent results of our tests for game consoles are available in the 1st cycle report (http://www.sipbench.eu/phase6.cfm)

RECOMMENDATIONS

Recommedations are provided from SIP-BENCH III experts to potential users of parental control tools (PARENTS) and tools provider companies.
Recommendations are drown-up on the basis of the main results of the 3rd testing cycle conducted within the SIP-BENCH III Study.
Recommendations are provided with reference to the three categories of parental control tools tested: tools for PC/MAC, tools for Mobile devices, alternative tools.

RECOMMENDATIONS FOR PARENTS

PC TOOLS

General recommendations

- Filtering tools help you to protect your children. However, it is better to consider them only as a partial solution. The filtering process is still not effective enough. Therefore, in addition to using the tool, it is also important that you properly establish a direct communication with your children/teenagers. Discuss with them about their activities on the Internet, find out what they like or dislike, share with them some Internet-related activities and stay up-to-date about the latest trends and threats.
- Parents should keep in mind that filters can be operated at several complementary levels: the operating system (Windows or Mac OS provide some filtering functionalities), Internet service provider, a software or an app installed on the device, browser, some websites themselves (e.g. Google or Bing offer Safe Search features).
- Some tools are capable of monitoring users' activities in a very detailed way which could violate a child's/teenager's privacy rights. Also, when activating the filtering tool, discuss with your children what kind of filter you want to set up and why.
- When a page is blocked, some filtering tools give children/teenagers the option to ask parents to unblock the page. If you want to keep the communication open with your children/teenagers and to increase the tool's effectiveness (as some non-harmful pages are often blocked by error), you should enable this tool option and remember to regularly check and react to your child's/teenager's requests. Not responding to the requests may be very frustrating for your children/teenagers.
- Most of the tools provide some customisations features and also the possibility to create several accounts. Be sure that you create one account for each of your children/teenagers configured according to his/her needs and age.
- After you have set up the tool or accessed the administration panel of the tool, make sure you log out of the configuration panel or configuration page so that your children/teenagers cannot access it. Some tools require that the computer be restarted after a

configuration (first time or subsequent modifications). To make sure that the tool is properly working, perform a search on Google with a keyword such as “porn” (not in the presence of your child!). When you try to open the first of the available search results those pages should be blocked.

- Parents should remember to regularly update the tool settings so that they correspond to the children’s/teenagers’ ages and IT skills.
- Parents should be aware that there are more and more devices to access the web. Apart from PCs, mobile phones and game consoles, there are also tablets. Parents should bear in mind that using a mobile device to access the Internet puts children/teenagers in a situation where they are usually more often alone than accompanied by an adult who can support them.
- In some cases, it is not the tool itself but the service provider (e.g. browser provider, social network, video website, etc.) that lacks proper content classification. Therefore, parents should remember that parental control tool is complementary to other actions in ensuring their children's/teenagers’ safety on the web.

Password protection and security issues

- Make sure that access to the tool configuration is password protected.
- Some tools make use of Windows accounts to manage user profiles and/or require the Windows’ admin password to prevent disabling and uninstalling. It is not always evident that this feature is used, so you should check this. In case of doubt, you can create a separate Windows account for your child/teenager and protect your own admin account with a password or software which manages the different profiles linked with the Windows profile. In this case, you should create a password-protected profile for each child/teenager who can access the Internet. Admin access should be possible only for an adult and be password protected. Be aware that many tools can be bypassed or uninstalled quite easily by children and teenagers. Therefore, check periodically if the filtering tool is still installed and working.
- In case of many tools, there is no difference for the effectiveness between the age profiles available (unless there is a possibility of the white list). Parents of small children should choose a tool based on a white list.

Content filtering

- Be aware that filtering usually does not work well on content related to violence, racism, drugs, self-harm or anorexia. The best options for dealing with such content are education and communication.
- With regards to social networks, check what the tool offers. Does it block access to social networks? Does it filter the content available in social networks? Are there any reporting options that list what the children/teenagers do on social networks?
- Usually tools filter badly the content present on the Social Media (Facebook, YouTube, Twitter, Tumblr, etc.) and generally the user-generated content (Blog, forum, etc.)
- Filtering techniques are mainly based on text analysis. Tools have difficulties to filter images or video.
- If your children/teenagers mostly use the Internet for communicating with others, check the software that they use (e.g. MSN, Skype or Peer-to-Peer software). Then, decide whether you want to filter their communication, for example, filter or block certain actions or limit time spent using the software. In these cases, be aware that there are very few tools that can block/filter communication activities and that their features will differ.
- With regards to user generated content you should be aware not only about the possibility for your children/teenagers to come across bad content but also that your children/teenagers may produce inappropriate content by themselves.
- Be aware that tools with white list only could deprive children/teenagers of their access to information right.

MOBILE PHONES

- Many applications do not address the children/teenagers appropriately and do not communicate clearly the objectives of the parental control tool. Remote management options allow parents controlling their children/teenagers unperceived while other tools give access to monitoring and reporting only in the child's/teenager's mobile phone. Nevertheless, it is advisable that parents discuss with children/teenagers the issues of filtering, monitoring and reporting, instead of doing this in secret.
- Most of the applications consist of browsers that replace the default browser installed on the mobile phones. It is often possible to by-pass the parental control tool by using the default browser or installing another browser. Therefore, the best way is to use combined solutions, the filtering tool and OS functions or additional tools to block the default browser or the installation of another browser.
- Parents should choose solutions that provide a unique configuration and remote monitoring access for both mobile and PCs.
- Many applications give access to content on the Internet and by-pass the parental control tools. Therefore, parents should continue to monitor the applications installed on the mobile phones of their children/teenagers.

RECOMMENDATIONS FOR TOOLS PROVIDER COMPANIES

PC TOOLS

General recommendations

- Tools should contain a message that provides parents with an explanation of both the capabilities of the tool and its limitations. The message should also motivate parents to engage in Internet activities with their children/teenagers and discuss with them Internet threats.
- Information about the tools filtering capability are often missing or misleading, it is necessary to have more transparent information from the software producer so that parents can estimate the risk that children/teenagers have access to inappropriate content through underblocking.
- The tools should include some advice for parents (for example on how to communicate with children/teenagers) not only on the tools'/companies' website but also alongside the installation and configuration process.

Usability

- Installation and configuration procedures should be kept simple and explained in a plain language. The software should:
    - be easy to learn,
    - follow consistent concepts,
    - conform with user expectations about how it works,
    - have an appealing design,
    - provide a good overview on all the features.

- Blocking should be transparent to users.
- Dialogue with the user should be easy to understand and when directed at children/teenagers it should use child/teenager's sensitive language.
- It is important to inform the users that the tool has some limits, what these limits are and what parents can do with this. This information would give users a clear picture of what the settings mean in practice and where they should be more careful.
- The blocking message is not clear addressed in many tools. It should be in plain language so that both children and parents can understand it easily.
- For many tools, the distinction between the installation and configuration is not really clear for parents; this point should be clearly addressed and set.
- Similarly, "reporting" a website is not clear for children/teenagers, i.e. whether the report is sent to the parents or the tool producer; this point should also be properly addressed.
- Providing suggestions of alternative websites if the searched page is blocked can be considered as a good practice.

Effectiveness

- Most of the tools are usually not very effective in filtering harmful web content. Adult content is not the only threat for children/teenagers. The tools should be more effective with regards to content about violence, racism, self-harm, and, also on user-generated content (social networks, blogs, forums, etc.).
- Although not distributed anymore, the AOL filtering tool was satisfactorily effective. Thus, it may serve as a best practice example for other software producers.
- The black list database should be updated at least contemporarily with the update of the tool.

- Databases should be updated regularly. Weekly update could be a solution reflecting rapid changes in the web.
- Most of the filters filter “old web”, while children and teenagers use web 2.0 (social networks, video-sharing websites). The tools have a low effectiveness on this kind of content. This should be better addressed.

Functionality

- Once the installation process is completed, default filtering should be in operation even when the user did not perform or finish the configuration.
- If the creation of user profiles within the filtering tool is linked with the Windows user profile system, parents should be clearly warned (with an alert in a pop-up window or similar) about the need to set up a separate Windows profile and make the admin account password protected. Even better, if there is only one Windows profile, the parent should be guided through the creation of the other profiles.
- Tools should clearly indicate what kind of filtering is performed on the social networks. Is the access to Facebook or similar websites blocked? Is the content filtered? Are interactions with other users filtered or blocked?
- It should be possible, by default or as an option, to make the child/teenager search the web using the safe mode of the three main search engines (Google Safe Search, Bing Safe Search or Yahoo! Safe Search).
- When a page is blocked, the child/teenager should be able to ask the parent to override the blocking when they feel that the blocked content is not harmful.
- Blocking applications: to keep it simple, parents should be provided with a list of applications installed on the computer, for example, in the Windows control panel, instead of having to locate the .exe file on the hard disk.
- Blocking personal data (name, address, phone number) being provided by the child/teenager should be implemented in all tools such as MSN and Skype and also work on websites (blogs, Facebook, webmail).

- Very often blocking categories are based on blocking content in the workplace (i.e. “sports”, “finance”, etc.). Tool providers should consider youth needs when creating the databases for black lists and white lists and provide explanations on what these refer to (to make it more transparent for the parents).
- The reporting of the online activities of the child/teenager and the blocked content should be simple, concise, and provide the essential relevant information. Sometimes, information provided appears to be designed for business use and not for home or private users.
- Communication between children/teenagers and parents is the most important issue in youth protection, therefore, the child/teenager should be always aware of the monitoring of his/her online activities.
- Tools should be more easy to configure and customise so that they reflect the growth and progresses of the child/teenager.
- Copy of the monitoring report should be automatically sent to the child (at least as an option to be activated). The wording of such reports should be clear and comprehensible.

Security

- Harmful content should not be accessible through Google Cache or Google Translator.
- Creation of a password for administration (and uninstallation) should be compulsory.
- The tools should work and be compatible with the most popular browsers, or, alternatively, block the download and installation of other browsers.
- The tools should be resistant to some simple hacking or by-passing actions:
    - Uninstalling the software without a password,
    - Changing date and time of the computer to override time limits of Internet usage,
    - Renaming a blocked application,
    - Closing the software through the Task Manager.

MOBILE PHONES

- For most of the children/teenagers, mobile phones are their personal items. This should be better reflected in mobile phones used by children/teenagers. Tools that work on PCs need to be adapted to mobile phones, not only with regards to the screen size and limited keyboard, but also with regards to addressing children/teeangers appropriately. Moreover, the objectives of parental control should be explained to children/teenagers in a comprehensible manner.
- If the filtering tool is a browser then it should not be possible to use, install, or access the Internet with another browser. Even if it is technically difficult, parents should be given a resolute warning that the default browser should be disabled. For example, parents may need to disable Safari if they want a filtering tool to work.
- Remote access to the software to configure and access the reporting features of the tool should be offered to parents. In particular, parents should be able to remotely access their children's/teenager's mobile phones.
- Parents should have the option to be alerted about attempts to install applications on their children's/teenager's mobile phones, to block the application installation or to block a single application.
- More and more often mobile phone users can access content using an application without the use of a browser. The industry should address this issue. How should content, accessed by users via these apps, be filtered?
- Configuration and monitoring functionality should be accessible for parents using remote PC access.
- Tools should pay attention to apps that provide personal data (including geo-localisation data of children/teenagers) or share the phone books. These functionalities or the apps should be blocked.
- Tools should provide some solutions for controlling and monitoring time spent using the device.

ALTERNATIVE TOOLS

- Number of websites in the white list should be long enough so that children/teenagers do not feel the borders of the “walled garden”.
- Items on the white list should be included carefully and aim at educating children/teenagers.
- White lists should be open so that parents can add additional sites they consider harmful.

METHODOLOGY KEY ISSUES

A description of the methodology adopted to identify users' needs and select parental control tools is provided together with the explanation of the testing methodology and the assesment of results.

METHODOLOGY: KEY ISSUES

Introduction

The benchmarking study is aimed at assessing a set of parental control tools according to ceratin features: functionality, effectiveness, usability, configurability, transparency, and security for the European users. Four benchmarking cycles are foreseen in the whole project, each cycle occurs every 8 months. The results of each benchmarking cycle consist in:

- Detailed test results by tool (fiches/tables) and synthetic results for key findings,
- Online searchable database that allows producing ranking lists according to specific needs of the users.

So far 2 cycles have been already carried out.

The present Report and the applied methodology described herein refer to the **3rd testing cycle**.

The assessment activity is based on a specific methodology that is properly described in the following pages.

Users' Needs

The definition of the users' needs was a starting point of the benchmarking study activity and is a key information to properly read the Report and appraise its content. The users' needs definition oriented the testing activity providing criteria for the tools selection and the dataset creation, the setting of parameters for the tools testing and the principles for the presentation of the benchmarking results.

The analysis of users' needs was carried out starting from a literature of existing studies and reports, complemented by the Consortium experience in the field in terms of the Internet usage and digital threats.

The users' needs with regard to usability have been identified in a first place based on previous experience derived from the work with children's welfare organisations and other experts in the field, especially at the Youth Protection Roundtable.

It was decided to tailor the analysis to the European PARENTS with CHILDREN or TEENAGERS aged in one of the two classes of age: ≤12 years old and ≥13 years old.
The analysis resulted in:

- The identification of main **categories** used to access the Internet: **PC, mobile devices (phones and tablets).**
- The identification of the actions performed by the children/teenagers that might expose the children/teenagers to risks**:**
  - **Visualizing** content present on websites, including content available in streaming and on the Internet through blogs, social networks and forums;
  - **Communicating online** by means of e-mail and social networking and Instant Massaging including video chat, VoIP and chat section available in gaming.
  - **Uploading/downloading and sharing** files (like applications and video) through the Web or Peer to Peer applications.
- The definition of the **needs in terms of functionality/security/effectiveness/usability** as reported in the tables of results in this Report.
- The identification of **three types of activities** that the parents may require the tools to be able to perform:
  - Filtering web-pages according to content topics (including the advertising present on web pages);
  - Blocking the usage of a protocol/application including the control of spending amount through mobile devices;
  - Monitoring the application/protocol usage and the Web content accessed.
- The selection of the **applications/protocols** or more generally the specific Internet spheres mainly used for these activities.

With reference to the content, from the anlysis aroused that parents are mostly concerned with the following topics grouped in two main categories:

Table 27 - Topics parents are most concerned with

Category	Description
Harmful Adult content	**Adult**: Adult sexually explicit content that could impair children's and teenagers' sexual development (main concern).
Other harmful content	**Violent and Crime**: Violent content that could impair children's and teenagers' moral and social development and growth and could instigate damage to others (e.g. weapons and bombs) and content related to skills/activity that could instigate damage to themselves or to others.
	Racist and hate material: Racist and hate material that could instigate damage to another or another's freedom and rights.
	Drug and Self-damage: Illegal drug taking and the promotion of illegal drug use and content that could instigate children and teenagers to damage themselves such as material that promotes suicide, anorexia, self-mutilation.
	Crime: Skills/activity that could instigate damage to themselves or to others.
	Gambling: Content that instigates gambling.

Selection of tools to be tested

The analysis shows that there are different solutions available on the market to address the above mentioned concerns of parents through parental control tools. According to the needs identified, **25 parental control tools** have been selected for this benchmarking testing cycle. The complete list is available in ANNEX 1 to this Report.

The selection of tools has been made to cover emerging parents' needs in terms of:

- categories of devices used (PCs, Mobile devices); in the 3rd cycle Game Consoles have not been finally considered for testing,
- operating systems used (Windows, Mac, Android Linux),
- languages,
- type of solutions (default systems like Microsoft Live family safety or, client software,) and
- capacity to meet parents' needs.

The selection of parental control tools that are the subject of testing and the benchmarking activity is carried out in parallel with the analysis of users' needs.

Tools have been selected according to a number of characteristics as listed below:

- Interface in several EU languages: the filtering tools shall have multilingual user interfaces covering most of the EU languages.
- Filter regardless of the language: the filtering tools should be able to filter multilingual content, at least in one EU language and, preferably, in several EU languages.
- Cover the main devices: the filtering tools have a version that can be executed on the main hardware devices and software systems offering Internet access to the users.
- Type of tools: stand-alone solutions, server solutions, ISP service provided with Internet connection, service provided by phone companies and default tools provided by software manufacturers or embedded in operating systems. Support the main Operating Systems: the filtering tools shall be supported on the main Operative Systems available on selected devices.

- Support the main browsers: the filtering tools shall support the main web browsers (Internet Explorer, Firefox, Google Chrome, Safari).
- Filtering methods (blacklist of URLs, white list of URLs, word lists, text analysis, image analysis).

The group of tools selected always include the main players (market share relevancy criterion) and also some interesting “outsiders” and tools whit interface and filtering capacity covering some less popular EU languages (for instance, Slovenian), as far as they are also available in English language for testing. If available, at least one free tool is also included for each main device.
Some Alternative Tools (walled gardens, child safe browsers) have also been also tested.

Usability tests

Usability of filtering software is crucial for its effectiveness. It is therefore necessary to pay attention to the usability of tools tested. Within the EU-SIP project Youth Protection Roundtable, one result achieved from the work with children's welfare experts and technical specialists was that filtering software products often do not unfold their full potential due to usability deficiencies. If the users are not able to adjust the products to their needs and maintain the software on their own system, the filtering results are poor. Deficiencies in usability shall be detected in the benchmarking by expert reviews.

Learning to know the functionalities of the products is a pre-condition for reviewing the usability. The test of the products' functionalities capabilities is targeted at identifying if the tool has really the functionalities and capabilities required to satisfy the parents' needs.

Testing strategy for Usability and Functionality (Capability)

The functionality capability test and the usability review are two processes going hand in hand. Identifying the spectrum of functions in parental control tools is an integral part of usability testing; testing methods will follow a certain strategy to ensure that no functionality remains undetected, while testing results is strictly separated.

Functionality tests

On a methodological point of view, the parental control tools have been first checked against an open-ended list of standardised functionalities that could be required to a parental control tool like: customising content filtering, allowance of remote management or settings for the provision of personal data.

Functionalities not available have been marked, but not followed further. Available functionalities have been reviewed with regards to their usability by experts in the laboratory. In case the usability reviews reveal further functionalities not detected earlier, these have been also reviewed in terms of usability. This strategic approach has ensured that the whole range of functionalities available is attributed to the product and reviewed in terms of usability. In the below table the list of functionalities to be checked is provided.

Table 28 - List of functionalities to be checked prior to usability test

Area of Need	Functionality/Capability	Specific Issues
Management	Management of User profiles	Create several profiles
	Remote Management	Manage on various devices
	Monitoring	Remote access to monitoring
Filtering Customisation	Topics	Customisation of Filtering Topics
	URLs White List	Restrict Browsing to White List
		Default White List
	URLs Black List	Modification OR Creation
		Creation of User's own Black List
Keywords	Keywords	Default Black List
		Default White List
		Creation of a User's Black List
		Creation of a User's White List
Time	Time Limit Settings	Set a specific time frame or web access duration
		Monitor / observe the time spent online
Blocking Message	Type	Ask for unblocking by parents
		Redirect to safe resources
Usage Restriction	Web	Block Access
		Monitor Access
	Safe search	Availability
	Social Networks	Block Access
		Monitor Usage
	Personal data Provision	Block
	Streaming	Block Access
		Monitor Access
	P2P	Block the application
		Monitor Downloads
	Skype	Block chat
		Block video chat
		Monitor
		Prevent new Contact
	Windows Life Messenger	Block chat
		Block video chat
		Monitor
		Prevent new Contact
	Email	Block email client and/or webmail access

Usability review in laboratory

For each filtering tool a usability review has been accomplished in parallel by two experts in a usability laboratory. This has ensured that usability of the products is tested in a standardised manner to achieve comparable and consolidated results.

Usability testing has considered the relevant usability aspects including: installation, configuration/customisation, general user experience, documentation, supported operating systems and updating capabilities.

The criteria tested in the 3rd Cycle of the SIP BENCH III benchmarking exercise are the following:

Usability

- Installation
- De-installation
- Speed
- Capabilities
- Configuration
- Maintenance
- Reporting
- Terminology
- Overall perception of the system
- Impact on system performance
- Degree of compatibility with client software likely to be found on a typical user's computer.

Configurability

- Parameter configuration
- Setting up classes of users (e.g. age, cultural background)
- Customising filtering criteria
- Possibility to manage and / or limit the time spent online and online purchases (such as app downloads etc.)

The transfer of these review criteria into the design of the usability criteria catalogue as well as the test settings is based first on DIN ISO. Secondly, the testing methodology builds on experiences from SIP BENCH II with regards to what is important to parents in their decision making about a tool (as described in Chapter 2 – Users' Needs Analysis). New technological developments like combined tools for different end devices with similar configuration settings and interfaces require adaptations in the testing methodology. The usability testing does not require an alternative methodology for special tools, like walled garden solutions, as they provide a user interface tool and since that interface is the main focus of usability testing.

The list of criteria has been arranged into **seven sub-categories** according to DIN ISO standards:

Table 29 – Sub-categories of criteria for tools testing

Sub-Category	Processes		
Suitability for the Task	Installation	Configuration	Usage
Self-Descriptiveness	Installation	Configuration	Usage
Controllability	Installation	Configuration	Usage
Conformity with User Expectations	Installation	Configuration	Usage
Error Tolerance	Installation	Configuration	Usage
Suitability for Individualisation	Installation	Configuration	Usage
Suitability for Learning	Installation	Configuration	Usage

In each sub-category the criteria have been applied to the processes of installation, configuration and – where applicable – usage.

Results from the usability review in laboratory

The usability analysis includes the description of the functionalities available and quantitative evaluation, in addition to comments and recommendations on the tools' usability. The quantitative evaluation of the usability is based on the experts reviews. By answering to the questionnaire, the two experts involved had to select answers corresponding to numerical values. Following the testing, the two experts have consolidated their results to achieve integrity and balance. This way, a numerical assessment of the tools' usability has been provided.

Types of Alternative Tools

Recently Alternative Tools have become more popular:

- **Alternative tools** can restrict access to the Internet completely or they can block Internet access for a defined application.
- The so called "**Walled Gardens"** are tools that filter websites based on a white list only. Therefore, there is no problem of underblocking. In walled gardens no harmful content can go through the filter by accident and this method is recommended mainly for young children.
- A third category "**Child Friendly Environment** " aims at educating children and its design is tailored for the youngsters.

Some oftware tools exist that mix the three approaches.

Importance of Joy of Use in Alternative Tools

The error page - in case a website is blocked - is the only part shown to the children/teenagers. Alternative tools aim at engaging children/teenagers through child-adapted tools and so the joy of use is more significant.

Instrument AttrakDiff

Apart from traditional usability, joy of use has also been tested via an additional instrument: the scale "Hedonic Quality" of the AttrakDiff [(2)] inventory. This scale has two subscales:

- Hedonic Quality – Stimulation
- Hedonic Quality – Identity

Overall Usability/UX score for Alternative Tools

In Usability evaluation the focus is on how well users can learn and use a product to achieve their scope.

Usability concentrates on tasks users want to perform with a product/tool. There is a recent tendency to extend the concept of usability to a more holistic view on the interaction between humans and systems, which is referred as User Experience (UX). User experience is a summary of the findings fun of use, aesthetics, emotions, stimulation or attractiveness. These quality aspects are not related to tasks users perform with a product/tool and are thus called non-task related or 'hedonic' aspects.

The overall score calculated in the SIP-BENCH III benchmarking study for Usability is obtained by combining the two elements:

- the classical Usability score and
- the User Experience score (UX / Usability).

The overall score is calculated according to the following formula: (1 x Hedonic Quality + 2 x classical Usability) / 3.

([2]) More information about AttrakDiff can be found at:
http://attrakdiff.de/ or in Hassenzahl, M., Burmester, M., & Koller, F. (2003) *AttrakDiff: Ein Fragebogen zur Messung wahrgenommener hedonischer und pragmatischer Qualität*
In: Ziegler, J. & Szwillus, G. (Hrsg.), Mensch & Computer 2003. Interaktion in Bewegung, S. 187-196, Stuttgart, Leipzig: B.G. Teubner
See: http://attrakdiff.de/files/mc2003_hassenzahl_review.pdf

Testing activity: Security test

The tools have been tested in order to verify if they prevent the user from by-passing or disabling the filter through a specific set of actions.

Peculiarities for Mobile Phones

The test has been carried out with reference to the external tools and based on a subset of criteria as indicated in the table below.

Criteria for Security assessment

The assessment was carried out through a BINARY model (Y/N):

- (Yes): the tool prevents the user from by-passing
- (No): the tool does not prevent the user from by-passing.

Table 30 - Set of criteria and scoring for security

Description of the score	Score	Type of actions tested for by-passing the tool (PC)	Mobile subset
Issues that make the tool easily non-operative	0	Using an alternative browser	x
	0	Disabling or uninstalling the software without a password	x
Critical or severe issues	1	Closing the filtering tool trough the Task Manager	
	1	Accessing the Web pages through the Google cache	x
	1	Reaching a website through translation sites (e.g., Google Translate)	x
	1	Renaming a blocked application	
Issues requiring some computer skills	2	Using the IP address instead of the URL	x
	2	Using a proxy instead of a direct connection to the Internet	x
	2	Changing time and date settings (to overcome time limits	x
Minor issues	3	Starting the computer in Safe Mode	x
No issues identified	4	No issues	

For those features (such as applications/protocols) which imply different aspects to be tested the methodology applied is synthesised in the below table:

Table 31 - Methodology for Security Testing

Action performed for by-passing:	Test bed	The test was successful (YES) if:
Using the IP address instead of the URL	10 IPs	All the IPs were blocked
Using an alternative browser	Google Chrome with 5 URLs	All the IPs were blocked
Using a proxy instead of a direct connection to the Internet	3 Proxies with 5 URLs each	The access to the websites was denied
Reaching a website through translation sites	Google Translate with 5 URLs	The access to the websites was denied
Disabling or uninstalling the software without a password	As managed directly by the tool or from the panel control	
Renaming a blocked application*	Test with Skype and Bit torrent **	Access to the application was blocked
Using Safe Mode		The tool was operative OR the access to the Internet was blocked
Changing time and date settings (to overcome time limits usage)	From the operating system	

*This test is performed only if the tool provides the parents with the possibility to block applications, otherwise it would be not available (N/A).

**This test is performed only for the tool that provides the possibility to block P2P applications and the applications opened despite the blockage (though unable to work) thus allowing the children/teenagers to access the configuration interface and change the port. Otherwise it would be not available (N/A).

Criteria for security scoring

Each action has been associated with a specific score ranging from 0 to 4 and each tool has been given a final score corresponding to the lowest score associated with a by-passing action: action assessed with a negative answer (“NO”). Each action has been given a different weight according to the level of skills required to perform it (the higher the level, the higher the score).

Testing activity: Effectiveness test

The effectiveness test aims at assessing whether a tool is able to block or not a specific harmful page and whether, at the same time, it is able to allow non-harmful pages. The test has been carried on a specific **data set** and followed a precise **methodology**.

Data used to test the tools

A sample of 4,000 pages (containing text, video and images) has been collected as a representative sample of the content a filtering tool is faced with on the Internet.

The sample has the following characteristics:

- It contains both harmful web-pages (that should be blocked by the tool) and non-harmful web-pages (that should not be blocked by the tool);
- Harmfulness of content has been separately valued both for users aged **≤ 12** (notably children) and **and/or for ≥ 13 years old** (notably teenagers).

Tests of user generated content filtering

User-generated content/web 2.0 has been tested through the effectiveness tests: part of the data set test is dedicated to this kind of content. Moreover, some capability tests have been performed by the experts to assess, for instance, the capacity of tools to filter outbound content (publishing content on Facebook or on a blog) or inbound specific content (content personalised according the user, multimedia content with no text).

With regards to user-generated content, these techniques may not be sufficient to provide effective filtering.

Content that is evolving over time

A blog is for instance accessed through a URL as any web page. The main difference is that the content is evolving through time due to comments added to the original post.

Content that is personalised by the user

Many websites offer the possibility to access customised content. For instance, accessing a web-site and after entering user name and password, each user may find different content. This personalised content could be provided upon clear customisation of the user himself or an analysis of user activity. For instance, Gmail provides some contextual advertisement according to the content of user e-mails.

Platforms hosting massively user generated content

A typical example is youtube.com where thousands of new videos are published every day. The uploaded videos cover a diversified type of content: both harmful and non-harmful. In these cases, the tools tested should offer a precise and appropriate solution to the blocking issue: not allowing or blocking all content website, but filtering them according to the harmfulness of the single content. Moreover, more content is published than any rating system can process.

Multimedia content with little textual information

Many of the most visited websites have a strong component of multimedia content like pictures or videos. It is very common to have user-generated resources with only multimedia content such as flickr.com website presenting a user webpage visualising only pictures and few words about the user. It is important to know if filtering tools are able to identify and rate multimedia content by the content itself and not only by the textual elements around it.

Outbound content

When thinking of parental control tools, one considers first the inbound content, in other words the fact that some harmful content could be visualized by the child/teenager. It is important to test also the filtering capacity of outbound content, that is to say whether the tool is able to filter the content that can be produced by the child/teenager (text or photo published on Facebook, chat on Skype, video uploaded on YouTube).

For each of the above mentioned contents the experts have assessed the tools with qualitative tests.

Content analysed int eh bechmarking expercise is related to the following topics: adult content, violence and crime, racism, drugs and self-damage, gambling (see Table 27 - Topics parents are most concerned with)

Content includes various types of web-content (Web sites, social networks, blogs, forums, video sharing sites).

Content analysed is available in the following languages: English, French, Italian, German, Spanish and Polish.

The web-pages have been classified from the parents' point of view.

The chart below shows the data set figures used during the **Effectiveness test**.
The data set does not include e-mail, chat, P2P or VOIP content. In relation to these type of data, the tools have been tested only from a functional point of view (Functionality test), i.e. in terms of the potentiality of the tool to block or monitor the application/protocol usage, see the '**Ethical Issues'** paragraph below.
Each Web page has been manually reviewed to assess the harmfulness and the topic related.

In the following table the data test set composition is shown according to the web type and to content type and appropriateness.

Table 32 - Data set composition

Data according to web type	Data according to content type and appropriateness			
	Harmful Adult content	Other harmful content	Non-harmful sexual related content	Other non-harmful content
Web Web-pages where users are limited to the passive viewing of content that was created for them	960	960	240	240
Web 2.0 Web-pages where users share the content produced directly by themselves (user-generated content). Examples are: blogs, forums, social networks, wiki, video-sharing sites (YouTube like)	640	640	160	160

As it was not possible to automate the tests for mobile phones, the tests have been carried out on a smaller data test set of 1,200 items ensuring the same balance between the various kind of content as for the complete data test set.

Methodology for Effectiveness assessment

The test is aimed at measuring how effectively each tool blocks harmful content and allows non-harmful content. The test has been carried out according to: language, age, topic and Web type (Web / Web 2.0).

For each tool an **automatic test** has been carried out to check if each page was blocked or not. This test has been performed with the default configuration of the software.

The reason for testing the effectiveness with a default configuration is that many users would not go through a detailed process of configuration but use the default configuration.

The tools effectiveness has been assessed in terms of performance in blocking harmful content and allowing non-harmful content. When a tool is not able to perform perfectly, two situations may occur: underblocking and overblocking. Underblocking occurs when the tool allows harmful content; overblocking occurs when the tool blocks non-harmful content.

Therefore, each tool performance has been measured in terms of both underblocking and overblocking (in the final ranking the two situations have been weighed differently according to the user's age:

- % Underblocking measures how much harmful content is not filtered. A good tool having a low underblocking, and your child will be rarely exposed to harmful content.
- % Overblocking measures how much non harmful content is blocked. A good tool will have a low overblocking, and non-harmful content will be rarely blocked.

Testing activity: Usability test

The usability tests are aimed at assessing whether a tool is easy to install, configure and also to use. If the users are not able to adjust the products to their needs and maintain the filter tools on their own system, it will lead to bad filtering results.

The usability has been assessed by a combination of two different approaches – including both end users tests and experts reviews. Two experts' reviews have been carried out independently, the results have been then comprised in one final score for each criterion.

Additionally, from the second cycle on, users have been asked to try out the products and fill in a short usability questionnaire.

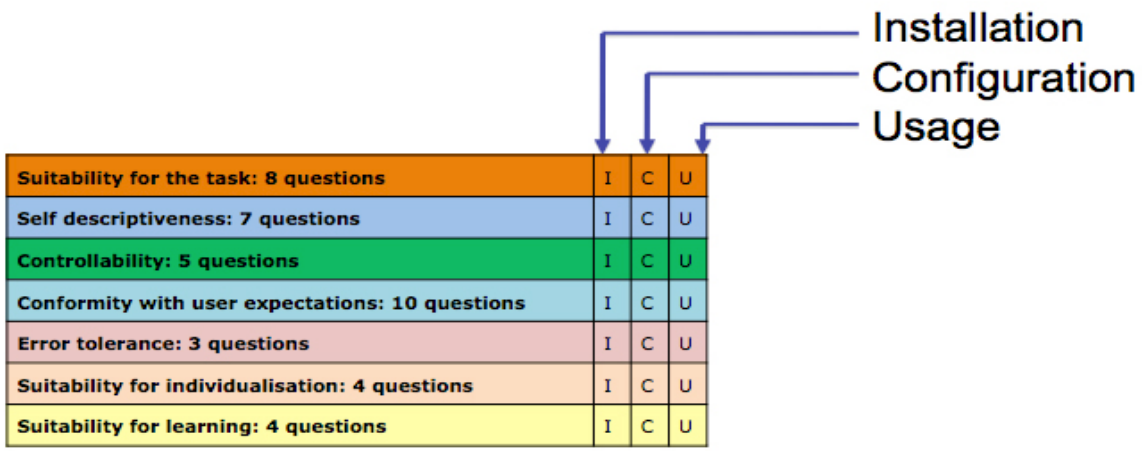
The users' answers have been analysed with regards to their judgment of the products. Based on this procedure, the users' voice is presented in each product's tool fiche as an additional piece of information for the decision making process of parents and other responsible adults in charge of minors.

The questionnaire includes 36 questions assigned to each of the seven sub-categories of criteria as shown in the figure below. Some of the questions have to be answered separately for each of the three processes while others do apply only to one or two of them.

The criteria are considered according to the process of:

- Installation
- Configuration
- Usage of the software.

Figure 3 – Groups of criteria for usability testing



Criteria for usability scoring

The scores for the groups of criteria are weighted according to an elaborated scheme assigning different weights according to the different relevance the criteria group gains in each process.

For the global score for each product:

- installation process has been given a weight of 20 %,
- configuration has been given a weight of 50 %, and
- usage has been given a weight of 30 %.

RESULTS DISCLOSURE AND ETHICAL/LEGAL ISSUES

Results disclosure

The results are published in this Report and on the website also in the format of a searchable database.

The results are mainly provided through tables and graphics. The common scale adopted is 0 to 4. In case of effectiveness, a % view of the results is also provided: % of the webpages underblocked or overblocked. The figures' rationale is explained in each specific testing methodology above and/or in each one of the "How to read the table" box.

Ethical and legal issues

The content/pages covered by the authentication procedure or generally related to the user's personal private communication (social network, chat, Instant Messaging, emailing) has been excluded from the data set used to test the tool effectiveness due to the EC commitment to respect the children's privacy rights.

The exchange on material protected by copyrights, which constitutes the most of material exchanged to Peer to Peer networks, has also been excluded from the data set used to test the tool effectiveness.

GLOSSARY

Anti-virus	The anti-virus software is used to prevent, detect, and remove computer viruses, worms, and Trojan horses.
Application	An application software, also known as an “application” or an "app", is a computer software designed to help the user to perform singular or multiple related specific tasks.
Blacklist	A list that identifies dangerous keywords, URL or website addresses that are blocked by the tool.
Blog	As an abbreviation for "Web blog" is a type or a part of a website usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics, music or video.
Browser	A "Web browser" or "Internet browser" is a software application for retrieving, presenting, and traversing information resources on the World Wide Web.
Cache	A file stored on the hard drive of computers in which the Internet browser stores previously accessed data so that future requests for that data can be processed more quickly.
Configuration	It is an arrangement of functional units according to their nature, number, and chief characteristics. Often, configuration pertains to the choice of hardware, software, firmware, and documentation and affects system function and performance.

Cookie	Also known as a "Web cookie", "browser cookie", and "HTTP cookie", it is a piece of text stored by a user's Web browser.
Download	Downloading is the process of transferring (software, data, character sets, etc.) from a distant to a nearby computer, from a larger to a smaller computer, or from a computer to a peripheral device.
E-mail	"Electronic mail", commonly called email or e-mail, is the method of exchanging digital messages across the Internet or other computer networks.
E-Mail Client	An "email client", "email reader", or more formally "mail user agent" (MUA), is a computer programme used to manage user's email.
File Sharing	File sharing is the practice of distributing or providing access to digitally stored information, such as computer programmes, multi-media (audio, video), documents, or electronic books.
Firewall	A firewall is a part of a computer system or network that is designed to block unauthorised access while permitting authorised communications.
HTTP	The "Hypertext Transfer Protocol" is a networking protocol for distributed, collaborative, hypermedia information systems: it is the foundation of data communication for the World Wide Web.

Installation	Installation (or setup) of a program is the act of putting the program onto a computer system so that it can be executed.
Instant Message	Instant messaging (IM) is a form of real-time direct text-based communication between two or more people using personal computers or other devices, along with shared software clients. The user's text is conveyed over a network, such as the Internet.
ISP (Internet Service Provider)	Also referred to as an "Internet access provider" (IAP), it is a company that offers its customers access to the Internet.
Instant Message	Instant messaging (IM) is a form of real-time direct text-based communication between two or more people using personal computers or other devices, along with shared software clients. The user's text is conveyed over a network, such as the Internet.
Messenger	MSN Messenger (now named Windows Live Messenger) is an instant messaging client created by Microsoft.
Online chatting	It refers to direct one-on-one chat or text-based group chat (also known as "synchronous conferencing"), using tools such as instant messengers, Internet Relay Chat, talkers and possibly Multi-User Domains.
Operating System	An operating system (OS) is a software, consisting of programmes and data, that runs on computers and manages the computer hardware providing common services for efficient execution of various application software. Windows, Mac OS or Linux are operating systems.

Overblocking	It occurs when the tool blocks non-harmful content.
P2P	"Peer-to-peer" (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes.
Protocols	A "communications protocol" is a formal description of digital message formats and the rules for exchanging those messages in or between computing systems and in telecommunications. Protocols may include signalling, authentication and error detection and correction capabilities.
Proxy	A proxy server is a server (a computer system or an application program) that acts as an intermediary for requests from clients seeking resources from other servers.
Skype	It is a software application that allows users to make voice calls and chat over the Internet.
Social network	A social network is an online service, platform, or site where people share ideas, activities, events, and interests within their individual or shared networks. Facebook is a social network.
Temporary Internet Files	Temporary Internet Files is a directory on Microsoft Windows computer systems used by Internet Explorer and other Web browsers to cache pages and other multimedia content, such as video and audio files, from websites visited by the user. This allows such websites to load more quickly the next time they are visited.

Underblocking	It occurs when the tool allows harmful content.
Uninstallation	It is the removal of all or parts of a specific application software.
Upload	Uploading is the sending of data from a local system to a remote system with the intent that the remote system should store a copy of the data being transferred.
URL	A "Uniform Resource Locator" specifies where an identified resource is available and the mechanism for retrieving it. The best-known example of the use of URLs is for the addresses of Web pages on the World Wide Web, such as http://www.example.com/.
Virus	A computer virus is a computer programme that can copy itself and infect a computer.
Web-based email	Email service offered through a web site (a webmail provider) such as Hotmail, Yahoo! Mail, Gmail, and AOL Mail.
Whitelist	A list that identifies keywords, URL or website addresses considered safe.

ANNEX 1 - TOOLS LIST

Device	Tool Name	Test-OS	Download URL
PC / MAC	F-Secure Internet Security	Win7	http://www.f-secure.com/en/web/home_global/internet-security#trial
	K9 Web Protection	Win7	http://www1.k9webprotection.com/getk9/download-software
	Mac Os X Parental Controls	Mac OS X	integrated in OS
	McAfee All Access	Win7	http://home.mcafee.com/store/all-access-security -> free trial
	Norton Online Family	Win7	https://onlinefamily.norton.com/familysafety/loginStart.fs -> "Sign up now" -> Norton Family ohne "Premier"
	Optenet PC	Win7	http://www.optenetpc.com/parental-control.html
	Panda	Win7	http://www.pandasecurity.com/germany/homeusers/solutions/global-protection/ -> Kostenfreie Test-Version herunterladen
	Puresight Owl	Win7	http://puresight.com/download-free-trial.html
	Qustodio	Win7	http://www.qustodio.com/download/
	Trend Micro Online Guardian	Win7	http://www.trendmicro.com/us/home/products/internet-safety/online-guardian/
Mobile	AVG Family Safety	iOS	http://www.avg.com/eu-en/avg-family-safety
	F-Secure Mobile Security	Android	https://play.google.com/store/apps/details?id=com.fsecure.ms.dc
	K9 Web Protection Browser (Mobile)	Android	https://play.google.com/store/apps/details?id=com.bluecoat.k9.android&hl=en
	Mobicip Safe Browser	Android	https://play.google.com/store/apps/details?id=mobicip.com.safeBrowser&hl=en
	Mobiflock	Android	https://play.google.com/store/apps/details?id=com.mobiflock.android&hl=en
	Mobile Parental Filter	Android	http://www.profiltechnology.com/en/home/mobile-parental-filter
	Net Nanny For Android	Android	https://play.google.com/store/apps/details?id=com.contentwatch.ghoti.cp.browser&hl=en
	Norton Online Family (Mobile)	Android	https://play.google.com/store/apps/details?id=com.symantec.familysafety
	Parentsaround (Mobile)	Android	http://www.parentsaround.com/
	Xooloo (Mobile)	Android	http://www.xooloo.net/en/mobile-parental-control
Alternative Tools	Care4teen	Win7	http://www.care4teen.com/download
	Kidzui	Win7	http://www.kidzui.com/
	Magic Desktop	Win7	http://www.magicdesktop.com/en-US/Download
	Famigo	Android	https://play.google.com/store/apps/details?id=com.famigo.sandbox
	Xooloo (Mobile) [younger age group]	Android	http://www.xooloo.net/en/mobile-parental-control