



# **Benchmarking of parental control tools for the online protection of children SIP-Bench II**

**Assessment results and methodology 4<sup>th</sup> Cycle**



## **SAFER INTERNET PROGRAMME**

Empowering and Protecting Children Online



## NOTICE



The project is Funded by the European Union, through the “Safer Internet Programme”  
<http://ec.europa.eu/saferinternet>

Prepared for: European Commission DG Information Society



Prepared by: Cybion Srl and Stiftung Digitale Chancen coordinated by INNOVA Europe  
(hereafter named as “the Consortium”)



**SIP-Bench II**  
Assessment  
Results and  
Methodology  
4th Cycle

## NOTICE

The study aims to benchmark the main functionalities, effectiveness and usability of most currently used filtering software from a technical and ‘fit-for purpose’ point of view, without any commercial or profit-related concern. The European Union, the European Commission or any person acting on their behalf are not responsible for the accurateness, completeness, use of the information contained in this Study, nor shall they be liable for any loss, including consequential loss, that might derive from such use or from the findings of the Study themselves.

The opinions expressed in this study are those of the authors and do not necessarily reflect the views of the European Commission.

Although the authors exercised all reasonable efforts to ensure the accuracy and the quality of the content of this publication, the Consortium assumes no liability for any inadvertent error or omission that may appear in this publication.

Product and company names mentioned herein are trademarks or registered trademarks of their respective owners. The readers are hereby advised and notified that they are under obligation to understand and know the same, and ensure due compliance as required. Please acknowledge that in the tables reporting the testing results, tools name may be shorten for ease of reading. The full name, author and version are provided within the TOOL LIST section.

Copyrights: the findings of the Study, the Report and its content and all the complement material is the sole and exclusive property of the European Commission.

Main references for feedback about the study:

Natalia Mielech  
INNOVA Europe  
Avenue des Arts 24  
B-1000 Bruxelles

# TABLE OF CONTENTS

HOW TO READ THE REPORT	6
INTRODUCTION	7
Objectives	7
Online Database of results	8
What are the parental control tools?	9
What are the main criteria for choosing a tool and type of test carried out?	10
RECOMMENDATIONS FOR PARENTS	14
RECOMMENDATIONS FOR SOFTWARE COMPANIES	16
PARENTAL CONTROL TOOLS: Global Ranking for PC Tools	19
Benchmarking cycles results comparison	22
PARENTAL CONTROL TOOLS FOR PERSONAL COMPUTERS	24
Functionality key findings	25
Functionality table	26
Effectiveness key findings	29
Effectiveness Performance	30
Effectiveness score view	31
Effectiveness overblocking and underblocking	32
Effectiveness related to topic	33
Effectiveness related to language	34
Effectiveness related to age	35
Effectiveness related to Web type	36
Usability key findings	37
Usability table	38
PARENTAL CONTROL TOOLS FOR MOBILE PHONE	39
Functionality key findings	40
Functionality tables	41
Effectiveness key findings	42
Effectiveness score view	44
Effectiveness overblocking and underblocking	45
Usability key findings	46
Usability table	49
PARENTAL CONTROL TOOLS FOR GAME CONSOLES	50
Functionality key findings	51
Functionality tables	52
Effectiveness key findings	53
Effectiveness score view	55
Effectiveness overblocking and underblocking	56
Usability key findings	57
Usability table	60
METHODOLOGY: KEY ISSUES	61
GLOSSARY	82
TOOLS LIST	86



# INDEX OF TABLES

Table 1 – Typology of NEEDS	10
Table 2 – NEEDS for functionality	11
Table 3 – NEEDS for Security	12
Table 4 – NEEDS for Effectiveness	12
Table 5 – NEEDS for Usability	13
Table 6 – PC Tools GLOBAL RANKING for ≤ 12 years old users	20
Table 7 – PC Tools GLOBAL RANKING for ≥ 13 years old users	21
Table 8 – Evolution of average ratings in the first four cycles	22
Table 9 – FUNCTIONALITY key findings	25
Table 10 – PC Tools FUNCTIONALITY results table and overall functionality and security score	27
Table 11 – PC Tools FUNCTIONALITY results table and overall functionality and security score	28
Table 12 – EFFECTIVENESS key findings	29
Table 13 – PC Tools EFFECTIVENESS results: score view	31
Table 14 – PC Tools EFFECTIVENESS results for topics: % of over/underblocked content	33
Table 15 – PC Tools EFFECTIVENESS results for languages: % of over/underblocked content	34
Table 16 – PC Tools EFFECTIVENESS results for users' age: % of over/underblocked content	35
Table 17 – PC Tools EFFECTIVENESS results for Web types: % of over/underblocked content	36
Table 18 – USABILITY key findings	37
Table 19 – PC Tools USABILITY results	38
Table 20 – MOBILE PHONES PARENTAL CONTROL TOOLS – Functionality key findings	40
Table 21 – MOBILE PHONES Tools FUNCTIONALITY – results table and overall functionality and security score	42
Table 22 – MOBILE PHONES Embedded Tools FUNCTIONALITY – results table	42
Table 23 – MOBILE PHONES PARENTAL CONTROL TOOLS – Effectiveness key findings	43
Table 24 – MOBILE PHONES Tools EFFECTIVENESS results – Score view	44
Table 25 – MOBILE Tools EFFECTIVENESS results for topics: % of over/underblocked content	46
Table 26 – MOBILE Tools EFFECTIVENESS results for languages: % of over/underblocked content	46
Table 27 – MOBILE Tools EFFECTIVENESS results for Web types: % of over/underblocked content	47
Table 28 – MOBILE Tools EFFECTIVENESS results for users' age: % of over/underblocked content	47
Table 29 – MOBILE PHONES PARENTAL CONTROL TOOLS – Usability key findings	48
Table 30 – MOBILE PHONES Tools USABILITY results	49
Table 31 – GAME CONSOLE PARENTAL CONTROL TOOLS – Functionality key findings	51
Table 32 – GAME CONSOLES Tools FUNCTIONALITY results table and overall functionality and security score	53
Table 33 – GAME CONSOLES Embedded Tools FUNCTIONALITY results table	53
Table 34 – GAME CONSOLE PARENTAL CONTROL TOOLS – Effectiveness key findings	54
Table 35 – GAME CONSOLES effectiveness related to topic – results table with a score view	55
Table 36 – GAME CONSOLES Tools EFFECTIVENESS results for languages: % of over/underblocked content	57
Table 37 – GAME CONSOLES Tools EFFECTIVENESS results for topics: % of over/underblocked content	57
Table 38 – GAME CONSOLES Tools EFFECTIVENESS results for Web types: % of over/underblocked content	58
Table 39 – GAME CONSOLES Tools EFFECTIVENESS results for users' age: % of over/underblocked content	58
Table 40 – GAME CONSOLES PARENTAL CONTROL TOOLS: Usability key findings	59



**SIP-Bench II**  
Assessment  
Results and  
Methodology  
4th Cycle

# INDEX OF TABLES

---

Table 41 – GAME CONSOLES Tools USABILITY results	60
Table 42 – USERS’ NEEDS: topics parents are concerned with	64
Table 43 – Methodology for functionality test related to blocking	67
Table 44 – Methodology for functionality test related to monitoring	68
Table 45 – Methodology for functionality test related to managing and filtering communication	68
Table 46 – Keeping a communication channel with the users	69
Table 47 – Ad-hoc set of criteria for the embedded tool	71
Table 48 – Set of criteria and scoring for security	72
Table 49 – Methodology for Security Testing	73
Table 50 – Data set composition	75
Table 51 – Criteria for effectiveness scoring – overblocking and underblocking weights	77
Table 52 – Criteria for effectiveness scoring – scoring scale	77
Table 53 – Groups of criteria for usability testing	78
Table 54 – Global rating weights	80



# HOW TO READ THE REPORT?

---

If you are looking for specific information, the text below will guide you through the Report.

## Do you want to know which tool is the best?

→ Go to the **Ranking**. It offers a synthesis of the results for PC tools. This rating was elaborated considering the average user's needs. Please note that your needs may be more specific – in this case, it is advised to look for particular information in the Report.

## Not only PCs!

Your CHILD may access the Internet not only with a **PC**, but also with a **mobile** phone or a **console**.

## Are you looking for a tool that could block Facebook or give you the possibility to limit the time your CHILD spends online?

→ Check the **Functionality** section. You will also discover all the functionalities available for all the tools.

**Does the tool block 50%, 75% or 90% of pornographic websites?** Does the tool allow your CHILD to visit acceptable websites? Does the tool filter well the content in your language?

→ Go to the **Effectiveness** section to see how tools filter the Internet.

Is it easy, difficult or almost impossible to install and configure the tools?

→ Go to the **Usability** section.

## Are you looking for information on a particular tool?

You have already installed a tool or have heard about one?

→ Check the **Tools list** at the end of the Report to see if it was tested. Then go the Tool fiche which is accessible at [www.yprt.eu/sip](http://www.yprt.eu/sip) and provides full test results for this tool.

→ You can also check the sections (**Functionality**, **Effectiveness**, **Usability**) of the Report to see how the tool performed compared to its competitors.

## Some words are unclear for you?

If you do not know what overblocking or black lists are, → go the **Glossary** section at the end of the Report, where we explain all the computer jargon.

## Would you like to know more?

To fully understand the tests we carried out,

→ read the **Methodology** section at the end of the Report.



# INTRODUCTION

---

## Objectives

This Report is the fourth out of 5 reports that will be published on a six-monthly basis containing the results of the Study - Benchmarking of parental control tools for the online protection of children - SIP-Bench II - funded by the European Commission in the framework of the Safer Internet Programme.

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

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

The Report aims to guide the end-users (notably PARENTS) in a clear and immediate way through the assorted panorama of parental control tools available on the market.

The results of the study will be also available online in a downloadable version and through a searchable database that allows producing ranking lists adjusted to the PARENTS' specific needs.

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.



# INTRODUCTION

## Online Database of results

SIP-Benchmark II, Results of the 4th test cycle, Summer 2012

### Ranking for age-group up to twelve years

Click on a column header to sort the ranking list accordingly. You can click also on a tool's name to get the complete data sheet for this particular tool as a pdf file.

Scores range from 0 to 4, with 4 points standing for excellent and 0 points standing for poor.

Show list for age-group thirteen years and older in a new window

Tool name	Functionality	Effectiveness	Usability	Security	Overall score
PureSight Owl	3.4	2.3	3.05	4	2.674
Kaspersky Pure	3.4	2	2.53	3	2.298
Norton Online Family	1.8	2.2	3.07	1	2.246
Telekom Kinderchutz Software	1.9	2.2	2.32	1	2.104
Trend Micro Online Guardian	1.8	1.8	2.88	3	1.968
K9 Web Protection	1.8	1.8	2.83	1	1.886
F-Secure IS 2012	1.3	1.6	2.54	3	1.876
Net Nanny	2.4	1.5	2.36	3	1.868
Windows Live Family Safety	2.8	1.6	2.66	1	1.860
Profil Parental Filter 2	3.4	1.2	2.56	3	1.792
Safe Eyes	3	1.1	2.44	4	1.752
AVG Family Safety	2.4	1.4	2.85	1	1.738
Cybetrixiva	2.8	1	2.3	4	1.644
Enolias Net Filter	1.5	1.5	2.37	1	1.634
McAfee Family Protection	2.7	1.1	2.36	3	1.632
Xoligo	1.5	1.4	2.57	1	1.610
Mac OS X Parental Controls	2.4	1	2.61	3	1.594
CyberPatrol	2.5	1.1	2.36	1	1.456
Whitecat	1.2	1.3	1.81	1	1.370
OpenDNS home	1.6	1	2.72	0	1.312
Net-Intelligence	1.9	1.1	2.12	0	1.280
CyberPatrol	2.2	0.6	2.66	2	1.252
Mobile	1.8	0.9	2.22	1	1.244
Qayide	0.6	0.8	2.04	3	1.208
Goldenet Webfilter PC	2.4	0.8	1.82	0	1.068

Change main selection   Change main selection and keep additional features   Change additional features

Review the results of the first cycle  
Review the results of the second cycle  
Review the results of the third cycle

### How to use the online database

The online database can be found at <http://www.yprt.eu/sip>.

Users select parental control tools according to their individual needs and interests.

In SIP-Benchmark, the tools' effectiveness is tested for the two age groups of children up to twelve years and over thirteen years old. The tools are also differentiated by device, language and operating system. In the database users make their choice of these aspects and get a results table sortable by the overall score or the scores for functionality, effectiveness, usability and security.

In addition, the database provides a tool fiche for each product with detailed information about the product and its test results. These tool fiches are linked with the table and thus can be easily downloaded.



SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle



# INTRODUCTION

---

## What are the parental control tools?

It is important to empower children and young people to use online media safely and responsibly. In addition to that, there are software and other instruments, that can be used to help to protect children. Apart from the clear advantages and opportunities, the Internet carries numerous threats to CHILDREN/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 protect 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 your PC or download an app on your mobile phone.
- 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 may:

- Customize 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 MSN Messenger or Peer to Peer applications.
- Monitor: PARENTS may receive reports on the activity of CHILD/TEENAGER in the Internet, getting the information about the sites that have been accessed or blocked, which applications have been used, etc.

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

The first thing PARENTS should consider is the device used by the CHILDREN/ TEENAGERS to access the Internet. Apart from PC,

which is still the most common device, mobile phones and game consoles are increasingly used by youngsters to access the Internet. In this Report the tools are divided by device. For this benchmarking cycle we have selected and tested:

- 25 PC parental control tools.
- 5 Mobile parental control tools.



# INTRODUCTION

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

The criteria guiding the choice of the most appropriate tool are different according to the parents' specific concerns referring to the following broad 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**.

**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.**

Test Type	What it consists in	Where results are synthesized
<b>FUNCTIONALITY</b>	It assesses which functionalities the tool successfully provides - Does the tool have the functionality you need? For instance, is it possible to block the access to social networks? Is it possible to have a different filtering for your 7 year-old daughter and your 16 year-old son?	Functionality tables
<b>SECURITY</b>	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
<b>EFFECTIVENESS</b>	It measures how much 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? Does the tool allow your CHILD to visit acceptable websites?	Effectiveness tables
<b>USABILITY</b>	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

Table 1 - Typology of NEEDS

In order to have a more detailed overview of the specific testing criteria, the following tables should be complemented with:

- The tools specific and **detailed fiches** (more detailed information is available, especially for functionalities and security).
- The **Methodology** key issues section.



# INTRODUCTION

Read the following needs to find out yours (**PARENTS**) and verify in the related tables which is /are the tool/s that best match/es your requirements:

Area of Need	Description	Table
<b>COMPATIBILITY</b>	If you already have the device, you have to check whether the tool is compatible with the related operating system (for instance Windows, Linux, Mac OS) and the related version (for instance XP, Vista,7).	<b>FUNCTIONALITY</b>
<b>DIFFERENT USERS</b>	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 different customized features.	
<b>CUSTOMIZATION OF FILTERING</b>	If you have specific needs with regards to contents 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 all the remaining.	
<b>KEYWORDS</b>	If you are particularly concerned with some words that your CHILDREN/TEENAGERS may find in content (webpages and communication messages).	
<b>TIME RESTRICTION</b>	If you are worried about the time your child is spending on the Internet (whether browsing, playing or communicating).	
<b>USAGE RESTRICTIONS</b>	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: <ul style="list-style-type: none"> <li>• Surfing the Web (WEB ACCESS).</li> <li>• Watching/listening to video/images/music in streaming (STREAMING through the Web).</li> <li>• Sharing contents by uploading or downloading (P2P).</li> </ul>	
<b>USAGE RESTRICTIONS RELATED TO COMMUNICATION ACTIVITIES</b>	The <b>inward/outward communication activity</b> constitutes one of the PARENTS increasing concern. 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/TEENS could easily come into contact with malicious or potentially dangerous people that profit from the anonymity granted by the username or they could <b>be the actors of bullying, sexting</b> 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. <b>SKYPE, MSN Messenger</b> (Instant Messaging), email client e.g. Outlook, Thunderbird or webmail provider, e.g. Yahoo!, Gmail.	

Table 2 – NEEDS for functionality



# INTRODUCTION

Area of Need	Description	Table
SECURITY	<p>Today, especially TEENAGERS could be able to by-pass or uninstall the tool. Depending on your CHILD's computer skills, you should select the tool also considering its resistance to various type of violations such as:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• By-pass the tool: changing the time settings (if time limit usage restriction is applied).</li> </ul>	SECURITY

Table 3 - NEEDS for Security

Area of Need	Description	Table
TOPIC of CONTENT	You might have different needs in terms of topics to be filtered and should choose the most effective tools accordingly.	EFFECTIVENESS
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 contents 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 ages, 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 <b>age: ≤ 12 and ≥ 13 years old.</b> (more details in the section <i>Methodology key issues</i> )	
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 4 - NEEDS for Effectiveness



# INTRODUCTION

Area of Need	Description	Table
<b>INSTALLATION</b>	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.	<b>USABILITY</b>
<b>CONFIGURATION</b>	You might want to set up different degrees of strength of filtering although 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 easy to learn.	
<b>USAGE</b>	The alert message in case of blocking should be easily understandable for children as well as for their parents. You might want to decide on your tool reacts in case it blocks a website. Not every tool provides a reporting function. Nonetheless, reporting should be easy to handle and understand.	

Table 5 - NEEDS for Usability



# RECOMMENDATIONS FOR PARENTS

---

## PC Tools

### General

- Filtering tools help you to protect your children. However, it is better to treat them only as a partial solution. The filtering process is still not effective enough. Therefore, in addition to using the tool, you should remember the importance of direct communication with your children. Discuss with them their activities on the Internet, find out what they like or dislike, organise some Internet related activities with them and stay up-to-date about the latest trends and threats.
- Parents should keep in mind that filter can be operated at several complementary levels: The operating system (Windows or Mac OS provide some filtering functionalities), The internet service provider, a software or an app installed on the device, the browser, some websites themselves (Google or Bing offers a Safe Search features for instance).
- Some tools are capable of monitoring users' activities in a very detailed way which could violate child's privacy rights. Also, activating the filtering tool, discuss with your children what kind of filter you want to setup and why.
- When a page is blocked, some filtering tools give children the option to ask parents to unblock the page. If you want to keep the communication open with your children 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 children's requests. Not responding to the requests may be very frustrating for your children.
- Most of the tools provide some customizations features and also the possibility to create several accounts. Be sure that you create one account for each of your children configured according to their 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 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 working properly, perform a search on Google with a keyword such as "porn". (Not in front of your child!) When you try to open the first of the available search results, those pages should be blocked.

### 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 being 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 teenager/child 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 by-passed or uninstalled quite easily by children and teenagers. So, check periodically that the filtering tool is still installed and working.



# RECOMMENDATIONS FOR PARENTS

---

## 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?
- 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 the time spent using the software to within a specific timeframe. In these cases, be aware that there are very few tools that can block/filter communication activities and that their features will differ.

## Consoles

- Be aware that your children may use their game consoles to access the Internet.
- Be aware that your children may interact with other people when playing games. These interactions are not normally filtered by parental control tools.

## Mobile phones

- Many applications do not address the children appropriately and do not communicate clearly the objectives of parental control tool. Remote management options allow parents controlling their children unperceived while other tools give access to monitoring and reporting only in the child's mobile phone. Nevertheless, parents should discuss with children the issues of filtering, monitoring and reporting and not do this in secret.
- Most applications consist of browsers that replace the default browsers installed on the mobile phones. It is often possible to by-pass the parental control tool by installing another browser.
- 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.



# RECOMMENDATIONS FOR SOFTWARE COMPANIES

---

## General

- 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 talk with them about Internet threats.

## Usability

- Installation and configuration procedures should be kept simple and explained in 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 features.
- Blocking should be transparent to users.
- Dialogue with the user should be easy to understand and when directed at children should use child sensitive language.

## Effectiveness

- Most tools are usually not very effective in filtering harmful web content. In any case, adult content is not the only threat to children. It is important that such tools also be much more effective with regard 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 database containing the black list should be updated at least with every update of the tool.

## Functionality

- After the installation process is completed, default filtering should be in operation even when the user did not perform or finish a configuration.





# RECOMMENDATIONS FOR SOFTWARE COMPANIES

---

- 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 in the creation of the other profiles".
- Tools should clearly indicate what kind of filtering is performed on 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 force the child/teenager to 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 parents).
- The reporting of the online activities of the child/teenager and the blocked content should be simple, concise, and provide the essential pertinent information. Sometimes, information provided appears to be designed for business use and not for home or private users.
- Communication between children and parents is the most important issue in youth protection, therefore, the child should always be aware of the monitoring of his/her online activities.

## 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.



# RECOMMENDATIONS FOR SOFTWARE COMPANIES

---

## Mobiles

- For most of the children, mobile phones are their personal items. Industry should better reflect this particular situation of mobile phones used by children. 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 appropriately. Moreover, objectives of parental control should be explained to children 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 mobile phones.
- Parents should have the option to be alerted about attempts to install applications on their children's mobile phones, to block the application installation or to block a single application.
- Increasingly with mobile phones, 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 by parents using remote PC access.
- Tools should pay attention to apps that provide personal data (including geo-localisation data of teenagers) or share the phone books. These functionalities or the apps should be blocked.
- Tools should provide some solutions for spending monitoring.

## Consoles

- Among children who access the Internet, 26% use game consoles.
- The industry must give more attention to the game consoles market to raise awareness that consoles are used to access the Internet.
- It should be possible to configure the tool from a remote PC as many parents are unfamiliar with consoles.
- Tools should be effective and provide a satisfactory filtering level.



## **PARENTAL CONTROL TOOLS: GLOBAL RANKINGS for PC TOOLS**

---

The global ranking was calculated only for the PC tools since there were only few tools for mobiles that were able to filter webpages.

The PC tools are ranked on the basis of the overall scores assigned for each of the tests carried out (functionality, effectiveness, security and usability).

**Two final rankings** were produced **according to the two age categories** (for details on the ranking criteria see: *Methodology key issues* section).



# PARENTAL CONTROL TOOLS: GLOBAL RANKINGS for PC TOOLS



SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

PC Tools ranking assessed for ≤ 12 years old users								
Rank/25	Tool	Functionality	Effectiveness	Usability	Security	Rating		* Price €
	<i>Average across 25 tools</i>	<b>2,16</b>	<b>1,36</b>	<b>2,47</b>	<b>2,28</b>	<b>1,72</b>		
	<i>Best values</i>	<b>3,4</b>	<b>2,3</b>	<b>3,07</b>	<b>4,0</b>	<b>2,67</b>		
1	PURESIGHT OWL	3,4	2,3	3,05	4,0	2,67	●●●○	45,00
2	NORTON ONLINE FAMILY	1,8	2,2	3,07	4,0	2,49	●●●○	Free
3	KASPERSKY PURE	3,4	2,0	2,53	3,0	2,30	●●●○	59,95
4	K9 WEB PROTECTION	1,6	1,8	2,63	4,0	2,13	●●●○	Free
5	TELEKOM KINDERSCHUTZ SOFTWARE	1,9	2,2	2,32	1,0	2,10	●●○○	24,95
6	TREND MICRO ONLINE GUARDIAN FOR FAMILIES	1,6	1,6	2,88	3,0	1,97	●●○○	23,40
7	NET NANNY	2,4	1,5	2,38	4,0	1,95	●●○○	31,20
8	F-SECURE INTERNET SECURITY 2012	1,3	1,6	2,54	3,0	1,88	●●○○	49,95
9	WINDOWS LIVE FAMILY SAFETY	2,8	1,6	2,66	1,0	1,86	●●○○	Free
10	PROFIL PARENTAL FILTER 2	3,4	1,2	2,56	3,0	1,79	●●○○	39,99
11	SAFE EYES	3,0	1,1	2,44	4,0	1,75	●●○○	37,00
12	AVG FAMILY SAFETY	2,4	1,4	2,85	1,0	1,74	●●○○	52,55
13	MCAFEE FAMILY PROTECTION	2,7	1,1	2,36	4,0	1,71	●○○○	36,95
14	CYBERSIEVE	2,8	1,0	2,30	4,0	1,64	●○○○	26,48
15	ENOLOGIC NET FILTER	1,5	1,5	2,37	1,0	1,63	●○○○	39,95
16	XOOLoo	1,5	1,4	2,57	1,0	1,61	●○○○	29,99
17	MAC OS X PARENTAL CONTROLS	2,4	1,0	2,61	3,0	1,59	●○○○	Free
18	MOBICIP	1,8	0,9	2,22	4,0	1,48	●○○○	8,00
19	CYBERSITTER	2,5	1,1	2,36	0,0	1,38	●○○○	30,16
20	OPENDNS HOME	1,6	1,0	2,72	0,0	1,31	●○○○	Free
21	WHITENET	1,2	1,3	1,81	0,0	1,29	●○○○	24,95
22	NET-INTELLIGENCE	1,9	1,1	2,12	0,0	1,28	●○○○	37,43
23	CYBERPATROL	2,2	0,6	2,66	2,0	1,25	●○○○	30,00
24	DAVIDE	0,6	0,8	2,04	3,0	1,21	●○○○	60,00
25	OPTENET WEBFILTER PC	2,4	0,8	1,82	0,0	1,07	●○○○	32,00

Table 6 - PC Tools GLOBAL RANKING for ≤ 12 years old users

\*Prices are for a one-year licence

# PARENTAL CONTROL TOOLS: GLOBAL RANKINGS for PC TOOLS



SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

PC Tools ranking assessed for ≥ 13 years old users								
Rank/25	Tool	Functionality	Effectiveness	Usability	Security	Rating		* Price €
	<i>Average across 25 tools</i>	<b>2,16</b>	<b>1,35</b>	<b>2,47</b>	<b>2,28</b>	<b>1,82</b>		
	<i>Best values</i>	<b>3,4</b>	<b>2,1</b>	<b>3,1</b>	<b>4,0</b>	<b>2,74</b>		
1	PURESIGHT OWL	3,4	2,1	3,05	4,0	<b>2,74</b>		45,00
2	NORTON ONLINE FAMILY	1,8	1,9	3,07	4,0	<b>2,44</b>		Free
3	KASPERSKY PURE	3,4	1,5	2,53	3,0	<b>2,18</b>		59,95
4	NET NANNY	2,4	1,5	2,38	4,0	<b>2,17</b>		31,20
5	K9 WEB PROTECTION	1,6	1,6	2,63	4,0	<b>2,17</b>		Free
6	PROFIL PARENTAL FILTER 2	3,4	1,4	2,56	3,0	<b>2,13</b>		39,99
7	TREND MICRO ONLINE GUARDIAN FOR FAMILIES	1,6	1,7	2,88	3,0	<b>2,12</b>		23,40
8	SAFE EYES	3,0	1,2	2,44	4,0	<b>2,10</b>		37,00
9	MCAFFEE FAMILY PROTECTION	2,7	1,2	2,36	4,0	<b>2,05</b>		36,95
10	F-SECURE INTERNET SECURITY 2012	1,3	1,7	2,54	3,0	<b>2,01</b>		49,95
11	CYBERSIEVE	2,8	1,0	2,30	4,0	<b>1,94</b>		26,48
12	WINDOWS LIVE FAMILY SAFETY	2,8	1,7	2,66	1,0	<b>1,93</b>		Free
13	TELEKOM KINDERSCHUTZ SOFTWARE	1,9	1,9	2,32	1,0	<b>1,85</b>		24,95
14	MAC OS X PARENTAL CONTROLS	2,4	1,0	2,61	3,0	<b>1,80</b>		Free
15	AVG FAMILY SAFETY	2,4	1,3	2,85	1,0	<b>1,71</b>		52,55
16	MOBICIP	1,8	0,8	2,22	4,0	<b>1,69</b>		8,00
17	ENOLOGIC NET FILTER	1,5	1,5	2,37	1,0	<b>1,60</b>		39,95
18	XOOLoo	1,5	1,3	2,57	1,0	<b>1,54</b>		29,99
19	DAVIDE	0,6	1,1	2,04	3,0	<b>1,51</b>		60,00
20	CYBERPATROL	2,2	0,7	2,66	2,0	<b>1,48</b>		30,00
21	CYBERSITTER	2,5	1,2	2,36	0,0	<b>1,42</b>		30,16
22	NET-INTELLIGENCE	1,9	1,2	2,12	0,0	<b>1,30</b>		37,43
23	OPENDNS HOME	1,6	1,0	2,72	0,0	<b>1,27</b>		Free
24	OPTENET WEBFILTER PC	2,4	1,1	1,82	0,0	<b>1,25</b>		32,00
25	WHITENET	1,2	1,1	1,81	0,0	<b>1,09</b>		24,95

Table 7 - PC Tools GLOBAL RANKING for ≥ 13 years old users

\*Prices are for a one-year licence

# Benchmarking cycles results comparison

Comparison of the results of the first three cycles reveals progress made by these tools and the industry. Ratings used for this comparison were calculated from effectiveness, functionality, security and usability scores. For each cycle, all PC tested tools have been considered. The values of effectiveness scores are not compared as the calculation method has been changed for the 4<sup>th</sup> cycle.

	Functionality	Usability	Security
1st Cycle	2,1	2,6	2
2nd Cycle	2,1	2,51	1,44
3rd Cycle	2,2	2,48	1,9
4th Cycle	2,1	2,47	2,3

Table 8 - Evolution of average ratings in the first four cycles

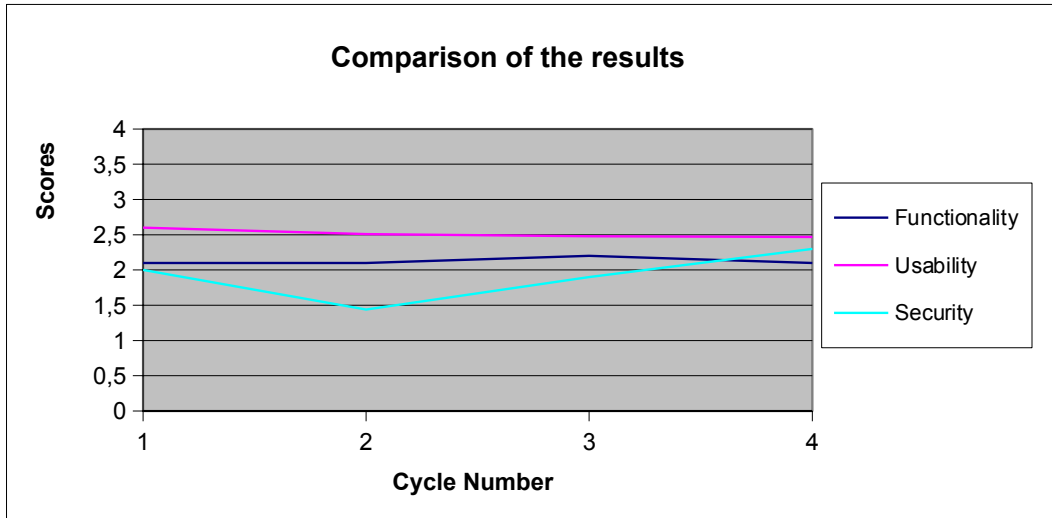


Figure 1 - Graphical representation of the evolution of average ratings in the first four cycles



# Benchmarking cycles results comparison

---

## Security

Average security is almost stable during the first four cycles, it should be noted that 10 out of 25 tools have a score equal to 0 or 1, this makes them inoperative from a security point of view. Software producers did not succeed in correcting major security flaws, even if some tools are slightly improving.

## Functionalities

**Average functionalities rating is almost the same** in the first four cycles (2.1). There is no significant improvement in this field.

## Usability

The average usability rating of 2,47 is almost the same compared to the 3<sup>rd</sup> cycle (2,48).

The usability of software products usually improves with revised or updated versions. Differences in the rating of the products' usability are mainly due to the change in the experts' judgement caused by the perception of new or updated products with improved usability.

For the 22 tools tested in the 2<sup>nd</sup> cycle and 3<sup>rd</sup> cycle:

- 5 products scored less than in the 3<sup>rd</sup> cycle.
- 3 products scored better than in the 3<sup>rd</sup> cycle.
- 14 products scored almost the same.





PC

**SIP-Bench II**  
Assessment  
Results and  
Methodology  
4th Cycle

# 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 the CHILDREN/TEENAGERS to access the Web pages, share experiences and contents through social networks, communicate with people.



## PC PARENTAL CONTROL TOOLS: Functionality key findings

<p style="text-align: center;"><b>None of the 25 tested tools reaches the complete functionality coverage.</b>  <b>The most complete one is rated 3,4 on a 4 scale. 12 tools are rated under 2.</b>  <b>The 3 highest scoring products are: Kaspersky (3,4), PureSight (3,4) and Profil (3,4).</b></p>	
<b>Customization of Web content filtering</b>	Most of the tools provide the PARENT with the complete set of customization functionalities (topic + URL and black/white lists). Keywords filtering option is uncommon: 10 out of 25 tools offer this option. 16 tools give the possibility to block access to social networks and 15 tools give the possibility to force the user to use the Safe Search functionality of the most common search engines.
<b>Protocols and Applications</b>	The tools rarely provide the option to block an <b>entire protocol</b> whereas blocking <b>applications</b> are more common.
<b>Management of users profiles</b>	Most of the tools enable the PARENTS to create and manage different profiles for users with different needs. 5 tools can be used only with one profile.
<b>Restricting Web access</b>	22 tools enable PARENTS to block the access specifically to the Internet (whether using a specific functionality or using the “time restrictions”).
<b>Streaming</b>	The majority of the tools are able to block Web based streaming provided by YouTube, if not with a specific options, at least by adding it to a black list. Blocking the specific application which allows streaming such as Windows Media Player is possible for less than half of the tools.
<b>Communication activities</b>	18 tools are able to block MSN Messenger and 16 are able to block Skype. Possibility to filter contacts is still rare: only 4 tools provide a functionality that works correctly for MSN. 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 Voip or Video chat only.
<b>Monitoring</b>	Most of the tools are able to provide the PARENTS with at least basic report on the users’ web activity (visited websites or violations). Some of these also offer specific alerts with violations and a more detailed report. There are few tools able to report on protocols/applications usage. 11 tools are able to monitor MSN, only 3 tools give the parent information on their child’s activity on social networks while no tool is able to provide information on the number and names of downloaded files through Peer to Peer applications (e.g.: eMule or BitTorrent).
<b>Interaction</b>	Only 8 tools give the PARENT possibility to personalise the blocking page. None of the tools redirects the CHILD/TEENAGER to safe research.
<b>Language Interface</b>	English is the most frequent language whereas the tools’ choice is limited for many other European languages.
<b>Security</b>	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.



**SIP-Bench II**  
 Assessment  
 Results and  
 Methodology  
 4th Cycle

Table 9 – Functionality key findings

# PC PARENTAL CONTROL TOOLS: Functionality table

## How to read the table

The table shows the tools capability (Yes/No) to satisfy the PARENTS NEEDS (see Table 2 – NEEDS for functionality) as grouped in major area of concern and related to specific issues. As far as the URLs White/Black lists and keywords are concerned, the tables show a synthetic view of the outputs which included the testing of more detailed issues (such as presence of a default URLs/keywords white list, creation of a user's own URLs/keywords both white and black list, restriction of browsing to a URLs white list): in the table the test was represented as positive (Y) if at least one of the specific functionalities was successfully tested. The detailed test results are available in each tool fiche that provides also information on: TYPE OF PRODUCT (Client/Server), OS (specific), PRICE, LANGUAGE. Note: in case of Security Suite (see **Appendix - Tool list**) the functionalities were analyzed with reference to the parental control interface and not with reference to the Security/Firewall interface.

<b>Y:</b>	Yes
<b>N:</b>	No
<b>Y:</b>	Web-based only (web-based streaming or email)
<b>B:</b>	Block
<b>M:</b>	Monitor
<b>Cf:</b>	Contact Filter
<b>B/W list:</b>	Black/White list
<b>W, M, L (OS):</b>	Windows, Mac, Linux

<b>F:</b>	<b>Global Functionality Rate.</b> The tool was scored from 0 to 4 according to the number of the tested functionalities covered (see: Methodology key issues section):
0 ≥ 1	Very poor functionality coverage (up to 25% of functionalities)
1 ≥ 2	Poor functionality coverage (between 25% and 50% of functionalities)
2 ≥ 3	Good functionality coverage (between 50% and 75% of functionalities)
3 > 4	Very good functionality coverage (between 75% and 100% of functionalities)
4	Excellent functionality coverage (100% of functionalities covered)

<b>S:</b>	<b>Global Security Rate.</b> The security was scored from 0 to 4 (for criteria see: <i>Methodology key issues</i> section):
0 =	Weaknesses that make the tool easily non-operative (the tool is unsecured against plain child/teenager hacking attacks)
1 =	Critical or severe weaknesses
2 =	Critical or severe weaknesses requiring some computer skill
3 =	Minor weaknesses
4 =	No relevant weakness identified (the tool is almost secured against main child/teenager hacking attacks)



# PC PARENTAL CONTROL TOOLS: Functionality table

Area of need	Compatibility	Mgmt		Filtering customization			Keywords	Time	Interaction	F	S
Functionality	OS	Users	Access	Content filtering			keywords	Time	Interaction	Score	Score
Specific issue	W/M/L	Users profiles	Monitor	Topics	Urls White list	Urls Black list	B/W list	Time limit	Blocking Message		
KASPERSKY PURE	W	Y	N	Y	Y	Y	Y	Y	Y	3,4	3
PROFIL PARENTAL FILTER 2	W	Y	Y	Y	Y	Y	N	Y	Y	3,4	3
PURESIGHT OWL	W	Y	Y	Y	Y	Y	Y	Y	N	3,4	4
SAFE EYES	W, M	Y	Y	Y	Y	Y	Y	Y	N	3,0	4
CYBERSIEVE	W	Y	Y	Y	Y	Y	Y	Y	N	2,8	4
WINDOWS LIVE FAMILY SAFETY	W	Y	Y	Y	Y	Y	N	Y	Y	2,8	1
MCAFFEE FAMILY PROTECTION	W	Y	Y	Y	Y	Y	N	Y	N	2,7	4
CYBERSITTER	W	Y	Y	Y	Y	Y	Y	Y	Y	2,5	0
AVG FAMILY SAFETY	W	Y	Y	Y	N	Y	N	Y	N	2,4	1
MAC OS X PARENTAL CONTROLS	M	Y	N	N	Y	Y	N	Y	N	2,4	3
NET NANNY	W, M	Y	Y	Y	Y	Y	Y	Y	Y	2,4	4
OPTENET WEBFILTER PC	W	Y	N	Y	Y	Y	Y	Y	N	2,4	0
CYBERPATROL	W	Y	N	Y	Y	Y	Y	Y	N	2,2	2
NET-INTELLIGENCE	W	Y	Y	Y	Y	Y	N	Y	N	1,9	0
TELECOM KINDERSCHUTZ SOFTWARE	W	Y	N	Y	Y	Y	Y	Y	Y	1,9	1
MOBICIP	W, L	Y	Y	N	Y	Y	N	Y	N	1,8	4
NORTON ON LINE FAMILY	W, M	Y	Y	Y	N	Y	N	Y	Y	1,8	4
K9 WEB PROTECTION	W, M	N	N	Y	Y	Y	Y	Y	N	1,6	4
OPENDNS HOME	W, M, L	Y	Y	Y	Y	Y	N	N	Y	1,6	0
TREND MICRO ON LINE GUARDIAN FOR FAMILIES	W	Y	Y	Y	N	Y	N	Y	N	1,6	3
ENOLOGIC NET FILTER	W	Y	N	Y	N	Y	N	Y	N	1,5	1
XOOLoo	W, M	Y	N	Y	Y	Y	N	Y	N	1,5	1
F-SECURE INTERNET SECURITY 2012	W	Y	N	Y	Y	Y	N	Y	N	1,3	3
WHITENET	W	N	N	N	Y	Y	N	Y	N	1,2	0
DAVIDE	W,M,L	Y	N	Y	N	N	N	N	N	0,6	3

Table 10 - PC Tools FUNCTIONALITY results table and overall functionality and security score (part 1)

Note: The value present in the column F (Global Functionality Rate) and S (Global Security Rate) is based on the values on results of the two parts of the table (the second part is on the next page).



PC

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

# PC PARENTAL CONTROL TOOLS: Functionality table

Area of need	Usage restriction																	F	S
	Web access		Safe Search	Social Networks		Personal data	Streaming		P2P		Skype			MSN			email	Score	Score
	B	M	Availability	B	M	B	B	M	B	M	B	M	Cf	B	M	Cf	B		
KASPERSKY PURE	Y	Y	Y	Y	Y	Y	Y*	Y	Y	N	Y	Y	N	Y	Y	Y	Y	3,4	3
PROFIL PARENTAL FILTER 2	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	Y	N	Y	Y	Y	Y	3,4	3
PURESIGHT OWL	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	3,4	4
SAFE EYES	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y	N	Y	Y	N	Y	3,0	4
CYBERSIEVE	Y	Y	Y	Y	N	N	Y*	Y	Y	N	N	Y	N	Y	Y	N	Y	2,8	4
WINDOWS LIVE FAMILY SAFETY	Y	Y	Y	Y	N	N	Y*	Y	Y	N	Y	Y	N	Y	Y	Y	Y*	2,8	1
MCAFFEE FAMILY PROTECTION	Y	Y	Y	Y	Y	N	Y	N	Y	N	Y	Y	N	Y	Y	N	Y	2,7	4
CYBERSITTER	Y	Y	N	Y	N	N	Y	N	Y	N	Y	N	N	Y	N	N	Y	2,5	0
AVG FAMILY SAFETY	Y	Y	Y	Y	N	N	Y	Y	Y	N	Y	N	N	Y	Y	N	Y	2,4	1
MAC OS X PARENTAL CONTROLS	Y	Y	N	N	N	N	Y	Y	Y	N	Y	Y	N	Y	Y	N	Y	2,4	3
NET NANNY	Y	Y	Y	Y	N	N	Y	N	N	N	N	N	N	Y	Y	N	Y	2,4	4
OPTENET WEBFILTER PC	Y	Y	Y	Y	N	N	Y	N	Y	N	Y	N	N	Y	N	N	Y	2,4	0
CYBERPATROL	Y	Y	N	N	N	Y	Y	N	Y	N	Y	N	N	Y	N	N	Y	2,2	2
NET-INTELLIGENCE	Y	Y	Y	Y	N	N	N	Y	N	N	N	Y	N	N	Y	N	N	1,9	0
TELECOM KINDERSCHUTZ SOFTWARE	Y	N	N	Y	N	N	Y	N	N	N	Y	N	N	Y	N	N	Y	1,9	1
MOBICIP	Y	Y	Y	N	N	N	N	Y	Y	N	Y	N	N	Y	N	N	N	1,8	4
NORTON ON LINE FAMILY	N	Y	Y	Y	N	Y	Y	N	N	N	N/A	N/A	N/A	N/A	N/A	N/A	Y	1,8	4
K9 WEB PROTECTION	Y	Y	Y	Y	N	N	Y	N	N	N	N	N	N	N	N	N	Y	1,6	4
OPENDNS HOME	Y	Y	N	Y	N	N	Y	N	N	N	N	N	N	N	N	N	Y	1,6	0
TREND MICRO ON LINE GUARDIAN FOR FAMILIES	Y	Y	N	Y	N	Y	Y	N	N	N	N	N	N	N	N	N	Y	1,6	3
ENOLOGIC NET FILTER	N	Y	N	N	N	Y	N	Y	N	Y	Y	N	N	Y	N	N	N	1,5	1
XOOLoo	N	Y	N	N	N	N	Y*	N	Y	N	Y	N	N	Y	N	N	Y*	1,5	1
F-SECURE INTERNET SECURITY 2012	Y	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	Y	1,3	3
WHITENET	Y	Y	N	N	N	N	N	N	Y	N	Y	N	N	Y	N	N	N	1,2	0
DAVIDE	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	0,6	3

Table 11 - PC Tools FUNCTIONALITY results table and overall functionality and security score (part 2)



PC

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

## PC PARENTAL CONTROL TOOLS: Effectiveness key findings



**SIP-Bench II**  
Assessment  
Results and  
Methodology  
4th Cycle

<p>In general, tools have low effectiveness.</p> <p>The highest scoring products for <math>\leq 12</math> years old children are PURESIGHT OWL (2,3 out of 4), TELEKOM KINDERSCHUTZ SOFTWARE and NORTON ONLINE FAMILY (2,2 out of 4). The highest scoring products for <math>\geq 13</math> years old children are PURESIGHT OWL (2,1 out of 4), TELEKOM KINDERSCHUTZ SOFTWARE and NORTON ONLINE FAMILY (1,9 out of 4)</p> <p>Only three tools out of 25 scored above 2 for the <math>\leq 12</math> years old children class and one 2 for <math>\geq 13</math> years old children class.</p>	
<b>Underblocking/ Overblocking</b>	<p>The underblocking rate is higher than 20 % for all tested tools.</p> <p>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.</p> <p>It might be hypothesised 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.</p> <p>Less than 20% of the data test set used belongs to the existing black lists and the data test set consists of 6000 items. This may explain why effectiveness results may be lower than the ones proposed by other similar tests.</p>
<b>Age classes</b>	<p>The tools perform quite similarly with a configuration for the two age classes (<math>\leq 12</math> and <math>\geq 13</math>).</p> <p>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:</p> <ul style="list-style-type: none"> <li>• No level of filtering available.</li> <li>• Personalisation by content categories that both applies to children and teenagers.</li> </ul> <p>In most of the cases, the tools perform better for the <math>\geq 13</math> age class, as it the scoring gives less importance to underblocking for teenagers that for children.</p>
<b>Web and Web 2.0</b>	<p>The tools present lower effectiveness on Web 2.0 content. In particular, the tools which achieve better results than the others have generally a 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 webiste 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.</p>
<b>Topics</b>	<p>The adult content is better filtered than the "other" content categories. WHITENET filters only adult content. Some tools achieve an underblocking lower than 10% (NORTON ONLINE FAMILY, KASPERSKY PURE, K9 WEB PROTECTION, TELEKOM KINDERSCHUTZ SOFTWARE), which is almost good. On the "other" content categories (except of gambling) only a few tools has an underblocking close to 30%. Most of them have very low effectiveness (more than 70% of underblocking).</p>
<b>Languages</b>	<p>Tools work better on English languages than other languages. Even considering only English content, all the tools have an underblocking rate higher than 20%. Some tools provide better results for one language, like TELEKOM KINDERSCHUTZ SOFTWARE (German and Spanish) or XOOLOO for French, but there is no outstanding tool for languages other than English.</p>

Table 12 – Effectiveness key findings

# PC PARENTAL CONTROL TOOLS: Effectiveness Performance

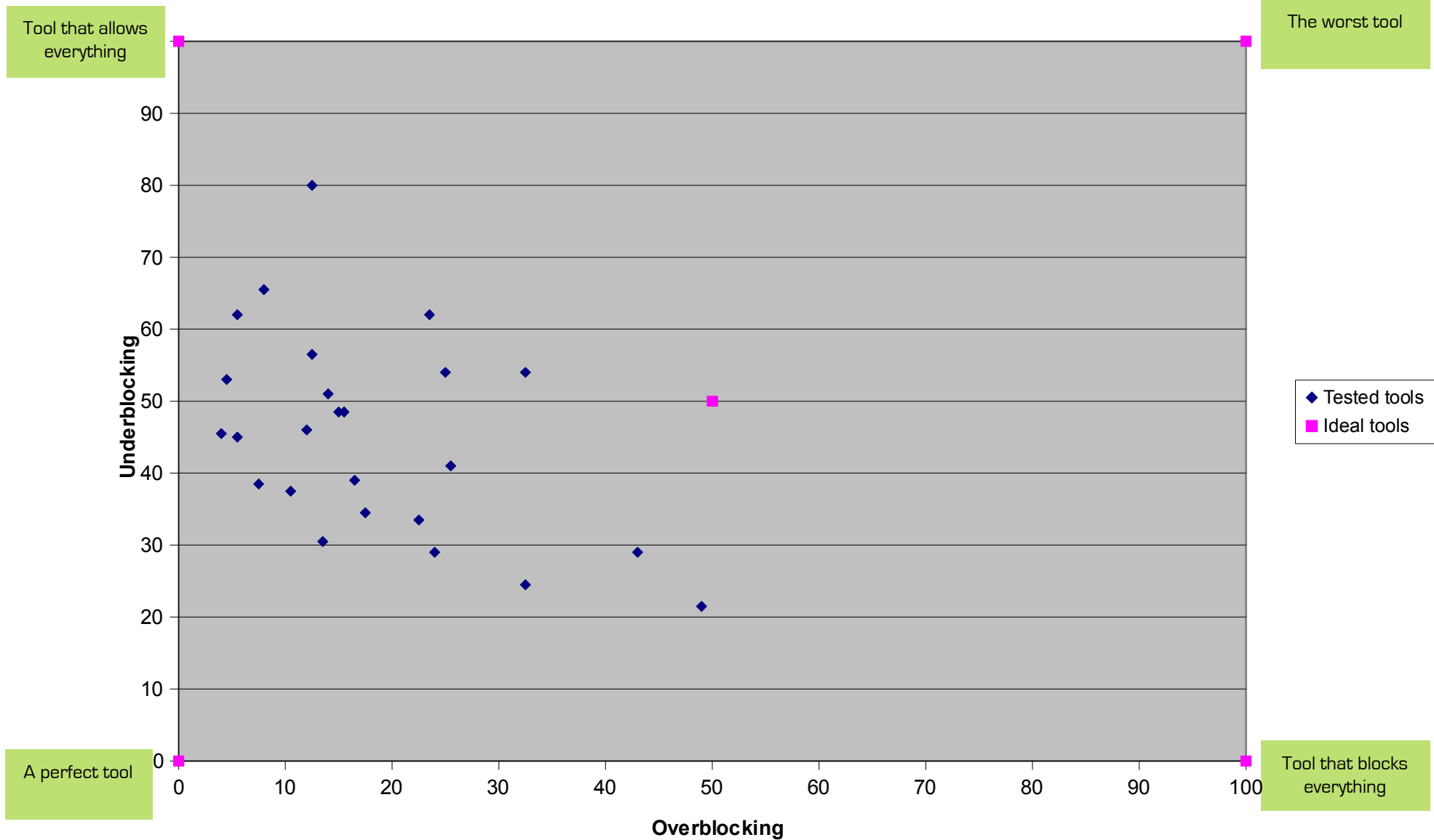


Figure 2 - Each point represents the overblocking and underblocking of a tool.

# PC PARENTAL CONTROL TOOLS: Effectiveness (score view)

Effectiveness assessed according to topic and age

Topic	Adult		Other		Overall Score	
	<12	>13	<12	>13	<12	>13
AVG FAMILY SAFETY	2,8	2,6	0,0	0,0	1,4	1,3
CYBERPATROL	1,2	1,4	0,0	0,0	0,6	0,7
CYBERSIEVE	2,0	2,0	0,0	0,0	1,0	1,0
CYBERSITTER	2,2	2,4	0,0	0,0	1,1	1,2
DAVIDE	1,6	2,2	0,0	0,0	0,8	1,1
ENOLOGIC NET FILTER	3,0	3,0	0,0	0,0	1,5	1,5
F-SECURE INTERNET SECURITY 2012	3,2	3,4	0,0	0,0	1,6	1,7
K9 WEB PROTECTION	3,6	3,2	0,0	0,0	1,8	1,6
KASPERSKY PURE	3,2	2,4	0,8	0,6	2,0	1,5
MAC OS X PARENTAL CONTROLS	2,0	2,0	0,0	0,0	1,0	1,0
MCAFFEE FAMILY PROTECTION	2,2	2,4	0,0	0,0	1,1	1,2
MOBICIP	1,8	1,6	0,0	0,0	0,9	0,8
NET NANNY	3,0	3,0	0,0	0,0	1,5	1,5
NET-INTELLIGENCE	2,2	2,4	0,0	0,0	1,1	1,2
NORTON ONLINE FAMILY	3,4	2,8	1,0	1,0	2,2	1,9
OPENDNS HOME	2,0	2,0	0,0	0,0	1,0	1,0
OPTENET WEBFILTER PC	1,6	2,2	0,0	0,0	0,8	1,1
PROFIL PARENTAL FILTER 2	2,4	2,8	0,0	0,0	1,2	1,4
PURESIGHT OWL	2,8	2,6	1,8	1,6	2,3	2,1
SAFE EYES	2,2	2,4	0,0	0,0	1,1	1,2
TELEKOM KINDERSCHUTZ SOFTWARE	3,4	2,8	1,0	1,0	2,2	1,9
TREND MICRO ONLINE GUARDIAN FOR FAMILIES	3,2	3,4	0,0	0,0	1,6	1,7
WHITENET	2,6	2,2	0,0	0,0	1,3	1,1
WINDOWS LIVE FAMILY SAFETY	3,2	3,4	0,0	0,0	1,6	1,7
XOOLOO	2,8	2,6	0,0	0,0	1,4	1,3

Table 13 - PC Tools EFFECTIVENESS results: score view

## 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...) taking into account two different class of age ( $\leq 12$  years old and  $\geq 13$  years old). An overall score was 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 tool was scored from 0 to 4 according to the number of the tested functionalities covered (see *Methodology key issues* section):

- 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 only provide 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 results on adult contents and bad results on other contents.



PC

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

## 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 nonharmful 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 is, the better the tool is.



PC

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle



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

### 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 in % of overblocked or underblocked content.

Topic	Adult content		Violence and Crime		Racist		Drugs & Self-Damage		Gambling	
	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking
AVG FAMILY SAFETY	23	11	18	71	14	55	17	48	19	29
CYBERPATROL	22	37	4	95	2	96	8	93	4	96
CYBERSIEVE	23	28	40	45	11	80	26	69	36	32
CYBERSITTER	11	26	2	90	2	97	1	98	2	96
DAVIDE	5	35	5	74	1	76	4	64	7	45
ENOLOGIC NET FILTER	14	24	12	86	29	66	8	90	34	30
F-SECURE INTERNET SECURITY 2012	5	19	3	73	3	84	7	69	13	39
K9 WEB PROTECTION	20	9	18	74	13	64	4	61	17	22
KASPERSKY PURE	65	7	39	58	42	67	61	26	78	10
MAC OS X PARENTAL CONTROLS	28	22	19	77	9	82	5	70	10	52
MCAFFEE FAMILY PROTECTION	18	21	16	61	16	60	9	54	23	46
MOBICIP	37	20	27	43	38	63	32	66	31	70
NET NANNY	10	15	10	83	4	82	8	31	10	13
NET-INTELLIGENCE	16	26	9	70	7	65	12	74	16	45
NORTON ONLINE FAMILY	30	5	14	62	20	55	15	40	20	23
OPENDNS HOME	29	25	30	62	21	49	20	67	11	42
OPTENET WEBFILTER PC	6	48	5	77	4	81	2	67	6	52
PROFIL PARENTAL FILTER 2	4	21	9	50	7	75	3	65	11	50
PURESIGHT OWL	25	15	34	35	31	26	32	22	23	28
SAFE EYES	18	21	16	61	16	60	9	54	23	46
TELEKOM KINDERSCHUTZ SOFTWARE	30	8	37	44	43	36	31	29	46	26
TREND MICRO ONLINE GUARDIAN FOR FAMILIES	7	23	9	69	7	68	6	63	11	45
WHITENET	41	19	5	94	8	95	7	97	5	98
WINDOWS LIVE FAMILY SAFETY	9	14	9	85	14	77	9	76	10	90
XOOLOO	20	12	10	70	7	79	13	68	19	37

Table 14 - PC Tools EFFECTIVENESS results for topics: % of over/underblocked content



PC

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

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



PC

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

Language	English		German		Italian		Spanish		French		Polish	
	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking
AVG FAMILY SAFETY	25	24	23	41	21	34	14	40	13	36	8	54
CYBER PATROL	15	75	9	77	1	86	19	88	13	80	3	77
CYBERSIEVE	30	39	73	26	26	42	32	61	10	45	9	63
CYBERSITTER	12	59	4	78	4	74	8	81	6	72	1	78
DAVIDE	6	42	7	56	5	55	2	63	1	55	2	72
ENOLOGIC NET FILTER	15	41	24	53	16	61	27	57	15	48	11	60
F-SECURE INTERNET SECURITY 2012	4	40	3	39	4	57	5	63	4	44	2	58
K9 WEB PROTECTION	27	26	14	40	13	43	6	44	9	38	8	42
KASPERSKY PURE	76	12	59	19	44	31	66	20	45	17	22	19
MAC OS X PARENTAL CONTROLS	15	32	10	60	13	76	10	82	11	71	8	85
MCAFFEE FAMILY PROTECTION	14	31	11	40	14	52	15	47	20	40	12	69
MOBICIP	23	41	36	57	31	56	28	50	35	50	38	59
NET NANNY	6	32	9	34	5	51	7	50	5	41	9	43
NET-INTELLIGENCE	13	29	14	53	12	69	9	68	14	40	7	61
NORTON ONLINE FAMILY	25	18	20	33	21	44	11	41	12	32	15	39
OPENDNS HOME	35	30	10	45	25	52	28	49	30	51	9	50
OPTENET WEBFILTER PC	9	52	5	51	6	66	3	53	4	56	2	73
PROFIL PARENTAL FILTER 2	9	26	5	48	0	76	1	73	2	33	0	75
PURESIGHT OWL	37	20	27	32	30	35	30	27	22	32	14	35
SAFE EYES	14	31	11	40	14	52	15	47	20	40	12	64
TELEKOM KINDERSCHUTZ SOFTWARE	33	16	24	16	36	29	42	22	37	24	41	26
TREND MICRO ONLINE GUARDIAN FOR FAMILIES	9	30	5	45	10	61	4	54	45	44	0	63
WHITENET	33	55	22	56	4	66	40	75	28	60	5	57
WINDOWS LIVE FAMILY SAFETY	13	46	8	44	16	40	12	59	16	49	4	63
XOOLoo	10	29	7	51	38	54	10	66	77	29	16	43

Table 15 - PC Tools EFFECTIVENESS results for languages: % of over/underblocked content

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

### 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 in % of overblocked or underblocked content.

Age	≤12		≥13	
	Overblocking	Underblocking	Overblocking	Underblocking
AVG FAMILY SAFETY	19	34	29	24
CYBER PATROL	10	82	15	78
CYBERSIEVE	26	43	24	65
CYBERSITTER	7	66	9	65
DAVIDE	4	51	4	55
ENOLOGIC NET FILTER	23	44	8	53
F-SECURE INTERNET SECURITY 2012	7	53	4	37
K9 WEB PROTECTION	18	35	17	34
KASPERSKY PURE	51	23	47	20
MAC OS X PARENTAL CONTROLS	17	64	8	49
MCAFFEE FAMILY PROTECTION	25	36	20	31
MOBICIP	43	58	22	50
NET NANNY	12	35	9	40
NET-INTELLIGENCE	13	46	11	46
NORTON ONLINE FAMILY	14	29	13	32
OPENDNS HOME	27	42	24	40
OPTENET WEBFILTER PC	4	72	7	52
PROFIL PARENTAL FILTER 2	5	46	3	45
PURESIGHT OWL	34	25	31	24
SAFE EYES	20	36	20	31
TELEKOM KINDERSCHUTZ SOFTWARE	46	35	40	23
TREND MICRO ONLINE GUARDIAN FOR FAMILIES	8	39	7	38
WHITENET	24	61	23	63
WINDOWS LIVE FAMILY SAFETY	14	51	14	51
XOOLOO	16	64	14	33

Table 16 - PC Tools EFFECTIVENESS results for users' age: % of over/underblocked content



PC

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

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

### 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 in % of overblocked or underblocked content.

Web Type	Web		Web 2.0	
	Overblocking	Underblocking	Overblocking	Underblocking
AVG FAMILY SAFETY	16	28	27	45
CYBER PATROL	10	77	13	90
CYBERSIEVE	32	34	23	66
CYBERSITTER	5	57	5	82
DAVIDE	4	45	5	65
ENOLOGIC NET FILTER	16	46	20	56
F-SECURE INTERNET SECURITY 2012	6	38	2	72
K9 WEB PROTECTION	12	30	29	52
KASPERSKY PURE	61	14	65	23
MAC OS X PARENTAL CONTROLS	10	39	16	69
MCAFEE FAMILY PROTECTION	15	32	47	31
MOBICIP	32	46	34	62
NET NANNY	8	31	11	69
NET-INTELLIGENCE	10	35	19	69
NORTON ONLINE FAMILY	14	30	16	30
OPENDNS HOME	21	41	46	47
OPTENET WEBFILTER PC	3	55	4	73
PROFIL PARENTAL FILTER 2	3	38	5	69
PURESIGHT OWL	21	27	59	23
SAFE EYES	13	36	25	59
TELEKOM KINDERSCHUTZ SOFTWARE	38	16	35	31
TREND MICRO ONLINE GUARDIAN FOR FAMILIES	6	31	5	51
WHITENET	24	53	29	76
WINDOWS LIVE FAMILY SAFETY	12	45	16	53
XOOLOO	15	41	16	45

Table 17 - PC Tools EFFECTIVENESS results for Web types: % of over/underblocked content



PC

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

## PC PARENTAL CONTROL TOOLS: Usability key findings

<p>Thirteen out of 25 tools gain better scores for installation and configuration than for usage. Two products score less than 2 points, thus not reaching the threshold of 50 % of 4 points, twenty-one products range between 2 and 2,99, two products score in the top area and gain 3 points or more.</p>	
<p><b>General findings</b></p>	<p>Some of the tools keep the installation and configuration procedure 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.</p> <p>Only few products provide additional information about filtering in general and about limitations and restrictions of the filtering procedures.</p> <p>About one third of the tools provide a web-based configuration. This is an increasing number over the last four test cycles. 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.</p>
<p><b>Findings on the installation process</b></p>	<p>A high percentage of tools keep the installation process very simple. In some cases the installation process runs on the 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.</p>
<p><b>Findings on the configuration process</b></p>	<p>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 of 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 strength of filtering for all content categories, while others allow to differentiate the strength of filtering between different content categories.</p> <p>Several tools do not explain their filter categories, although some categories are quite unusual with regards to youth protection, i.e. sports or humour.</p>
<p><b>Findings on the usage of the tools</b></p>	<p>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.</p> <p>Testing 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.</p>

Table 18 – Usability key findings



PC

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

# PC PARENTAL CONTROL TOOLS: Usability table

## 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 – 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

Usability Tests	AVG FAMILY SAFETY	CYBERPATROL	CYBERSIEVE	CYBERSITTER	DAVIDE	ENOLOGIC NET FILTER	F-SECURE INTERNET SECURITY 2012	K9 WEB PROTECTION	KASPERSKY PURE	MAC OS X PARENTAL CONTROLS	MCAFFEE FAMILY PROTECTION	MOBICIP	NET NANNY	NET-INTELLIGENCE	NORTON ONLINE FAMILY	OPENDNS HOME	OPTENET WEBFILTER PC	PROFIL PARENTAL FILTER 2	PURESIGHT OWL	SAFE EYES	TELEKOM KINDERSCHUTZ SOFTWARE	TREND MICRO ONLINE GUARDIAN FOR FAMILIES	WHITENET	WINDOWS LIVE FAMILY SAFETY	XOOLOO
<b>I</b>	2,78	1,72	2,59	2,50	2,63	2,62	2,89	2,61	2,53	/	2,56	2,14	2,43	2,32	2,59	2,98	2,52	2,47	3,07	2,70	2,73	2,57	2,75	/	2,78
<b>C</b>	2,99	3,24	2,33	2,54	1,76	2,11	2,63	2,78	2,46	2,66	2,41	2,21	2,32	1,91	3,07	2,95	1,64	2,42	3,12	2,54	2,23	3,00	1,52	2,65	2,80
<b>U</b>	2,66	2,31	2,05	1,97	2,11	2,65	2,18	2,39	2,64	2,52	2,14	2,29	2,44	2,32	3,41	2,17	1,63	2,86	2,93	2,08	2,20	2,87	1,66	2,68	2,06
<b>Overall score</b>	<b>2,85</b>	<b>2,66</b>	<b>2,30</b>	<b>2,36</b>	<b>2,04</b>	<b>2,37</b>	<b>2,54</b>	<b>2,63</b>	<b>2,53</b>	<b>2,61</b>	<b>2,36</b>	<b>2,22</b>	<b>2,38</b>	<b>2,12</b>	<b>3,07</b>	<b>2,72</b>	<b>1,82</b>	<b>2,56</b>	<b>3,05</b>	<b>2,44</b>	<b>2,32</b>	<b>2,88</b>	<b>1,81</b>	<b>2,66</b>	<b>2,57</b>

Table 19 - PC Tools USABILITY results





**MOBILE**

**SIP-Bench II**  
Assessment  
Results and  
Methodology  
4th Cycle

# PARENTAL CONTROL TOOLS FOR MOBILE PHONES

FINDINGS FOR  
FUNCTIONALITY, SECURITY, EFFECTIVENESS, USABILITY

## **Mobile phones and the Internet**

Smart phones are one of the most fashionable device 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



### MOBILE

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

<p><b>There are only few tools able to filter the web-pages content and they have limited functionalities compared to the tools available for PCs.</b></p> <p>One tested mobile phone (iPhone) enables CHILDREN/TEENAGERS to browse the Internet. iPhone is equipped with an embedded parental control tool which is able to restrict the usage of some protocols/applications such as accessing the Internet, YouTube and e-mail. It is also able to carry out some content filtering basing on national ratings. However, an external parental control tool is necessary to filter web-pages browsing according to the content.</p> <p>The other operating system, Android, does not provide an embedded tool. The only way to filter the internet is to use an external tool.</p>	
<b>Web Content Filtering</b>	<p>Except <b>K9</b>, all tools give the parents to personalise the filtering through the choice of filtered topics.</p> <p>None of the tools gives the possibility to manage a white or black list of keywords</p> <p><b>K9</b> allows the user to browse according to its default black/white list of Urls. No customization is possible either according to topic categories or to keywords or black/white URLs lists. The Safe Search is available but it is related to the <b>K9</b> browser (not specifically to Google or Bing or Yahoo!).</p> <p>Except <b>K9</b>, all tools give parents the possibility to manage the tool online (from a PC or their own mobile device). For some tools, Norton for example, it is possible to manage both the mobile tool and the PC tool (provided that user installed both tools on teenager's device).</p>
<b>Applications/Protocols and other issues</b>	<p>Concerning usage restriction and monitoring, the tools offer very limited functionalities, in particular for Skype, MSN or streaming which are very popular among teenagers.</p>

Table 20 – MOBILE PHONES PARENTAL CONTROL TOOLS – Functionality key findings



# MOBILE PHONES PARENTAL CONTROL TOOLS: Functionality tables

**How to read the table for EXTERNAL PARENTAL CONTROL TOOL:** the table shows the tools capability (Yes/No) to satisfy the PARENTS NEEDS (see Table 2 – NEEDS for functionality) as grouped in major area of concern and related specific issues. As far as the URLs White/Black lists and keywords are concerned the table shows a synthetic view of the outputs which included the testing of more detailed issues (such as presence of a default URLs/keywords white list, creation of a user's own URLs/keywords both white and black list, restriction of browsing to a URLs white list): in the table the test was represented as positive (Y) if at least one of the specific functionalities was successfully tested. The detailed test results are available in each tool fiche that provides also info on: PRICE and LANGUAGE.

<b>Y:</b>	Yes
<b><u>Y:</u></b>	Web-based only (Web-based streaming or email)
<b>N:</b>	No
<b>B:</b>	Block
<b>M:</b>	Monitor
<b>cF:</b>	Contact Filter
<b>B/W list:</b>	Black and or white list (possibility to filter content according to keywords black and white list provided by default or created/modified by the PARENT)
<b>F:</b>	<b>Global Functionality Rate.</b> The tool was scored from 0 to 4 according to the number of the tested functionalities covered (see: <i>Methodology key issues</i> section): 0 ≥ 1 Very poor functionality coverage (up to 25% of functionalities) 1 ≥ 2 Poor functionality coverage (between 25% and 50% of functionalities) 2 ≥ 3 Good functionality coverage (between 50% and 75% of functionalities) 3 > 4 Very good functionality coverage (between 75% and 100% of functionalities) 4 Excellent functionality coverage (100% of functionalities covered)
<b>S:</b>	<b>Global Security Rate.</b> The security was scored from 0 to 4 (see: <i>Methodology key issues</i> section): 0 = Weaknesses that make the tool easily non-operative (the tool is unsecured against plain child/teenager hacking attacks) 1 = Critical or severe weaknesses 2 = Critical or severe weaknesses requiring some computer skills 3 = Minor weaknesses 4 = No relevant weakness identified (the tool is almost secured against main child/teenager hacking attacks)



MOBILE

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

# MOBILE PHONES PARENTAL CONTROL TOOLS: Functionality tables



## MOBILE

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

External Parental control tool	Area of need	Compatibility	Filtering customization						Keywords	Time	Personal data	Usage restriction				Usage restriction related to communication				F	S			
	Functionality/Specific issue	OS	Web filtering	Topics	Content filtering			Safe Search	Keywords B/W list	Time Restriction		Web access		Streaming		Skype			MSN			email	Score	Score
					Urls White list	Urls Black list	Social networks					B	M	B	M	B	M	F	B	M	F			
K9 WEB PROTECTION BROWSER	iPhone 3.0 or later	Y	N	N	N	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	0,7	0,0
AVG FAMILY SECURITY	iPhone 3.0 or later	Y	Y	N	Y	Y	Y	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	Y	1,6	0,0
F-SECURE MOBILE SECURITY	Android 2.2 or later	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	N	N	Y	Y	N	N	Y	N	N	N	Y	2,4	0,0
MOBICIP SAFE BROWSER	iPhone 3.0 or later	Y	Y	Y	N	Y	Y	Y	N	Y	N	N	Y	N	Y	N	N	Y	N	N	Y	Y	2,4	0,0
NORTON ONLINE FAMILY MOBILE	Android 2.2 or later	Y	Y	N	Y	N	Y	Y	N	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	1,2	0,0

Table 21 – MOBILE PHONES Tools FUNCTIONALITY – results table and overall functionality and security score

Embedded Parental control tool	Area of need	Usage restriction										Usage restriction related to communication								
	Functionality/Specific issue	Web access		Application running		Application download		Application Purchase		Video streaming		Video playing		Skype			MSN			email
		B	F	B	F	B	F	B	F	B	F	B	F	B	M	Cf	B	M	Cf	B
IPHONE 4 ver. 4.3	Y		Y	Y	Y	Y	Y	Y	Y*	Y**	Y	Y	N	N	N	N	N	N	N	Y

Table 22 – MOBILE PHONES Embedded Tools FUNCTIONALITY – results table

## MOBILE PHONES PARENTAL CONTROL TOOLS: Effectiveness key findings

<p>Very few tools for mobile phones provide the functionality of filtering the Web. All tested solutions also exist for PC. The effectiveness of the mobile solutions is slightly lower than the one assessed for the similar PC products.</p>	
<b>Age classes</b>	The tools have similar results for CHILDREN and TEENAGERS. Indeed, the results of underblocking are almost the same for the two age categories.
<b>Web and Web 2.0</b>	Both tools perform better on web than on web 2.0.
<b>Topics</b>	Concerning underblocking, all tools except <b>AVG FAMILY SECURITY</b> the two tools offer an almost decent underblocking values on adult content (between 15% and 25%). Other categories are badly filtered, with a very high underblocking for both tools.
<b>Languages</b>	The tools are more positively assessed with reference to English content than to other languages.

Table 23 – MOBILE PHONES PARENTAL CONTROL TOOLS – Effectiveness key findings



### MOBILE

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

## MOBILE PHONES PARENTAL CONTROL TOOLS: Effectiveness (score view)

Topic	Adult		Other		Overall Score	
	≤12	≥13	≤12	≥13	≤12	≥13
AVG FAMILY SECURITY MOBILE	2,0	2,0	0,0	0,0	1,0	1,0
F-SECURE CHILD SAFE	2,2	2,4	0,0	0,0	1,	1,2
K9 MOBILE	3,2	3,4	0,0	0,0	1,6	1,7
MOBICIP	1,0	1,0	0,0	0,0	0,5	0,5
NORTON ONLINE FAMILY MOBILE	1,8	1,6	1,4	1,8	1,6	1,7

Table 24 – MOBILE PHONES Tools EFFECTIVENESS results – Score view

### How to read the table

The table shows how effective the tool is in filtering harmful content. The tool was scored both with reference to the “adult” content and to the “other harmful” content (drugs and self-damage, violence and crime, racism...) taking into account two different classes of age (≤12 years old and ≥13 years old). An **overall score** was 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 thorough 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 section):

- 0 Very weak - The tool is less effective than a random tool
- 1 Weak - The tool has 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 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



## MOBILE

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

## MOBILE PHONES 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 both in terms of 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 of the 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 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 is, the better the tool is.



**MOBILE**

**SIP-Bench II**  
Assessment  
Results and  
Methodology  
4th Cycle

# MOBILE PHONES PARENTAL CONTROL TOOLS: Effectiveness (over/underblocking)



## MOBILE

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

Topic	Adult content		Violent and crime		Racist		Drugs and self-damage		Gambling	
	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking
AVG FAMILY SECURITY MOBILE	35	45	43	35	30	82	24	70	64	43
F-SECURE CHILD SAFE	25	14	20	73	15	56	19	53	23	33
K9 MOBILE	30	20	23	80	21	67	13	64	24	30
MOBICIP	13	23	9	74	3	84	9	72	16	43
NORTON ONLINE FAMILY MOBILE	35	20	17	63	21	57	18	41	21	26

Table 25 - MOBILE Tools EFFECTIVENESS results for topics: % of over/underblocked content

Language	English		German		Italian		Spanish		French		Polish	
	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking
AVG FAMILY SECURITY MOBILE	26	28	20	36	22	43	16	42	12	38	10	56
F-SECURE CHILD SAFE	30	29	15	44	18	42	13	50	10	42	11	44
K9 MOBILE	27	28	12	39	15	42	12	47	8	39	12	40
MOBICIP	25	43	40	60	35	60	30	55	35	62	40	61
NORTON ONLINE FAMILY MOBILE	25	24	22	47	21	36	14	47	12	39	16	49

Table 26 - MOBILE Tools EFFECTIVENESS results for languages: % of over/underblocked content

# MOBILE PHONES PARENTAL CONTROL TOOLS: Effectiveness (over/underblocking)



## MOBILE

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle

Web type	Web		Web 2.0	
	Overblocking	Underblocking	Overblocking	Underblocking
AVG FAMILY SECURITY MOBILE	13	30	28	49
F-SECURE CHILD SAFE	7	40	4	76
K9 MOBILE	12	29	28	54
MOBICIP	35	51	39	64
NORTON ONLINE FAMILY MOBILE	16	35	17	36

Table 27 - MOBILE Tools EFFECTIVENESS results for Web types: % of over/underblocked content

Age	≤12	
	Overblocking	Underblocking
AVG FAMILY SECURITY MOBILE	20	30
F-SECURE CHILD SAFE	7	38
K9 MOBILE	17	42
MOBICIP	45	61
NORTON ONLINE FAMILY MOBILE	14	36

Table 28 - MOBILE Tools EFFECTIVENESS results for users' age: % of over/underblocked content

## MOBILE PHONES PARENTAL CONTROL TOOLS: Usability key findings

The scores for the mobile tools range between 2,04 and 2,91.	
<b>General Findings</b>	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 three out of five 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. One tool offers a parallel application with one for the child's and one for the parent's mobile phone.
<b>Findings on the installation process</b>	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.
<b>Findings on the configuration process</b>	The complexity of the configuration process differs: three out of five tools provide a web-based configuration but only one of them provides additional configuration steps directly on the device. Tools with application-based configuration have less opportunities to offer a wide spectrum of functions. The configuration on the device also might challenge parents not familiar with mobile phones. Information about how to proceed after the installation is sometimes missing or badly linked within the smart phone's application.
<b>Findings on usage</b>	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. Only one of the tools addresses the alert message for a blocked web site to children but alert messages are mostly comprehensible to youth and adults. None of the tools allows appropriate reaction to the alert message. Reporting function is comprehensible for all products but one, and the amount of information is adequate.

Table 29 – MOBILE PHONES PARENTAL CONTROL TOOLS – Usability key findings



### MOBILE

SIP-Bench II  
Assessment  
Results and  
Methodology  
4th Cycle



## MOBILE PHONES PARENTAL CONTROL TOOLS: Usability table

	AVG FAMILY SAFETY (MOBILE)	F-SECURE MOBILE SECURITY	K9 WEB PROTECTION BROWSER	MOBICIP SAFE BROWSER	NORTON ONLINE FAMILY MOBILE
<b>I</b>	/	/	/	/	/
<b>C</b>	2,55	2,06	2,44	2,49	2,75
<b>U</b>	2,22	2,09	2,29	2,65	3,11
Overall Score	2,42	2,07	2,38	2,55	2,89

Table 30 - MOBILE PHONES Tools USABILITY result

### 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 - 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**



**MOBILE**

**SIP-Bench II**  
Assessment  
Results and  
Methodology  
4th Cycle



**GAME  
CONSOLE**

**SIP-Bench II**  
Assessment  
Results and  
Methodology  
4th Cycle

# PARENTAL CONTROL TOOLS FOR GAME CONSOLES

## FINDINGS FOR FUNCTIONALITY, SECURITY, EFFECTIVENESS, USABILITY

### **Game consoles and the Internet**

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

**Note:** Game consoles were not tested under the fourth cycle. This is due to the fact that no new filter appeared on the market at that time. Nevertheless, Readers can find here game consoles results from the previous benchmarking cycle (ie from the third cycle).

## GAME CONSOLE PARENTAL CONTROL TOOLS: Functionality key findings

Every tested console has its own embedded parental control tool but none is able to filter Web pages according to the content. The two consoles that enable the users to browse the Web (Wii and PS3) may use an external Web filtering tool (Astaro and Trend Micro Kids Safety) for this functionality.

There are only few tools for consoles providing filtering functionalities and some of them still seem to be in a development phase. The 3 embedded tools are focused on the control of other online activities: chatting with other players, online gaming and content downloading/purchasing (apart from a series of offline activities filtering).

<b>Web browsing</b>	Two out of three of tested consoles provide the users with the possibility to search the Web. XBox does not.
<b>Online communication</b>	All the embedded tools can block the chat, but only XBox provides the PARENT with the possibility to filter contacts.
<b>Access to the Internet</b>	All the consoles enable the PARENTS to switch off the access to the Internet. XBox access to the Internet is bound to a pay-for-subscription and limited.
<b>Content filtering</b>	None of the tools offers content filtering basing on categories or other types of customization such as URL/keywords black/white lists.
<b>Monitoring</b>	None of the tools (embedded or external) is able to monitor the online CHILD/TEENAGER activity.
<b>Language Interface</b>	Trend Micro has a multi-language interface whereas Astaro has an English one. The embedded tools language depends on the consoles that are available in several EU languages.

Table 31 – GAME CONSOLE PARENTAL CONTROL TOOLS – Functionality key findings



# GAME CONSOLE PARENTAL CONTROL TOOLS: Functionality tables

## How to read the table for External Parental control tool.

The table shows the tools capability (Yes/No) to satisfy the PARENTS NEEDS (see Table 2 – NEEDS for functionality) as grouped in major area of concern and related specific issues. As far as the URLs black/white lists and keywords are concerned, the tables show a synthetic view of the outputs which included the testing of more detailed issues (such as presence of a default URLs/keywords white list, creation of a user's own URLs/keywords both white and black list, restriction of browsing to a URLs white list): in the table the test was represented as positive (Y) if at least one of the specific functionalities was successfully tested. The detailed test results are available in each tool fiche that provides also info on PRICE and LANGUAGE.

<b>Y:</b>	Yes
<b>N:</b>	No
<b>N/A:</b>	Not Available
<b>B:</b>	Block
<b>M :</b>	Monitor
<b>Cf :</b>	Contact Filter
<b>B/W list:</b>	Black and or white list (possibility to filter content according to keywords black and white list provided by default or created/modified by the PARENT)

**F:** **Global Functionality Rate.** The tool was scored from 0 to 4 according to the number of the tested functionalities covered (see: Methodology key issues section):

0 ≥ 1	Very poor functionality coverage (up to 25% of functionalities)
1 ≥ 2	Poor functionality coverage (between 25% and 50% of functionalities)
2 ≥ 3	Good functionality coverage (between 50% and 75% of functionalities)
3 > 4	Very good functionality coverage (between 75% and 100% of functionalities)
4	Excellent functionality coverage (100% of functionalities covered)

**S:** **Global Security Rate.** The security was scored from 0 to 4 (see: Methodology key issues section):

0 =	Weaknesses that make the tool easily non-operative (the tool is not protected from child/teenager hacking attacks)
1 =	Critical or severe weaknesses
2 =	Critical or severe weaknesses requiring some computer skill
3 =	Minor weaknesses
4 =	No relevant weakness identified (the tool is almost secured against main child/teenager hacking attacks)

# GAME CONSOLE PARENTAL CONTROL TOOLS: Functionality tables

External parental control tool	Area of need	Web content filtering			Users profiles	Filtering Customization			Provision of personal data	Keywords	Time restrictions	F	S
	Functionality/Specific issue	Filtering of web-pages	Blocking social networks	Safe Search	Management	Topic filtering	Black list	White list		Keywords	Time limit settings	Score	Score
ASTARO (Wii)	Y	N	N	N	N	N	N	N	N	N	N	0,6	4
TREND MICRO KIDS SAFETY (PS3)	Y	N	Y	N	N	N	N	N	N	N	N	1,1	2
N/A (Xbox 360)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Table 32 –GAME CONSOLES Tools FUNCTIONALITY results table and overall functionality and security score

Embedded parental control tool	Area of need	Web Access	Content Purchasing	Online communication		Online Gameplay	
	Functionality/Specific issue	Blocking access to the Internet	Content purchase blocking	B	F	B	F
Wii	Y	Y	Y	Y	N	Y	N
PS3	Y	Y	Y	Y	N	Y	Y
Xbox 360	Y	Y	Y	Y	Y	Y	Y

Table 33 –GAME CONSOLES Embedded Tools FUNCTIONALITY results table

## How to read the table for Embedded Parental control tool:

Y: Yes  
 N: No  
 B: Block  
 M: Monitor  
 Cf: Contact Filter  
 F: Filter  
 N/A: Not Available



**GAME CONSOLE**

**SIP-Bench II**  
 Assessment  
 Results and  
 Methodology  
 4th Cycle

## GAME CONSOLE PARENTAL CONTROL TOOLS: Effectiveness key findings

<p>There are only few tools for consoles providing Web filtering functionalities.          No tool is available for the Xbox as this device cannot be directly connected to the Internet.          A tool for PS3 has been tested: it offers similar but slightly lower results compared to the product for PC produced by the same company.          A tool for Wii was tested but the filtering functionality was not effective. Therefore, all harmful pages were shown to the user.</p>	
<b>Underblocking/Overblocking</b>	We can assume that PS3 TREND MICRO operates on the basis of a URLs blacklist and allows all pages not present in its black list, for that reason the overblocking is very low while the underblocking is high.
<b>Age classes</b>	<p>The tool performs quite similarly with a configuration for the two age classes (<math>\leq 12</math> and <math>\geq 13</math>). Part of the explanation lies in the fact that the tools do not give a real possibility to create personalised profiles according to the age:</p> <ul style="list-style-type: none"> <li>• No level of filtering available.</li> <li>• No possibility of choosing content categories to be filtered or not</li> </ul>
<b>Web and Web 2.0</b>	Web 2.0 filtering performance is lower than traditional Web.
<b>Topics</b>	Concerning topics, TREND MICRO performs better filtering on adult content rather than other categories of content. For PS3, some categories are completely ignored like Crime or Self-damage while other non-adult content categories are badly filtered.
<b>Languages</b>	The tool filters better on English content than other languages.

Table 34 – GAME CONSOLE PARENTAL CONTROL TOOLS – Effectiveness key findings



## GAME CONSOLE PARENTAL CONTROL TOOLS: Effectiveness (score view)

Topic	Adult		Other		Overall Score	
	≤12	≥13	≤12	≥11	≤12	≥13
ASTARO (Wii)	0,0	0,0	0,0	0,0	0,0	0,0
TREND MICRO KIDS SAFETY (PS3)	1,4	1,8	0,6	1,6	1,0	1,7

Table 35 -GAME CONSOLES effectiveness related to topic: results table with a score view

The filtering functionality of ASTARO is ineffective and all harmful pages are shown to the user.

There is no possibility to customize TREND MICRO according the age of the user. Due to the different rating calculus methods per the age classes, scores are different.

### How to read the table.

The table shows how tools are effective in filtering harmful content. The tool was scored both with reference to the “adult” content and to the “other harmful” content (drugs, violence, racism...) taking into account two different classes of age [≤12 years old and ≥13 years old]. An **overall score** was 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 tool was scored from 0 to 4 according to the number of the tested functionalities covered (see Methodology key issues section):

- 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

## GAME CONSOLE PARENTAL CONTROL TOOLS: Effectiveness

---

### 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 contents will be rarely blocked.**

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





# GAME CONSOLE PARENTAL CONTROL TOOLS: Effectiveness

## How to read the tables

Each table shows how effective the tools are in blocking content with reference to the **topic** and the six **languages**.

PARENTS can verify how effective each tool is in relation to the topic they are more interested in. Results in % of content overblocked or underblocked.

Language		ASTARO (Wii)	TREND MICRO KIDS SAFETY (PS3)
English	Overblocking	0	13
	Underblocking	100	47
Italian	Overblocking	0	16
	Underblocking	100	60
German	Overblocking	0	6
	Underblocking	100	56
Spanish	Overblocking	0	5
	Underblocking	100	61
French	Overblocking	0	8
	Underblocking	100	48
Polish	Overblocking	0	14
	Underblocking	100	68

Table 36 - GAME CONSOLES Tools EFFECTIVENESS results for languages: % of over/underblocked content

Topic		ASTARO (Wii)	TREND MICRO KIDS SAFETY (PS3)
Adult content	Overblocking	0	12
	Underblocking	100	32
Violent and crime	Overblocking	0	0
	Underblocking	100	81
Racist	Overblocking	0	0
	Underblocking	100	78
Drugs and self-damage	Overblocking	0	0
	Underblocking	100	69
Gambling	Overblocking	0	22
	Underblocking	100	56

Table 37 - GAME CONSOLES Tools EFFECTIVENESS results for topics: % of over/underblocked content

The filtering functionality of ASTARO is ineffective and all harmful pages are shown to the user.

There is no possibility to customise TREND MICRO according the age of the user. Due to different rating calculus methods per age class, the score differs.

# GAME CONSOLE PARENTAL CONTROL TOOLS: Effectiveness

## How to read the tables

Each table shows how effective the tools are in blocking content with reference to the **age and Web types** (Web/Web 2.0).

With regards to the web types, the tools were tested both on user generated content or Web 2.0 (blogs, social networks, forums) and traditional web content (pages of websites).

PARENTS can verify how effective is each tool in relation to the topic they are more interested in. Results in % of content overblocked or underblocked.

Web type		ASTARO (Wii)	TREND MICRO KIDS SAFETY (PS3)
Web	Overblocking	0	13
	Underblocking	100	49
Web 2.0	Overblocking	0	0
	Underblocking	100	69

Table 38 - GAME CONSOLES Tools EFFECTIVENESS results for Web types: % of over/underblocked content

Age		ASTARO (Wii)	TREND MICRO KIDS SAFETY (PS3)
≤12	Overblocking	0	6
	Underblocking	100	46
≥13	Overblocking	0	7
	Underblocking	100	47

Table 39 - GAME CONSOLES Tools EFFECTIVENESS results for users' age: % of over/underblocked content

The filtering functionality of ASTARO is ineffective and all harmful pages are shown to the user.

There is no possibility to customise TREND MICRO according the age of the user. Due to the different rating calculus methods per age class, the



**GAME  
CONSOLE**

**SIP-Bench II**  
Assessment  
Results and  
Methodology  
4th Cycle

## GAME CONSOLES PARENTAL CONTROL TOOLS: Usability key findings

Compared to parental control tools for PC, those for game consoles seem to be less known by parents. Nonetheless, they can be useful and the configuration of game consoles can be entertaining. Nonetheless, they can be useful and also provide parents with a kind of joy of use.	
<b>Installation</b>	It is a challenge for parents to learn about and to decide on the need to install an additional parental control tool on game consoles. ASTARO for Wii and TREND MICRO for PS3 serve as applications installed nearly automatically with the download. Therefore, there is no installation process to be handled by the user.
<b>Configuration</b>	<p>ASTARO for Wii and TREND MICRO for PS3 provide barely any option for configuration, therefore the configuration of the settings for youth protection on the consoles themselves was included in the test.</p> <p>The process might be unfamiliar for parents and is not well supported. Some parts are difficult to understand.</p>
<b>Usage</b>	<p>As most parental control tools work in the background of the consoles, there is less usage than with other computer software. Nonetheless, it is important that parents can easily handle the alert messages to keep them involved with the products.</p> <p>Both parental control tools do not address the alert message for a blocked web site to children and youth but to adults only. Also no appropriate option for reaction to the alert message is provided. No reporting is offered.*</p>

Table 40 – GAME CONSOLES PARENTAL CONTROL TOOLS: Usability key findings

\*During the 3<sup>rd</sup> test cycle it was not possible to connect with the ASTARO server. As a result the filtering functions were not operating and alert messages occurred. Therefore, the assessment of the alert message is related to the last two testing cycles.



## GAME CONSOLES PARENTAL CONTROL TOOLS: Usability table

	ASTARO (Wii)	TREND MICRO KIDS SAFETY (PS3)
<b>I</b>	/	/
<b>C</b>	1,88	1,76
<b>U</b>	1,72	2,07
<b>Overall Score</b>	<b>1,82</b>	<b>1,88</b>

Table 41 - GAME CONSOLES Tools USABILITY results

### 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 - 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**



**GAME CONSOLE**

**SIP-Bench II**  
Assessment  
Results and  
Methodology  
4th Cycle

# METHODOLOGY: KEY ISSUES

---

## Introduction

The benchmarking study aimed at assessing the tools according to various features: functionality, effectiveness, usability, configurability, transparency, security for the European users. Five benchmarking cycles are foreseen, each cycle every 6 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 adjusted to the needs of the users

The assessment activity was based on a specific methodology. The Report and the methodology described herein refer to the **4<sup>th</sup> Cycle**.

## Users' Needs

The definition of the users' needs was a starting point of the study activity and is key to reading of the Report: It oriented the testing activity providing some criteria for the tools selection and for the dataset creation, the parameters for the tool testing and the key to the presentation of the results.

The analysis of users' needs was carried out starting from a literature of existing studies and reports and complemented by our experience in the field in terms of the Internet and digital threats. The users' needs with regard to usability have been identified in a first place based on previous experiences derived from the work with children's welfare organizations and other experts in the field, esp. at the Youth Protection Roundtable.

It was decided to tailor this analysis to the European PARENTS having CHILDREN or TEENAGERS included in one of the two classes of age: ≤12 years old and ≥13 years old.

The analysis resulted in:

- The identification of 3 main **devices** used to access the Internet: **PC, mobile phones and game consoles**.
- 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 Messaging 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.



## METHODOLOGY: KEY ISSUES

---

- The definition of the **needs in terms of functionality/security/effectiveness/usability** as reported in the tables 2, 3, 4 and 5 of this Report.
- The identification of **three types of activities** that the PARENTS would require the tool 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: (Web, Web 2.0, Instant Messaging, P2P, Streaming, email).



## METHODOLOGY: KEY ISSUES

---

The analysis resulted in:

- The identification of 3 main **devices** used to access the Internet: **PC, mobile phones and game consoles.**
- 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 Messaging 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 2, 3, 4 and 5 of this report.
- The identification of **three types of activities** that the PARENTS would require the tool to be able to perform:
  - **Filtering web-pages** according to content topics.
  - **Blocking the usage** of a protocol/application.
  - **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: (Web, Web 2.0, Instant Messaging, P2P, Streaming, email).



## METHODOLOGY: KEY ISSUES

With reference to the content, the parents are mostly concerned with the following topics, that have been grouped into two categories :

<b>Harmful Adult content</b>	<b>Adult:</b> Adult, sexually explicit content that could impair children's and young adults' sexual development ( <u>main</u> concern).
<b>Other harmful content</b>	<b>Violent and Crime:</b> Violent content that could impair children's and young adults' moral and social development 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.
	<b>Racist and hate material:</b> Racist and hate material that could instigate damage to another or another's freedom and rights.
	<b>Drug and Self damage:</b> 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.
	<b>Crime:</b> Skills/activity that could instigate damage to themselves or to others.
	<b>Gambling:</b> Content that instigates to gambling.

Table 42 – USERS' NEEDS: topics parents are concerned with





# METHODOLOGY: KEY ISSUES

---

## Selection of tools to be tested

There are numerous filtering solutions. 30 tools have been considered in this test. The selection was aimed at covering the parents' needs in terms of devices (PCs, Mobile Phones, Consoles), operating systems (Windows, Mac, Linux), languages, type of solutions (default systems like Microsoft Vista parental control, client software, ISP solutions) and capacity to meet their needs.

## SPECIAL NOTE FOR MOBILE PHONES AND GAME CONSOLES

The tests aimed at covering the main operating systems: iPhone, BlackBerry, Symbian, Windows Mobile, and Android. The attention was focused on one popular smart phone: iPhone. On the supply side, the situation noted during the first cycle test has not changed: the filtering tools available for the selected mobile phones for the European consumers' usage are still few and show some limitations in terms of functionalities when compared to those available for PCs. In particular, there are only few tools able to filter web-pages content and they are sometimes limited to some specific countries. Most of the existing parental control tools are mainly focused on the control and monitoring of these types of activities more than web-filtering. This is mainly due to the fact that until recently they were primarily used to communicate via phone calls, SMS, MMS. The tools selected for the test are:

- AVG FAMILY SECURITY MOBILE for iPhone, iPad, iPod, iOS 3.0 or later
- K9 WEB PROTECTION BROWSER for iPhone, iPad, iPod Touch, iOS 3.0 or later
- MOBICIP SAFE BROWSER for iPhone, iPad, iPod Touch, iOS 3.0 or later
- NORTON SAFETY MINDER, Android 2.2 (or later)
- F-SECURE MOBILE SECURITY, Android 2.2 (or later)

Game consoles were not tested under the fourth cycle. This is due to the fact that no new filter appeared on the market at that time. Nevertheless, Readers can find here game consoles results from the previous benchmarking cycle (ie from the third cycle).

As far as **game consoles** are concerned, three most popular were selected: **PlayStation 3 v. 3.61**, **XBox 360** and **Wii v4.3**. Each console has **its own embedded parental control system** that was tested. Moreover, PlayStation 3 and Wii allow web-browsing and for this reason we have tested 2 external tools able to filter web-content:

- ASTARO parental controls for Wii.
- Trend Micro Kids Safety for PlayStation 3.
- No tool has been tested for XBox360 since the console does not allow directly web-browsing (the online activities are "online communication" via games chat, "online gaming" and accessing the XBox Live platform; the filtering is managed by the embedded parental control tool).



## METHODOLOGY: KEY ISSUES

### Testing activity: functionality test

The functionality test is targeted at testing if the tool really has the functions required to satisfy the parents' needs.

The tools were tested on Windows, except for OpenDNS Basic and Mac OS parental controls tested on MAC and Mobicip tested on Linux (Ubuntu distribution),

The applications/protocols for testing were selected among the most popular and the most fashionable for CHILDREN/TEENAGERS.

In case of Security Suites the functionalities were analyzed with reference to the Parental Control interface and not with reference to the Security/Firewall interface.

### NOTE FOR OTHER INFORMATION INCLUDED IN THE TOOL FICHE

<b>Operating System Compatibility</b>	The results reported the editors declaration.
<b>Language Interface</b>	
<b>Price</b>	

### Methodology for Functionality assessment

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

- [Yes]: the tool has the functionality and it works correctly.
- [No]: the tool does not have the functionality or it does not work correctly.

The parents needs were grouped in the following macro-areas and in each macro-area a series of specific tests were carried out as synthesized in the following tables:

- **Blocking the usage** of a protocol/application (ref. Table 43 – Methodology for functionality test related to blocking)
- **Monitoring** the application/protocol usage and the Web content accessed (ref. Table 44 – Methodology for functionality test related to monitoring)
- **Managing** and customizing the tool with reference to filtering (ref. Table 45 – Methodology for functionality test related to managing and filtering customization)
- **Keeping a communication channel** with the children/teenager (ref. Table 46 – Keeping communication channel with the users)



# METHODOLOGY: KEY ISSUES

## Blocking the usage

The functionality test related to "**Blocking the usage of a protocol/application**" was carried out according to the criteria synthesized below:

Type of action	Protocol/Application	Applications used for test	The test was successful (YES) if:
Accessing the Internet	HTTP (Web)	- Explorer - Mozilla	Both applications were blocked
Listening/Watching	Streaming	- YouTube (Web based streaming)	YouTube was blocked
Instant Messaging	MSN protocol	- Windows Live Messenger MSN	MSN was blocked
	Skype protocol	- Skype	Skype was blocked
File sharing	P2P	- eMule 0.50 - Bit Torrent	The application was blocked
Email	HTTP	- Web based (Gmail; Yahoo; Hotmail)	Web mail was blocked
Social networks	HTTP (Web)	- Explorer - Mozilla	The access to Facebook was blocked
Safe search	HTTP (Web) - Explorer	- Explorer - Mozilla	The filtering sets the Google Safe Search, the Bing Safe Search and Yahoo! Safe Search and the CHILD/TEEN is unable to remove it
Provision of personal data	MSN protocol	- Explorer - Mozilla	An instant message containing the personal data previously defined was blocked

Table 43 – Methodology for functionality test related to blocking



## METHODOLOGY: KEY ISSUES

### Monitoring

**Monitoring** was intended as the possibility for the parents to be reported on the children/teenagers activity on the web.

Monitoring related to the usage of web which implies personal communications contents was carried out in compliance with the end-users privacy rights. I.e. in case of Instant Messaging (Skype and MSN), the monitoring test was aimed at assessing ONLY if the tool reported the parent about the access to the protocol; in case of Social Network the monitoring test was aimed at assessing if the tool reported the parent about the "duration" of the specific social networking activity. In any case, the possibility to acknowledge the content provided and received by the end-user during the communication activities was not in the scope of this study since this possibility might violate the end-users' (children/teenagers) privacy rights.

The functionality test related to "**Monitoring** the application/protocol usage and the Web content accessed" was carried out according to the criteria synthesized below:

Type of action	Protocol/Application	Applications used for test	The test was successful (YES) if:
<b>Accessing the Internet Listening/ Watching</b> <b>Online chatting</b> <b>Instant Messaging</b> <b>File sharing</b> <b>Social networks</b>	The same as detailed above	The same as detailed above	The tools provided the PARENTS with a short or detailed report with an evidence of the CHILD/TEENAGER access to the application. As far as streaming is concerned, the monitoring test refers to the tool reporting about the application usage only (and not to the Web streaming). As far as Social networks are concerned, the monitoring refers to the duration of Facebook usage.

Table 44 - Methodology for functionality test related to monitoring

Type of action	Type of test	The test was successful (YES) if:
<b>Managing different users profiles</b>	It was tested on 2 profiles	Both profiles worked correctly (shifting from one profile to another).
<b>Customizing content filtering</b>	It was tested activating the categories available and testing each of them accordingly: Categories (tested on 3 topics) URLs black/white list (tested on 10 URLs); keywords (tested on 5 keywords or 2 categories of keywords).	The 3 topics were all blocked (5 URLs each); if the 10 URLs were all blocked or allowed (URL block/white list); if all the 5 keywords (or defined grouped or keywords) were blocked or allowed.
<b>Contacting people through IM</b>	IM	The same as detailed above.
<b>Remote management</b>	It was tested on 2 profiles	It was possible to access the configuration and/or monitoring functionalities of the tool from a remote position by web and/or mobile phone

Table 45 - Methodology for functionality test related to managing and filtering communication



## METHODOLOGY: KEY ISSUES

Type of action	Methodology	The test was successful (YES) if:
<b>Blocking Message</b>	It was tested on 2 profiles, trying to access a blacklisted page.	At least one of the two following tests was successful: - It was possible for a child/teenager to ask the parent to unblock a Website. - When a webpage was blocked the user is redirected to a safe resource.

Table 46 – Keeping a communication channel with the users



## METHODOLOGY: KEY ISSUES

---

### Peculiarities for Mobile Phones and Game Consoles

#### Mobile Phones:

The mobile phones tools were also considered separately since even if they are increasingly used to access the Web, they are primarily used to communicate via phone calls, SMS, MMS. For these reasons, the existing parental control tools are mainly focused on the control and monitoring of these types of activities more than on Web filtering.

The test was carried out following the same criteria as for the PC but using a subset of functionalities: some functionalities tested for PCs are useless for mobile phones, therefore they were not included in the testing criteria: the management of different users profiles (as phone is typically a personal device with one user only), the P2P application, since they refer to activities usually not performed through the device.

As far as iPhone is concerned, an ad hoc test was carried out also on the embedded parental control functionalities. As for consoles, the built-in parental restrictions are useful to complement the filtering options offered by the external parental control tool.

#### Game Consoles:

The parental control tools for the game consoles were considered separately from PCs since:

- Their primary use is not Web surfing but game and online game (including chatting). The functionality test was therefore primarily focused on verifying online gaming and chatting filtering options.
- Unlike PCs and mobile phones, game consoles provide the PARENTS with a set of integrated (embedded) parental control functionalities which do not include websites filtering. The embedded tool provides functionalities for filtering online chat, online gaming and content downloading (apart from offline activities filtering).



## METHODOLOGY: KEY ISSUES

Two functionality tests were carried out:

- One specific test in order to test the **embedded parental control tools** of each console. The test was carried out with reference to the functionalities that can manage the user's online activities
- One test in order to assess the **external parental control tools** available for PlayStation 3 and Wii (Trend Micro Kids Safety and Astaro, respectively). XBox does not allow the user to browse the Web, therefore there is no Web-content filtering external tool available (or necessary). A subset of criteria for the external control tool was used:

Type of action tested	Description
Blocking access to Internet	Restrict the child/teen access to the Internet channel
Chat blocking	Prevent child/teen from chatting with other players
Chat Filtering	Set with whom the child/teen can chat
Content purchase blocking	Prevent the child/teen from purchasing (pay-for content)
Budget restriction	Define the budget a user can spend for purchasing content
Online game-play blocking	Prevent the child/teen from playing online (allow only off-line game play)
Online game-play filtering	Filtering game basing on the content topics
Web content filtering	Filtering the content that the chid/teen can access to the Web basing on the topics

Table 47 - Ad-hoc set of criteria for the embedded tool

### Criteria for functionality scoring:

Only external parental control tools were scored for mobile phones and game consoles. One general comprehensive score was attributed to functionality (**Functionality Rate**). The criteria were the following: 1 point was given to each existing and working functionality ["Y" - see each PC, MOBILE and GAME CONSOLES functionality results table]. In case of Streaming and Email the tool was given 1 point for Web based streaming or email and 1 point for the related application. The total score is the sum of the points. The definitive score reported in the column is the total score scaled from 0 to 4. The two decimal figure was rounded up to a one decimal figure.



# METHODOLOGY: KEY ISSUES

## Testing activity: security test

The tools were 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 and Game Consoles

The test was 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.

Description of the score	Sc	Type of actions tested for by passing the tool (PC)	Mobile/Console
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 (ex. 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 usage)	x
Minor issue	3	Starting the computer in Safe Mode	x
	3	Changing the port of Peer-to-Peer application	x
No issues identified	4	No issues	

Table 48 - Set of criteria and scoring for security





## METHODOLOGY: KEY ISSUES

For those features (such as applications/protocols) which imply different aspects to be tested, the methodology is synthesized below:

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 the port of Peer-to-Peer application**	e-Mule and BitTorrent	When the two applications were blocked changing the default port to two different ports
Changing time and date settings (to overcome time limits usage)	From the operating system	

Table 49 - Methodology for Security Testing

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

\*\*This test was performed only if the tool provides the possibility to block P2P applications and if after having set the blockage the applications opened (though unable to work) thus allowing the CHILD/TEEN to access the configuration interface and change the port. Otherwise it would be not available (N/A).

### Criteria for security scoring

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



## METHODOLOGY: KEY ISSUES

---

### 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 was carried on a specific **data set** and followed a precise **methodology**.

### Data used to test the tools

A sample of 6000 pages (containing text, video and images) have been collected as representative 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 content (that should not be blocked by the tool).
- Harmfulness of content has been separately valued both for  $\leq 12$  (notably children) and **and/or for  $\geq 13$  years old** (notably teenagers).



## METHODOLOGY: KEY ISSUES

- Content is related to the following topics: adult content, violence and crime, racism, drugs and self-damage, gambling (see – Users Needs: topics parents are concerned with).
- It includes various types of web-content (Web sites, social networks, blogs, forum, video sharing sites).
- It includes content in the following languages: English, French, Italian, German, Spanish and Polish.
- The web-pages have been classified from the point of view of the PARENT.

The chart below shows the data set figures used for 4<sup>th</sup> Cycle during the **effectiveness test**. The data set for the effectiveness testing does not include e-mail, chat, P2P or VOIP content. With relation to these type of data, the tools were 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 **Ethical Issues** paragraph below. Each Web page has been manually reviewed to assess the harmfulness and the topic related. Data according to web type/  
Data according to content type and appropriateness.

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	1200	1200	600	600
Web 2.0 Web pages where users share the contents produced directly by themselves (user generated content). Examples are: blogs, forums, social networks, wiki, video sharing sites (YouTube like)	800	800	400	400

Table 50 – Data set composition

As it was not possible to automate the tests for mobile phones and consoles, the tests have been carried out on a smaller data test set of 1200 items following the same balance between the various kind of content as for the complete data test set.



## METHODOLOGY: KEY ISSUES

---

### Methodology for effectiveness assessment

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

For each tool an **automatic test** was carried out to see if each page was blocked or not. This test was performed three times:

- With the default configuration of the software.
- Having configured the software for a child ( $\leq 12$  years old).
- Having configured the software for a teenager ( $\geq 13$  years old).

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 **configuration** for children and teenagers was made according to the features offered by each software, like setting a level of filtering or choosing categories to be filtered.

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 performance was measured in terms of both underblocking and overblocking (in the final ranking the two situations will be weighed differently according to the user's age):

- % 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 contents will be rarely blocked.



# METHODOLOGY: KEY ISSUES

## Criteria for effectiveness scoring

The effectiveness score is calculated starting from average of the effectiveness results according to the topics (adults and non adults) for the two age classes.

There is a unique value including overblocking and underblocking which are weighted differently according the age. For children ( $\leq 12$ ) the underblocking is more critical than for teenagers ( $\geq 13$ ). The weights chosen are the following:

	$\leq 12$	$\geq 13$
<b>Underblocking</b>	4	3
<b>Overblocking</b>	1	2

Table 51 - Criteria for effectiveness scoring - overblocking and underblocking weights

This value combining underblocking and overblocking is then scored according to the following scale:

Score	Criteria
<b>4</b>	<b>&lt; 10%</b>
<b>3</b>	<b>&lt; 20%</b>
<b>2</b>	<b>&lt; 30%</b>
<b>1</b>	<b>&lt; 50%</b>
<b>0</b>	<b>&gt; 50%</b>

Table 52 - Criteria for effectiveness scoring - scoring scale

When the value of underblocking is higher than 50%, the score given to overblocking is also 0, irrespective of the actual value. On the contrary, if the filter does not filter at all a topic, the overblocking value is 0% and underblocking value is 100. In this case, the score would not be equal to zero and would a false idea of the effectiveness of the tool. The treshold of 50% is chosen because an underblocking value highrt than 50 % implies that the tool filters worse than a random tool.



# METHODOLOGY: KEY ISSUES

## Testing activity: usability test

The usability tests are aimed at assessing whether a tool is easy to install, configure and also to use. Within the EU-SIP project Youth Protection Roundtable, result achieved from the work with children’s welfare experts and technical specialists was that filtering tools 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 filter tools on their own system, it will lead to bad filtering results.

The usability was assessed by a combination of two different approaches – including both end users tests and experts reviews. Two experts’ reviews were carried out independently, The results were then comprised to one final score for each criterion. Additionally, from the second cycle on, users were asked to try out the products and fill in a short usability questionnaire. The users’ answers were analysed with regards to their judgment of the products. Based on this procedure, the users’ voice is presented in each product’s toolfiche as an additional piece of information for the decision making process of parents and other responsible adults in charge of minors.

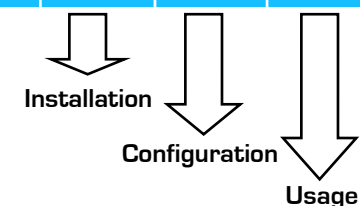
The complete list of criteria comprises of 36 questions. They are related to the process of:

- Installation
- Configuration
- Usage of the software

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.

Suitability for the task: 8 questions	I	C	U
Self descriptiveness: 7 questions	I	C	U
Controllability: 5 questions	I	C	U
Conformity with user expectations: 10 questions	I	C	U
Error tolerance: 3 questions	I	C	U
Suitability for individualization: 4 questions	I	C	U
Suitability for learning: 4 questions	I	C	U

Table 53–Groups of criteria for usability testing



## METHODOLOGY: KEY ISSUES

---

### Criteria for usability scoring

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

For the global score for each product the installation process was given a weight of 20 %, configuration has a weight of 50 % and usage has a weight of 30 %.



# METHODOLOGY: KEY ISSUES

## Global rating issues

The final ranking was calculated on the basis of the overall scores assigned for each of the test (functionality, effectiveness, security and usability) carried out.

In case of effectiveness, the overall score considered was the score representing the performance of each tool with reference to the content topic (“Adult” / “Other”) as shown in Table 13 – PC Tools EFFECTIVENESS results: score view.

Two final rankings were produced according to the two classes of age.

The four components of the final ranking are weighed differently according the age classes. The differences are the following:

- **For children (≤12 years old)** the security has a lower weight than for the teenagers as security issues (by-passing or hacking the software) are less critical.
- **For teenagers (≥13years old)**, the functionality are valued as more relevant than for children. Children will mainly have basic Internet skills.
- For children, effectiveness is more important than for teenagers.

	Weight %	
	≤12	≥13
Effectiveness	64	52
Functionality	8	13
Usability	20	20
Security	8	15

Table 54 – Global rating weights





## METHODOLOGY: KEY ISSUES

---

### Results disclosure

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

The results were 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 authentication procedure or generally related to the user’s personal private communication (social network, chat, Instant Messaging, emailing) was 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, was also excluded from the data set used to test the tool effectiveness.



# GLOSSARY

<b>Anti-virus</b>	The anti-virus software is used to prevent, detect, and remove computer viruses, worms, and Trojan horses.
<b>Application</b>	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.
<b>Blacklist</b>	A list that identifies dangerous keywords, URL or website addresses that are blocked by the tool.
<b>Blog</b>	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.
<b>Browser</b>	A "Web browser" or "Internet browser" is a software application for retrieving, presenting, and traversing information resources on the World Wide Web.
<b>Cache</b>	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.
<b>Configuration</b>	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.
<b>Cookie</b>	Also known as a "Web cookie", "browser cookie", and "HTTP cookie", it is a piece of text stored by a user's Web browser.
<b>Download</b>	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.



## GLOSSARY

<b>E-mail</b>	"Electronic mail", commonly called email or e-mail, is the method of exchanging digital messages across the Internet or other computer networks.
<b>E-Mail Client</b>	An "email client", "email reader", or more formally "mail user agent" (MUA), is a computer program used to manage user's email.
<b>File Sharing</b>	File sharing is the practice of distributing or providing access to digitally stored information, such as computer programs, multi-media (audio, video), documents, or electronic books.
<b>Firewall</b>	A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications.
<b>HTTP</b>	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.
<b>Installation</b>	Installation (or setup) of a program is the act of putting the program onto a computer system so that it can be executed.
<b>Instant Message</b>	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.
<b>ISP (Internet Service Provider)</b>	Also referred to as an "Internet access provider" (IAP), it is a company that offers its customers access to the Internet.
<b>Messenger</b>	MSN Messenger (now named Windows Live Messenger) is an instant messaging client created by Microsoft.
<b>Online chatting</b>	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.



# GLOSSARY

<b>Operating System</b>	An operating system (OS) is a software, consisting of programs and data, that runs on computers and manages the computer hardware and provides common services for efficient execution of various application software. Windows, Mac OS or Linux are operating systems.
<b>Overblocking</b>	It occurs when the tool blocks non-harmful content.
<b>P2P</b>	"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.
<b>Protocols</b>	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 signaling, authentication and error detection and correction capabilities.
<b>Proxy</b>	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.
<b>Skype</b>	It is a software application that allows users to make voice calls and chat over the Internet.
<b>Social network</b>	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.
<b>Temporary Internet Files</b>	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.
<b>Underblocking</b>	It occurs when the tool allows harmful content.
<b>Uninstallation</b>	It is the removal of all or parts of a specific application software.



## GLOSSARY

---

<b>Upload</b>	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.
<b>URL</b>	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 <a href="http://www.example.com/">http://www.example.com/</a> .
<b>Virus</b>	A computer virus is a computer program that can copy itself and infect a computer.
<b>Web-based email</b>	Email service offered through a web site (a webmail provider) such as Hotmail, Yahoo! Mail, Gmail, and AOL Mail.
<b>Whitelist</b>	A list that identifies keywords, URL or website addresses considered safe.



# TOOLS

Parental Control Tools for PC
AVG FAMILY SAFETY
CYBERPATROL
CYBERSIEVE
CYBERSITTER
DAVIDE
ENOLOGIC NET FILTER
F-SECURE INTERNET SECURITY 2012
K9 WEB PROTECTION
KASPERSKY PURE
MAC OS X PARENTAL CONTROLS
MCAFEE FAMILY PROTECTION
MOBICIP
NET NANNY
NET-INTELLIGENCE
NORTON ONLINE FAMILY
OPENDNS HOME
OPTENET WEBFILTER PC
PROFIL PARENTAL FILTER 2
PURESIGHT OWL
SAFE EYES
TREND MICRO ONLINE GUARDIAN FOR
WHITENET
WINDOWS LIVE FAMILY SAFETY
XOOLOO

Parental Control Tools for Mobile Phones
AVG FAMILY SECURITY (MOBILE)
K9 WEB PROTECTION BROWSER
MOBICIP SAFE BROWSER
NORTON ONLINE FAMILY MOBILE
F-SECURE MOBILE SECURITY

Parental Control Tools for Game Consoles
ASTARO (for Wii)
TREND MICRO KIDS SAFETY (for PS3)
PARENTAL FILTER EMBEDDED IN THE XBOX 360 (functionality and usability assessment only)

