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

Assessment results and methodology 1st 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
1st Cycle

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 contents 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.

Main references for feedback about the study:
Silvia Pietropaolo
INNOVA Europe
Avenue des Arts 24
B-1000 Bruxelles
email: s.pietropaolo@innova-europe.eu

TABLE OF CONTENTS

INTRODUCTION

Objectives

This Report is the first 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:

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.

- To provide the end-users (notably PARENTS) with a detailed overview of the existing parental control tools benchmarked on 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 of tools that protect children and young people from the 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 supply.
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 database can be found at the following address:
http://www.yprt.eu/sip

INTRODUCTION

What are the parental control tools?

Besides the clear advantages and opportunities, the Internet carries numerous threats to CHILDREN/TEENAGERS: from the access to inappropriate content (e.g. pornography, violence, self-harm and illicit act incitement) to the exposition to online predators and to dangerous act of which they can be victims or actors (e.g. sexting, cyberbullying, pedophilia). Today, the market provides PARENTS with numerous instruments to protect their CHILDREN/TEENAGERS from such threats. They are better known as parental control tools.

It is possible to identify at least three ways through which using a parental control tool: - client installation on a PC; - subscription to an online filtering service (no need to install on the PC); - a combination of both solutions.

Parental control tools enable PARENTS to **play mainly three types of actions** to protect their CHILDREN/TEENAGERS:

- **Customization of Web content filtering**: let the CHILDREN/TEENAGERS view content according to a set of specific criteria defined during the configuration of the tool. The PARENTS may ask the tool to block or show content indicating the topic, a list of URLs or some specific keywords.
- **Blocking the usage:** block the usage of a protocol /application notwithstanding the inappropriateness of the content (e.g. the tool might prevent the children to watch streaming through Media Player).
- **Monitoring the application/protocol usage and the Web content accessed**: to be reported on **if** and/or **when** and/or for **how long** accessing a specific website, entering/using a specific application/protocol.

The possibility to acknowledge the content provided and received by the CHILDREN/TEENAGERS has not been considered within this study since this possibility violates the end-users privacy rights.

Regardless any possible classifications of parental control tools, it is important to consider first of all the type of **device** the CHILDREN/TEENAGERS use to access the Internet more frequently. Besides the PC, which is still the most common device, today also mobile phones and game consoles are increasingly being used to access the Internet.

In this report the tools are divided by device. For this benchmarking cycle we have selected and tested:

- **26 PC parental control tools.**
- **2 Mobile parental control tools.**
- **3 Console 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, therefore, different according to the parents' specific concerns referable to the following most general categories:

- Viewing/producing **inappropriate content**
- Being the victim/actor 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, **finding the balance among functionalities offered, effectiveness, security and usability performance.**

Test Type	What it consists in	Where results are synthesized
FUNCTIONALITY	It assesses which functionalities the tool successfully provides	Functionality tables
SECURITY	It assesses the tools resistance to the users' attempts to by-pass it by means of specific actions	Functionality tables dedicated column
EFFECTIVENESS	It measures how much each tool blocks harmful content and allows non-harmful content	Effectiveness tables
USABILITY	It assesses if it can be easily installed, configured, udes and mantained by average user	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 here, 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 better match/es your requirements:

Area of Need	Description	Table
COMPATIBILITY	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).	FUNCTIONALITY
DIFFERENT USERS	If the access to the device is open to more than one CHILD/TEENAGER with different filtering needs, you need to create and manage more than one user with specific and different customization features.	
CUSTOMIZATION OF FILTERING	If you have specific needs with respect 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.	
KEYWORDS	If you are particularly concerned with some words that your CHILDREN/TEENAGERS may find on content (webpages and communication messages).	
TIME RESTRICTION	If you are worried about the time your child is spending on the Internet (whether browsing or communicating).	
USAGE RESTRICTIONS	If you are interested in deciding which actions the CHILDREN/TEENAGERS can perform on the Web and when. The main actions you are concerned with are possible thanks 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 wish to totally 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: • Surfing the Web (**WEB ACCESS**). • Watching/listening to video/images/music in streaming (**STREAMING** through **Application** or **Web**). • Sharing contents by uploading or downloading (**FTP/P2P**).	
USAGE RESTRICTIONS RELATED TO COMMUNICATION ACTIVITIES	The **inward/outward communication activity** constitutes one of the PARENTS most feared and increasing concern. The communication/networking tools are an opportunity to make CHILDREN/TEENAGERS share their opinions and find new friends but they are also a danger: the 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 **be themselves the actors of bullying, sexting or performing malicious actions. In this case you could wish to block or monitor** the access to the following applications/protocols that allow: chatting and sending instant messaging or email to specific contacts – e.g. **SKYPE, MSN Messenger (Instant Messaging), IRC (chat protocol), 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	Today, especially TEENAGERS could be able to by-pass or un-install the tool. Depending on your children "hacking skills", you should select the tool also considering its resistance to various type of violations such as: • 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. • By-pass the tool: changing the time settings (if time limit usage restriction is applied). • Disabling the tool: closing it through the Task Manager, disabling/un-installing it without a password, Using a Live CD instead of the default OS, formatting the hard disk.	

Table 3 - NEEDS for Security

Area of Need	Description	
TOPIC of CONTENT	You might have different needs in terms of topics to be filtered and should choose the most effective tools accordingly.	
UNDERBLOCKING/ OVERBLOCKING	Each tool faces two problems: 1) blocking non harmful pages (over-blocking) 2) allowing harmful pages (under-blocking). You may decide to give more importance to over-blocking or under-blocking. For instance for a child you could prefer to	
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 **age: ≤ 10 and ≥ 11 years old.** (more details in the section Methodology key issues)	
LANGUAGE	The interface of the tool needs to be available in a language you are confident with. The tool should also be able to accurately filter the content in the language children and teenagers use most.	
WEB 2.0 and WEB	With the Web 2.0 (blog, forum, YouTube/daily motion, social networking) widening, the risk for CHILDREN/TEENAGERS to come into contact with inappropriate material produced by "unchecked" sources has increased. You should consider the kind of content mostly accessed by your children.	

Table 4 - NEEDS for Effectiveness

Area of Need	Description	Table
INSTALLATION	You might want a short installation process or no installation at all. You should be able to understand and manage the installation process quite well, i.e. choose between installation for beginners or advanced users.	USABILITY
CONFIGURATION	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.	
USAGE	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 own how the tool reacts in case of blocking a website. Not all tools provide a reporting function. Nonetheless reporting should be easy to handle and understand.	

Table 5 - NEEDS for Usability

PARENTAL CONTROL TOOLS: GLOBAL RANKINGS for PC TOOLS

The global ranking was calculated only for the PC tools since the tools for consoles were only 2 and for mobile there was only one tool 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

PC Tools ranking assessed for ≤ 10 years old users						
Rank/26	Tool	Functionality	Effectiveness	Usabiliy	Security	Rating
	Average across 26 tools	**2,1**	**1,2**	**2,60**	**2**	**1,600**
	Best values	**3,5**	**2,1**	**3,32**	**4**	**2,278**
1	Mac OS X	2,6	1,9	2,67	4	**2,278**
2	SafeEyes	3,0	2,1	2,52	1	**2,168**
3	Windows Vista	3,2	1,9	2,86	1	**2,124**
4	Cyber Patrol	2,4	1,7	3,32	2	**2,104**
5	CA Security S.	2,4	1,5	2,56	4	**1,984**
6	Kaspersky ISS	3,0	1,6	3,14	1	**1,972**
7	McAfee IS	1,3	2,0	2,63	0	**1,910**
8	Optenet	2,6	1,8	2,12	1	**1,864**
9	Profil	2,9	1,1	2,80	4	**1,816**
10	PureSight	3,0	1,0	2,75	4	**1,750**
11	CYBERSitter	2,4	1,5	2,47	1	**1,726**
12	Norton ISS	1,3	1,2	2,59	4	**1,710**
13	Net Nanny	2,2	0,9	2,54	4	**1,580**
14	Brightfilter	1,4	1,3	2,85	0	**1,514**
15	TFK	2,7	1,2	2,22	1	**1,508**
16	Intego	3,0	0,8	2,80	2	**1,472**
17	F-Secure	1,3	1,2	2,52	1	**1,456**
18	Alice	0,5	0,8	2,27	4	**1,326**
18	Zone Alarm	0,5	0,8	2,27	4	**1,326**
20	Vise	3,5	0,8	2,21	1	**1,314**
21	TrendMicro	1,4	0,8	2,85	1	**1,274**
22	OpenDNS Basic	1,3	0,8	3,11	0	**1,238**
23	eScan	1,4	0,5	2,40	4	**1,232**
24	CyberSieve	3,4	0,5	2,58	1	**1,188**
25	Norman	1,3	0,6	2,44	0	**0,976**
26	FilterPak	0,6	0,6	2,17	1	**0,946**

Table 6 - PC Tools GLOBAL RANKING for ≤ 10 years old users

PARENTAL CONTROL TOOLS: GLOBAL RANKINGS for PC TOOLS

PC Tools ranking assessed for ≥ 11 years old users						
Rank/26	Tool	Functionality	Effectiveness	Usabiliy	Security	Rating
	Average across 26 tools	2,1	1,6	2,6	2	1,900
	Best values	3,5	2,5	3,32	4	2,668
1	Mac OS X	2,6	2,3	2,67	4	**2,668**
2	Profil	2,9	1,7	2,80	4	**2,421**
3	PureSight	3,0	1,5	2,75	4	**2,320**
4	Norton ISS	1,3	1,9	2,59	4	**2,275**
5	Cyber Patrol	2,4	1,9	3,32	2	**2,264**
6	CA Security S.	2,4	1,5	2,56	4	**2,204**
7	SafeEyes	3,0	2,2	2,52	1	**2,188**
8	Intego	3,0	1,6	2,80	2	**2,082**
9	Windows Vista	3,2	1,8	2,86	1	**2,074**
10	Net Nanny	2,2	1,3	2,54	4	**2,070**
11	Kaspersky ISS	3,0	1,7	3,14	1	**2,052**
12	Optenet	2,6	2,1	2,12	1	**2,004**
13	Cyber-Sitter	2,4	2,0	2,47	1	**1,996**
14	McAfee IS	1,3	2,5	2,63	0	**1,995**
15	Alice	0,5	1,6	2,27	4	**1,951**
15	Zone Alarm	0,5	1,6	2,27	4	**1,951**
17	TFK	2,7	1,9	2,22	1	**1,933**
18	F-Secure	1,3	1,9	2,52	1	**1,811**
19	TrendMicro	1,4	1,6	2,85	1	**1,734**
20	CyberSieve	3,4	1,0	2,58	1	**1,628**
21	OpenDNS Basic	1,3	1,6	3,11	0	**1,623**
22	Brightfilter	1,4	1,6	2,85	0	**1,584**
23	eScan	1,4	0,5	2,40	4	**1,522**
24	Vise	3,5	0,6	2,21	1	**1,359**
25	FilterPak	0,6	1,2	2,17	1	**1,286**
26	Norman	1,3	1,2	2,44	0	**1,281**

Table 7 - PC Tools GLOBAL RANKING for ≥ 11 years old users

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, sharing experiences and contents through social networks, communicating with people.

PC PARENTAL CONTROL TOOLS: Functionality key findings

None of the test tools reaches the complete functionality coverage. The most complete one is rated 3,5 on a 4 scale. The 3 highest scoring products are: Vise (3.5), CyberSieve (3.4) and Windows Vista (3.2).	
Customization of Web content filtering	All the tools (apart from Mac OS X) provide the PARENTS with the possibility to block content according to categories based on topics. Most of the tools (84%) provide the PARENT with the complete set of customization functionalities (topic + URL and black/white lists). In all tools, the presence of a black/white lists works as a way to determine exceptions with respect to the categories that were selected by the users (block/allow mode). The keywords filtering option is uncommon: 12 out of 26 tools provide this option.
Protocols and Applications	The tools rarely provide the option to block an **entire protocol** (e.g. 27% for FTP) whereas blocking **applications** is more common (61% is able to block MSN or P2P applications).
Management of users profiles	Most of the tools enable the PARENTS to create and manage different profiles for users with different needs.
Restricting Web access	84% of the tools enable PARENTS to block the access specifically to the Internet (whether using a specific functionality or using the "time restrictions").
Streaming	The majority of the tools (with the exception of FilterPak) 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 Media Player is possible for less than a half of tools.
Communication activities	61% of the tools are able to block MSN Messenger but less than a half (46%) is able to block Skype. The 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 restrict blocking to Voip or Video chat only. Only 6 tools are able to block the entire IRC protocols explicitly. By the way it resulted that many tools are able to block specific IRC applications.
Monitoring	80% of the tools are able to provide the PARENTS with at least a basic report on the users' web activity (visited websites or violations). Some of these also provide specific alerts with violations and more detailed report. There are few tools able to report on protocols/applications usage. 12 tools are able to monitor MSN whereas no tool is able to provide information on the number and names of downloaded files through P2P applications.
Language Interface	English is the most frequent language whereas for many other European languages the tools' choice is limited.
Security	Some tools present some security weaknesses. The most common are: allow accessing to a prohibited page through translation sites or Google cache. Most parental controls block their blacklisted proxies only: for this aspect the security depends, therefore, on each tool's database richness. None of the tools is able to resist to the OS formatting or to the usage of a live CD.

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 info 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.

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

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 (for criteria see: Methodology key issues 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 "hacking" 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	Users	Filtering customization			Keywords	Time	Usage restriction							Usage restriction related to communication activities										F	S
Functionality	OS	Mgmnt	Content filtering			keywords	Time	Web access		Streaming		P2P		FTP	IRC			Skype			MSN			email		
Specific issue	W/M/L	Mgmt of users	Topics	Urls White	Urls Black list	B/W list	Time limit	B	M	B	M	B	M	B	B	M	Cf	B	M	Cf	B	M	Cf	B	Score	Score
Vise	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	Y	N	Y	3,5	1
CyberSieve	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y	N	Y	Y	N	Y	3,4	1
Windows Vista	W	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y	N	Y	Y	N	Y	3,2	1
PureSight	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y	N	N	N	Y	Y	Y	Y	3,0	4
Intego	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	N	N	Y	Y	N	Y	Y	N	Y	3,0	2
Kaspersky ISS	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y	N	Y	Y	Y	Y	3,0	1
Safe Eyes	W, M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	N	N	Y	Y	N	Y	Y	N	Y	3,0	1
Profil	W	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y	N	Y	Y	Y	Y	2,9	4
TFK	W	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y	N	Y	Y	N	Y	2,7	1
Mac OS X	M	Y	N	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y	N	Y	Y	N	Y	2,6	4
Optenet	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	Y	N	N	Y	N	N	Y	N	N	Y	2,6	1
CA Security S.	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	N	Y	N	N	N	N	N	Y	Y	Y	Y	2,4	4
Cyber Patrol	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	N	N	N	N	Y	N	N	Y	N	N	Y	2,4	2
CYBERsitter	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	N	N	N	N	Y	N	N	Y	N	N	Y	2,4	1
Net Nanny	W	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	N	Y	N	N	N	N	N	N	Y	Y	N	Y	2,2	4
eScan	W	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	1,4	4
Trend Micro	W	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	1,4	1
Brightfilter	W	Y	Y	Y	Y	N	Y	Y	N	Y	N	N	N	N	N	N	N	N	N	N	Y	N	N	Y	1,4	0
Norton ISS	W	Y	Y	Y	Y	N	Y	N	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	1,3	4
F-Secure	W	N	Y	Y	Y	N	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	1,3	1
OpenDNS Basic	W, M, L	Y	Y	Y	Y	N	N	Y	N	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N	Y	1,3	0
McAfee IS	W	Y	Y	Y	Y	N	Y	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	1,3	0
Norman	W	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	1,3	0
FilterPak	W	Y	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	0,6	1
Alice	W	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	0,5	4
Zone Alarm	W	N	Y	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	0,5	4

Table 8 - PC Tools FUNCTIONALITY results table and overall functionality and security score

PC PARENTAL CONTROL TOOLS: Effectiveness key findings

Underblocking/ Overblocking	The underblocking rate is higher to 20 % for all tested tools. The overblocking rate is low for some tools (inferior to 4%) but in these cases, the underblocking rate is very high. Overblocking and underblocking rates are linked: tools which have a low underblocking have also a high overblocking rate. Nevertheless no tool is characterised by a very low underblocking and a high overblocking. It might be hypothesised that tools rely mainly on black lists and keywords URL analysis, having the well-known limits associated with these techniques, in particular the difficulty to analyse user-generated content. Less than 20% of our data test set belongs to existing black lists and our data counts 6000 items. This may explain why effectiveness results may be lower than the ones proposed by other similar tests.
Age classes	The tools perform quite similarly with a configuration for the two age classes (<10 and > 11). Part of the explanation lies in the fact that many tools do not give a real possibility to create personalised profiles according to the age: • No level of filtering available. • Personalisation by content categories that both applies to children and teenagers.
Web and Web 2.0	The tools present a 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.
Topics	The adult content is better filtered than the "other" content categories. A category like self-damage, which contains almost only user-generated content, is very badly filtered by almost tools.
Languages	The tools work better on English languages than the other languages. Even considering only English content no tool reach an effectiveness lower than 20%. For languages other than English there is no outstanding tool.

PC PARENTAL CONTROL TOOLS: Effectiveness Performance

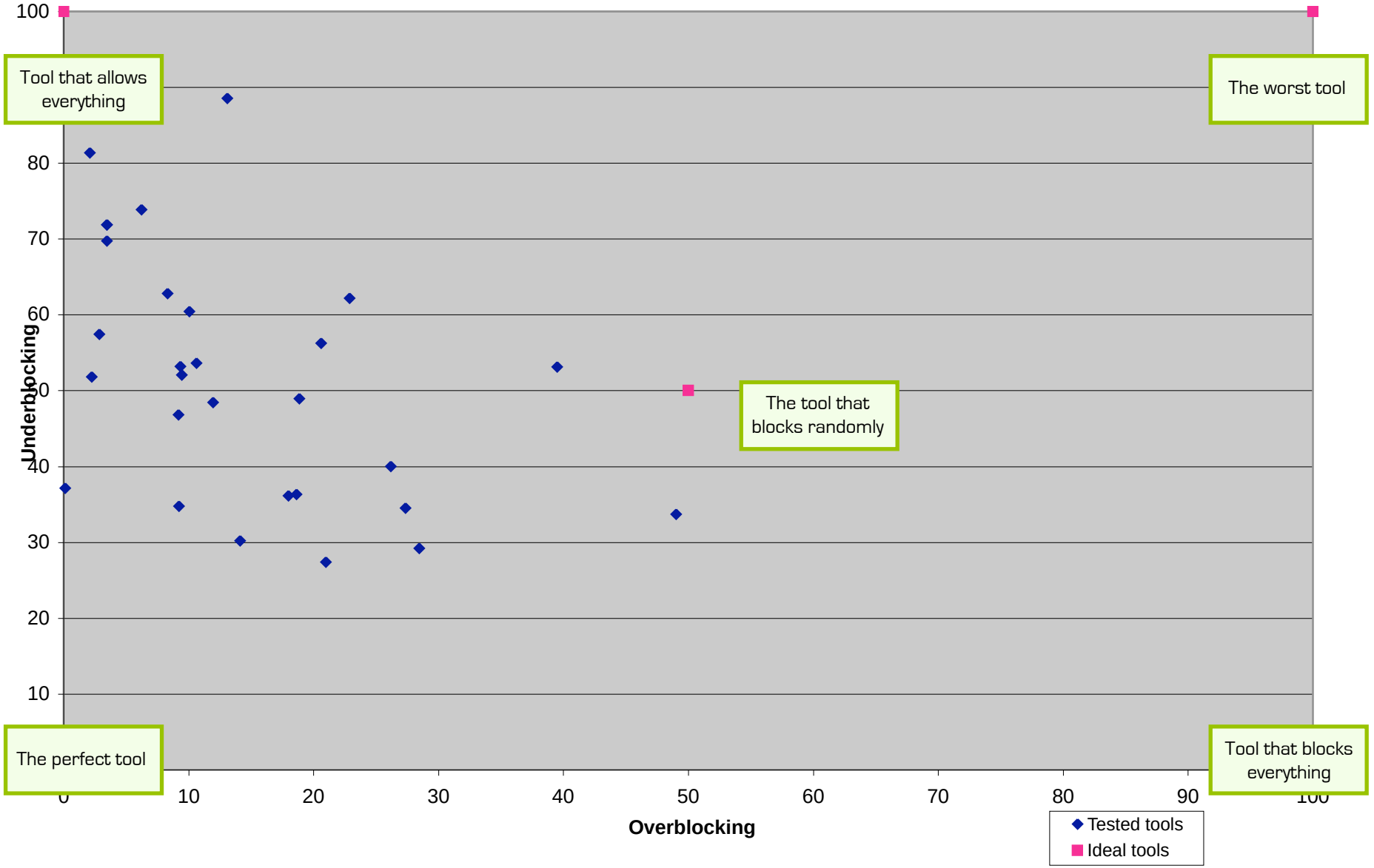


Figure 1 – Effectiveness performance

PC PARENTAL CONTROL TOOLS: Effectiveness (score view)

Effectiveness assessed according to topic and age

Topic	Adult		Other		Overall Score	
	≤10	≥11	≤10	≥11	≤10	≥11
Alice	0,8	1,6	0,8	1,6	**0,8**	**1,6**
Brightfilter	1,4	1,8	1,2	1,4	**1,3**	**1,6**
CA Security S.	1,8	1,6	1,2	1,4	**1,5**	**1,5**
CyberPatrol	3,0	3,0	0,4	0,8	**1,7**	**1,9**
CyberSieve	0,6	1,2	0,4	0,8	**0,5**	**1,0**
CYBERsitter	2,4	2,8	0,6	1,2	**1,5**	**2,0**
eScan	0,8	0,6	0,2	0,4	**0,5**	**0,5**
FilterPak	0,6	1,2	0,6	1,2	**0,6**	**1,2**
F-Secure	1,6	2,2	0,8	1,6	**1,2**	**1,9**
Intego	0,8	1,6	0,8	1,6	**0,8**	**1,6**
Kaspersky ISS	2,8	2,6	0,4	0,8	**1,6**	**1,7**
Mac OS X	3,0	3,0	0,8	1,6	**1,9**	**2,3**
McAfee IS	3,2	3,4	0,8	1,6	**2,0**	**2,5**
Net Nanny	1,4	1,8	0,4	0,8	**0,9**	**1,3**
Norman	0,6	1,2	0,6	1,2	**0,6**	**1,2**
Norton ISS	1,6	2,2	0,8	1,6	**1,2**	**1,9**
OpenDNS Basic	0,8	1,6	0,8	1,6	**0,8**	**1,6**
Optenet	2,2	2,4	1,4	1,8	**1,8**	**2,1**
Profil	1,4	1,8	0,8	1,6	**1,1**	**1,7**
PureSight	1,4	1,8	0,6	1,2	**1,0**	**1,5**
Safe Eyes	2,8	2,6	1,4	1,8	**2,1**	**2,2**
TFK	1,6	2,2	0,8	1,6	**1,2**	**1,9**
Trend Micro	0,8	1,6	0,8	1,6	**0,8**	**1,6**
Vise	0,8	0,6	0,8	0,6	**0,8**	**0,6**
Windows Vista	2,8	2,6	1,0	1,0	**1,9**	**1,8**
Zone Alarm	0,8	1,6	0,8	1,6	**0,8**	**1,6**

Table 9 - **PC Tools EFFECTIVENESS results: score view**

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 class of age (≤10 years old and ≥11 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.

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 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 is the tool.

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

How to read the table
The table shows how tools are effective 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 content overblocked or underblocked.

Topic	Adult content		Violent		Racist		Drugs		Crime		Selfdamage		Gambling	
	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking
Alice	2	76	1	93	6	67	3	56	7	68	14	93	23	46
Brightfilter	16	20	13	48	16	40	17	26	54	45	16	40	38	24
CA Security S.	30	23	11	57	12	47	21	26	45	47	19	49	41	31
CyberPatrol	12	18	14	77	22	67	23	49	23	49	48	57	37	13
CyberSieve	16	54	12	90	32	73	37	52	32	63	19	83	41	19
CYBERsitter	9	29	8	90	11	82	9	85	20	67	12	85	15	63
eScan	56	41	5	71	16	80	50	51	36	85	13	65	90	50
FilterPak	10	89	15	94	15	87	13	86	15	69	14	95	13	84
F-Secure	0	32	0	87	0	92	0	77	2	96	0	97	0	68
Intego	7	57	1	95	1	96	1	78	15	95	2	97	0	95
Kaspersky ISS	28	19	5	73	10	85	29	40	56	55	2	95	52	36
Mac OS X	16	17	11	78	20	85	0	91	0	94	0	96	0	85
McAfee IS	8	20	1	67	0	55	5	32	22	60	0	80	23	23
Net Nanny	18	44	4	87	16	53	41	31	23	59	6	86	55	32
Norman	12	86	14	93	16	87	11	86	14	69	12	96	7	84
Norton ISS	6	33	12	88	17	69	16	88	3	55	4	79	2	61
OpenDNS Basic	2	71	0	88	0	82	1	81	2	64	0	92	12	75
Optenet	19	22	4	62	10	46	9	23	45	50	3	79	27	23
Profil	13	45	2	77	3	53	2	63	2	63	8	89	5	61
PureSight	14	39	5	75	6	57	10	42	19	59	8	81	18	60
Safe Eyes	20	16	14	49	2	50	17	29	18	63	11	58	25	29
TFK	0	45	5	89	0	71	5	58	4	66	2	70	0	71
Trend Micro	7	79	1	84	3	66	2	53	26	59	3	75	19	56
Vise	50	36	51	34	73	34	62	37	100	32	64	35	34	40
Windows Vista	30	14	26	56	48	54	46	24	65	45	42	53	50	63
Zone Alarm	2	76	1	93	6	67	3	56	7	68	14	93	23	46

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

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

How to read the table
The table shows how tools are effective in blocking content in six different **languages**.
PARENTS can verify how effective each tool is for their language/s of interest. Results in % of content overblocked or underblocked.

Language	English		Italian		German		Spanish		French		Polish	
	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking
Alice	6	78	2	86	4	75	3	58	3	76	0	69
Brightfilter	10	22	33	39	8	36	28	31	27	28	24	38
CA Security S.	20	29	25	44	13	35	51	40	39	22	8	43
CyberPatrol	12	30	20	51	10	39	34	54	24	28	2	42
CyberSieve	20	56	16	76	10	69	33	60	25	62	17	60
CYBERsitter	11	48	4	65	8	57	11	64	17	50	5	67
eScan	43	59	27	56	0	40	63	50	46	49	9	44
FilterPak	17	91	13	78	9	91	13	95	10	92	21	73
F-Secure	1	39	0	77	0	58	0	76	0	52	0	59
Intego	6	77	4	76	2	75	3	74	4	59	0	75
Kaspersky ISS	26	33	19	55	14	44	28	48	30	40	9	47
Mac OS X	9	40	7	50	11	68	0	47	8	54	18	49
McAfee IS	6	26	12	49	7	43	6	43	13	30	0	51
Net Nanny	17	49	16	66	7	58	46	44	19	48	7	76
Norman	2	79	1	79	3	67	2	78	2	70	0	82
Norton ISS	0	56	21	52	44	88	0	84	13	51	0	61
OpenDNS Basic	2	79	1	79	3	67	2	78	2	70	0	82
Optenet	13	30	25	53	13	35	19	33	22	25	3	44
Profil	9	46	9	73	4	62	3	76	23	40	0	77
PureSight	10	45	10	65	7	57	25	56	17	52	4	65
Safe Eyes	10	22	17	43	9	33	11	42	27	27	2	41
TFK	1	43	13	63	0	81	0	77	0	62	0	98
Trend Micro	6	81	12	68	3	64	11	61	4	70	0	90
Vise	71	30	55	43	100	20	82	29	88	31	100	48
Windows Vista	24	31	47	32	35	29	56	28	42	24	32	25
Zone Alarm	6	78	2	86	4	75	3	58	3	76	0	69

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

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

Age	≤10		≥11	
	Overblocking	Underblocking	Overblocking	Underblocking
Alice	4	72	3	72
Brightfilter	21	25	21	29
CA Security S.	31	28	26	30
CyberPatrol	18	36	19	37
CyberSieve	22	62	24	62
CYBERsitter	11	65	9	56
eScan	45	46	34	60
FilterPak	12	88	14	90
F-Secure	0	49	0	25
Intego	1	80	6	60
Kaspersky ISS	24	40	29	40
Mac OS X	8	47	10	47
McAfee IS	7	35	12	35
Net Nanny	21	56	21	56
Norman	12	54	9	54
Norton ISS	10	53	8	53
OpenDNS Basic	2	81	2	82
Optenet	18	34	18	38
Profil	7	63	9	63
PureSight	18	39	6	58
Safe Eyes	14	28	14	32
TFK	3	57	3	58
Trend Micro	8	70	4	77
Vise	49	34	49	34
Windows Vista	52	21	3	48
Zone Alarm	4	72	3	72

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

How to read the table

The table shows how tools are effective according to **the age of the children**. Each tool has been configured for each category and tested.

PARENTS can verify how effective is each tool considering the age of their children.

Results in % of content overblocked or underblocked.

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

Web Type	Web		Web 2.0	
	Overblocking	Underblocking	Overblocking	Underblocking
Alice	5	71	6	82
Brightfilter	15	25	28	39
CA Security S.	22	31	37	39
CyberPatrol	18	33	14	51
CyberSieve	23	60	15	69
CYBERsitter	9	50	12	68
eScan	44	51	38	57
FilterPak	16	88	5	92
F-Secure	0	52	0	77
Intego	5	69	4	87
Kaspersky ISS	24	34	24	59
Mac OS X	8	40	9	70
McAfee IS	9	27	2	61
Net Nanny	19	51	21	60
Norman	52	64	32	78
Norton ISS	9	52	5	63
OpenDNS Basic	2	71	1	91
Optenet	15	30	20	49
Profil	10	51	6	73
PureSight	9	48	18	59
Safe Eyes	13	24	13	49
TFK	2	57	1	63
Trend Micro	5	75	11	72
Vise	60	37	45	23
Windows Vista	36	26	34	38
Zone Alarm	4	72	4	85

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

How to read the table

The table shows how effective are the tools 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 is each software considering the kind of content most accessed by their children. Results in % of content overblocked or underblocked.

PC PARENTAL CONTROL TOOLS: Usability key findings

On average the tools gain better scores for configuration than for installation and usage. The only 3 products which are rated over 3 out of 4 are: CyberPatrol (3.32), Kaspersky (3.14) and Open DNS (3.11).	
General findings	Part of the tools keep the installation and configuration procedure very simple to avoid mistakes of the parents but then the 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 misconfiguration and bad filtering results is high. Tools embedded in security suites have in most cases a higher complexity but less functionalities for parental control. Only a few products provide additional information about filtering in general and about limitations and restrictions of the filtering procedures.
Findings on the installation process	A high percentage of tools keep the installation process very simple. In some cases, the user barely acknowledges that he has started and completed the process. On average the tools gain better scores for configuration and installation than for usage.
Findings on the configuration process	It turns out – not surprisingly – that the configuration process is the key to the product. In several cases there are very few configuration options. In other cases configuration is very exhaustive and comprises a lot of functionalities. Most products allow to customise the tool to individual needs, but in some cases this is kind of camouflage only, i.e. setting up profiles according to the individual age of the user while the tool does only filter for a limited number of ages groups, That means you might get the same results for profiles aged 12 and 15 because they are both in the group 10 – 16 years old.
Findings on the usage of the tools	As most parental control tools work 'in the background', there is less usage than with other computer software. Nonetheless it is important that parents can easily handle the alert messages and the reporting to keep them involved with the products. Testing refers mainly to the usability of alert messages. Monitoring and reporting functionalities were tested as usage of the tools, where applicable.

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	Alice*	Brightfilter	CA Security Suite	CyberPatrol	CyberSieve	CyberSitter	eScan	FilterPak	F-Secure	Intego	Kaspersky ISS	Mac OS X	McAfee IS	Net Nanny	Norman	Norton ISS	OpenDNS Basic	Optenet	Profil	PureSight	Safe Eyes	TFK	Trend Micro	Vise	Windows Vista	Zone Alarm
I	/	2,4	2,92	2,4	2,54	2,4	2,4	2,5	3,19	2,8	2,9	/	2,8	2,5	3,3	3,07	2,9	2,2	2,68	2,75	2,3	2,1	2,5	2,3	/	2,6
C	/	3,5	2,78	3,8	2,82	3,01	2,2	2,2	2,36	2,5	3,3	2,6	2,7	2,6	2,6	2,73	3,4	2,3	2,59	2,94	2,62	2,5	3	2,1	3,2	2,4
U	/	2,1	1,96	3,2	2,22	1,6	2,7	1,9	2,33	3,2	3,2	2,8	2,5	2,4	1,6	2,05	2,8	1,7	3,23	2,45	2,5	1,9	2,8	2,4	2,4	1,9
Overall score	/	**2,9**	**2,6**	**3,3**	**2,6**	**2,5**	**2,4**	**2,2**	**2,5**	**2,8**	**3,1**	**2,7**	**2,6**	**2,5**	**2,4**	**2,6**	**3,1**	**2,1**	**2,8**	**2,8**	**2,5**	**2,2**	**3**	**2**	**3**	**2,3**

Table 14- PC Tools USABILITY results

PARENTAL CONTROL TOOLS FOR MOBILE PHONES

FINDINGS FOR FUNCTIONALITY, SECURITY, EFFECTIVENESS, USABILITY

Mobile phones and the Internet
Smart phones are one of the most fashion 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

There are only few tools able to filter the web-pages content and they are sometimes limited to some specific countries (the tool Ruby Star for Symbian OS is limited to United Kingdom and Irish users in Europe).

Both the two tested mobile phones/OS (iPhone 3GS and Nokia E75 - Symbian 3.1) enable CHILDREN/TEENAGERS to browse the Internet. iPhone is provided with an embedded parental control tool which is able to restrict the usage of some protocols/applications such as accessing to the Internet, YouTube, e-mail. It is also able to carry out some content filtering basing on national ratings. But an external parental control tool is necessary to filter web-pages browsing according to the content.

Web Content Filtering	The tool tested for Symbian OS is not able to filter Web content. It is able to filter email only. Its filtering activity is focused on more traditional phone related activities such as SMS, MMS and phone calls. Safe Eyes mobile tool available for iPhone is only able to filter Web content: • Its filtering activity is customizable in terms of categories with the exception of the categories that are blocked by default and that cannot be allowed. • A further possibility is to use black/white URL lists created by the PARENTS directly. • There is no possibility to create a keywords black list with reference to Web content filtering. The presence of a black/white list works as a tool to determine exceptions with respect to the categories that were selected by the users (block/allow mode). • Peculiarity: it filters only what is accessed through the Safe Eyes browser and not what is accessed through the Safari browser provided by default with the device (iPhone). For this reason the PARENTS must necessarily block the access to Safari using the iPhone built-in restriction functionalities, see dedicated section below.
Applications/Protocols and other issues	None of the tools is able to enable PARENTS to control applications/protocols with the exception of the email that can be managed by SecurityShield. The iPhone built-in parental control tool is able to block access to the Web protocol and to YouTube. It is also able to block streaming and application download, purchase and running also selectively basing on national ratings.
Webmail	Safe Eyes is able to block web-based email by adding it to the black list, but generally users access email using the specific application provided by the device which is blocked by the iPhone embedded parental control tool.

MOBILE PHONES PARENTAL CONTROL TOOLS: Functionality tables

How to read the table for EXTERNAL PARENTAL CONTROL TOOL: the table shows the tools capability (**Y**es/**N**o) 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.

Y: Yes
Y: Web-based only (Web-based streaming or email)
N: No
B: Block
M: Monitor
cF: Contact Filter
B/W list: 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 unsecured against plain child/ teenager hacking attacks)
- 1 = Critical or severe weaknesses
- 2 = Critical or severe weaknesses requiring some "hacking" skill
- 3 = Minor weaknesses
- 4 = No relevant weakness identified (the tool is almost secured against main child/teenager hacking attacks)

How to read the table for EMBEDDED PARENTAL CONTROL TOOL:

Y Yes
Y* Yes for YouTube only
Y** Yes for Podcasted music, video. Filtering is based on contents classified as EXPLICIT
N No
B Block
M Monitor
Cf Contact Filter

MOBILE PHONES PARENTAL CONTROL TOOLS: Functionality tables

External Parental control tool

Area of need	Compatibility	Filtering customization				Keywords	Time	Usage restriction				Usage restriction related to communication							F	S
Functionality/Specific issue	OS	Content filtering				Keywords	Time	Web access		Streaming		Skype			MSN			email	Score	Score
		Web filtering	Topics	Urls White list	Urls Black list	B/W list	Restriction	B	M	B	M	B	M	F	B	M	F	B		
SafeEyes Mobile (iPhone 3GS)	iPhone 3.0 or later	Y	Y	Y	Y	N	N	N	N	Y	N	N	N	N	N	N	N	Y	1,4	0
Security Shield 8.8.13 (Symbian 3.1)	BlackBerry, Symbian, Windows Mobile, or Android	N	N	N	N	Y(email)	N	N	N	N	N	N	N	N	N	N	N	Y	0,2	0

Table 15 – 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	B	F	B	F	B	F	B	F	B	F	B	M	Cf	B	M	Cf	B
iPhone 3GS	Y	Y	Y	Y	Y	Y	Y	Y*	Y**	Y	Y	N	N	N	N	N	N	Y
Nokia E75 - Symbian 3.1	N	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	N/A	N/A	N/A	N/A	N/A

Table 16– MOBILE PHONES Embedded Tools FUNCTIONALITY results table

MOBILE PHONES PARENTAL CONTROL TOOLS: Effectiveness key findings

Very few tools for mobile phones provide the functionality of filtering the Web. The solution tested for mobile (Safe Eyes Mobile 1.60) also exists for PC, but the effectiveness of the mobile solution is lower than the one assessed for computer (Safe Eyes PC).	
Age classes	The tool performs better for teenagers rather than for children.
Web and Web 2.0	Web and Web 2.0 filtering performance is similar for underblocking whereas for the overblocking the rate is higher with Web 2.0 content. Compared to the PC version, the results of underblocking are nearly the same whereas the results of overblocking are higher for mobile phones version.
Topics	The adult content is filtered better than the other content categories. The adult content is quite well filtered, in particular when compared to the PC tools average. Some other categories like Gambling or Crime are not filtered at all.
Languages	The tool is assessed better with reference to English content than with other languages.

MOBILE PHONES PARENTAL CONTROL TOOLS: Effectiveness (score view)

Topic	Adult		Other		Overall Score	
	≤10	≥11	≤10	≥11	≤10	≥11
	2,2	2,4	0,8	1,6	**1,5**	**2,0**

Table 17 – MOBILE PHONES Tools EFFECTIVENESS results: score view

How to read the table
The table shows how the tool is 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 (≤10 years old and ≥11 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 throughout 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

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

Underblocking and overblocking

The tool's effectiveness was assessed in terms of its 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 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 is the tool.

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

Topic		SafeEyes Mobile (iPhone 3GS)
Adult content	Overblocking	13
	Underblocking	26
Violent	Overblocking	0
	Underblocking	78
Racist	Overblocking	13
	Underblocking	74
Drugs	Overblocking	0
	Underblocking	95
Crime	Overblocking	33
	Underblocking	100
Selfdamage	Overblocking	0
	Underblocking	85
Gambling	Overblocking	0
	Underblocking	100

Table 18 – MOBILE Tools EFFECTIVENESS results for topics: % of over/underblocked content

Language		SafeEyes Mobile (iPhone 3GS)
English	Overblocking	16
	Underblocking	45
Italian	Overblocking	10
	Underblocking	54
German	Overblocking	0
	Underblocking	57
Spanish	Overblocking	9
	Underblocking	76
French	Overblocking	7
	Underblocking	57
Polish	Overblocking	0
	Underblocking	48

Table 19 – MOBILE Tools EFFECTIVENESS results for languages: % of over/underblocked content

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

Web type		SafeEyes Mobile (iPhone 3GS)
web	Overblocking	3
	Underblocking	68
web 2.0	Overblocking	35
	Underblocking	63

Table 20 – MOBILE Tools EFFECTIVENESS results for Web types: % of over/underblocked content

Age		SafeEyes Mobile (iPhone 3GS)
≤10	Overblocking	9
	Underblocking	53
≥11	Overblocking	9
	Underblocking	51

Table 21 – MOBILE Tools EFFECTIVENESS results for users' age: % of over/underblocked content

MOBILE PHONES PARENTAL CONTROL TOOLS: Usability key findings

There are only a few tools available that provide content filtering on mobile phones.	
Findings on the installation process	Both tools tested come as an application that is installed nearly automatically with the download. Therefore, there is no installation process to be handled by the user.
Findings on the configuration process	Safe Eyes mobile has a few options to configure the filtering on the mobile phone interface. There are more options for configuration when the process is done via a PC interface and then transferred to the mobile phone. The user can also use a combined configuration to control the usage on a PC interrelated with the usage of a mobile phone, i.e.. setting a shared time limit for both devices.
Findings on usage	There are only a few options for usage when Safe Eyes mobile is used on the mobile phone only. Extended options for reporting etc. can be used via the PC interface.

MOBILE PHONES PARENTAL CONTROL TOOLS: Usability table

	Safe Eyes Mobile (iPhone 3GS)	Security Shield 8.8.13 (Symbian 3.1)
I	/	/
C	2,32	2,04
U	1,87	/
Overall score	**2,15**	**2,04**

Table 22 – MOBILE PHONES 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

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.

GAME CONSOLE PARENTAL CONTROL TOOLS: Functionality key findings

All the tested consoles have their 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 a few tools for consoles providing filtering functionalities and for some of them they still seem 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 offline activities filtering).	
Web browsing	Two out of three of the tested consoles provide the users with the possibility to search the Web. XBox does not.
Online communication	All the embedded tools can block the chat, but only XBox provides the PARENT with the possibility to filter contacts.
Access to the Internet	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.
Content filtering	Both the external tools do not offer content filtering basing on categories or other types of customization such as URL/keywords black/white lists.
Monitoring	None of the tools (embedded or external) is able to monitor the online CHILD/TEENAGER activity.
Language Interface	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.

GAME CONSOLE PARENTAL CONTROL TOOLS: Functionality tables

How to read the table for External Parental control tool.

The table shows the tools capability (**Y**es/**N**o) 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.

Y: Yes
N: No
N/A: Not Available
B: Block
M : Monitor
Cf : Contact Filter
B/W list: 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 unsecured against plain child/teenager hacking attacks)
1 = Critical or severe weaknesses
2 = Critical or severe weaknesses requiring some "hacking" 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' profile	Filtering Customization			Keywords	Time restrictions	F	S
Functionality /Specific issue	Filtering of web-pages	Management	Topic filtering	Black list	White list	Keywords	Time limit settings	Score	Score
Astaro (Wii)	Y	N	N	N	N	N	N	0,6	4
Trend Micro Kids Safety (PS3)	Y	N	N	N	N	N	N	0,6	2
N/A (Xbox 360)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Table 23–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	Chat		Gameplay	
			B	F	B	F
Wii	Y	Y	Y	N	Y	N
PS3	Y	Y	Y	N	Y	Y
Xbox 360	Y	Y	Y	Y	Y	Y

Table 24 –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 PARENTAL CONTROL TOOLS: Effectiveness key findings

There are only a few tools for consoles providing Web filtering functionalities: their performance is lower than the tool for PCs.	
Underblocking/Overblocking	We can assume that PS3 Trend Micro operates on the basis of a URLs black list and allows all pages not present in its black list, for that reason the overblocking is very low and for the same reason the underblocking is high. The two tools tested offer quite similar results except for overblocking. The WII has a higher overblocking rate.
Age classes	The tools perform quite similarly with a configuration for the two age classes (<10 and > 11). A 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: • No level of filtering available • Personalisation by content categories that both apply to children and teenagers.
Web and Web 2.0	Web 2.0 filtering performance is lower than traditional Web.
Topics	Concerning topics, both tools perform a 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.
Languages	The tools filter better English content than other languages.

GAME CONSOLE PARENTAL CONTROL TOOLS: Effectiveness (score view)

Topic	Adult		Other		Overall Score	
	≤10	≥11	≤10	≥11	≤10	≥11
Astaro (Wii)	1,2	1,4	0,6	1,2	**0,9**	**1,3**
Trend Micro Kids Safety (PS3)	2,4	2,8	0,8	1,6	**1,6**	**2,2**

Table 25 –GAME CONSOLES effectiveness related to topic: results table with a score view

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 class of age (≤10 years old and ≥11 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 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 is the tool.

GAME CONSOLE PARENTAL CONTROL TOOLS: Effectiveness

How to read the tables
Each table shows how tools are effective 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	English		Italian		German		Spanish		French		Polish	
	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking
Astaro (Wii)	17	32	25	68	6	50	11	67	15	73	6	60
Trend Micro Kids Safety (PS3)	0	39	0	70	0	62	5	74	0	51	0	50

Table 26 – GAME CONSOLES Tools EFFECTIVENESS results for languages: % of over/underblocked content

Topic	Adult content		Violent		Racist		Drugs		Crime		Selfdamage		Gambling	
	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking
Astaro (Wii)	22	40	7	61	7	58	17	34	11	85	12	83	19	51
Trend Micro Kids Safety (PS3)	0	29	0	80	0	73	0	59	0	100	0	100	25	53

Table 27 – GAME CONSOLES Tools EFFECTIVENESS results for topics: % of over/underblocked content

GAME CONSOLE PARENTAL CONTROL TOOLS: Effectiveness

Age	≤10		≥11	
	Overblocking	Underblocking	Overblocking	Underblocking
Astaro (Wii)	16	49	22	49
Trend Micro Kids Safety (PS3)	1	52	3	52

Table 28 – GAME CONSOLES Tools EFFECTIVENESS results for Web types: % of over/underblocked content

Web type	Web		Web 2.0	
	Overblocking	Underblocking	Overblocking	Underblocking
Astaro (Wii)	18	44	11	63
Trend Micro Kids Safety (PS3)	2	43	0	74

Table 29 – GAME CONSOLES Tools EFFECTIVENESS results for users' age: % of over/underblocked content

How to read the tables

Each table shows how effective are tools 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.

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 also provide parents with a kind of joy of use.	
Installation	It is a challenge for parents to learn about and to decide on the need to install an additional parental control tool. For XBox there is no additional parental control tool (for URL filtering) available, XBox has reduced access to the Internet and is therefore not completely comparable to the other two devices.
Configuration	Configuration is less complex than for PC tools.
Usage	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 and the reporting to keep them involved with the products.

GAME CONSOLES PARENTAL CONTROL TOOLS: Usability table

	Astaro (Wii)	Trend Micro Kids Safety (PS3)	XBox 360 Embedded tool
I	/	/	/
C	2,49	2,38	2,96
U	1,83	1,47	2,32
Overall Score	**2,24**	**2,04**	**2,72**

Table 30 – 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

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 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 are referred to the **1st Cycle.**

Users' Needs

The definition of the users' needs was the starting point of the study activity and also the key to the 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 on 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: ≤10 years old and ≥11 years old.**

METHODOLOGY: KEY ISSUES

The analysis resulted in:

- The identification of the 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 chat software, e-mail or Instant Massaging including video chat, VoIP and chat section included 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, IRC protocols, P2P, FTP, Streaming, email).

METHODOLOGY: KEY ISSUES

- The **topics** they are mostly concerned with:

Harmful Adult content	**Adult**: Adult, sexually explicit content that could impair children's and young adults' sexual development (main concern)
Other harmful content	**Violent**: 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)
	Racist and hate material: Racist and hate material that could instigate damage to another or another's freedom and rights
	Drug: Illegal drug taking and the promotion of illegal drug use
	Crime: Skills/activity that could instigate damage to themselves or to others.
	Self damage: Content that could instigate children and teenagers to damage themselves such as material that promotes suicide, anorexia, self-mutilation.
	Gambling: Content that instigate to gamble.

Table 31 – Users Needs: topics parents are concerned with

METHODOLOGY: KEY ISSUES

Selection of tools to be tested

There are numerous filtering solutions. 31 tools have been considered in this test. The selection has been elaborated trying to cover at the best to the parents' reality 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 answer 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 2 popular smart phones: iPhone 3GS and Nokia E71 with Symbian 3.1 OS. It was noticed that 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 if 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 (the tool Ruby Star for Symbian OS is limited to United Kingdom and Irish users in Europe). 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:

- **Safe Eyes 1.60** for iPhone 3GS V4.0 (**iPhone 3GS** console has its **own embedded parental control system** that was tested also).
- **Security Shield 8.8.13** for Symbian 3.1 OS (but also BlackBerry, Symbian, Windows Mobile, and Android) tested on Nokia E71.

As far as **game consoles** are concerned, the three most popular were selected: **PlayStation 3- 549 v. 3.50, 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 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.

With the exception of OpenDNS Basic, Intego and Mac OS parental controls, the tools were tested on Windows.

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.

For those features (such as applications/protocols) testing which implies different aspects to be tested, the methodology is synthesized below in the following pages.

Blocking

Type of action	Protocol/Application	Applications used for test	The test was successful (YES) if:
Accessing the Internet	HTTP (Web)	- Explorer - Mozilla	Both the applications were blocked
Listening/Watching	Streaming	- YouTube (Web based streaming) - Media Player (application)	YouTube was blocked Media Player was blocked
Online chatting	IRC	- mIRC 7.14 (Windows) - PIRCH (Windows) - Colloquy (Mac) - XChat (Mac)	Both the 2 applications were blocked (the test assessed the tool capability to block explicitly the **IRC protocol** and not a set of applications)
Instant Messaging	MSN protocol	- Windows Live Messenger MSN	MSN was blocked
	Skype protocol	- Skype	Skype was blocked
File sharing	P2P	- eMule 5.0	The application was blocked
File uploading/downloading	FTP	- FileZilla 3.3.4.1	The application was blocked (the test assessed the tool capability to block explicitly the **FTP protocol** and not a set of applications)
email	HTTP	- Web based (Gmail; Yahoo; Hotmail)	Web mail was blocked
email	POP3	- Client (Outlook express; Mozilla Thunderbird; Outlook; Mac Mail)	At least one of the clients was blocked

Table 32- Methodology for functionality test related to blocking

METHODOLOGY: KEY ISSUES

Monitoring* and contacting

Monitoring was intended as the possibility for the user to be reported on if and/or when and/or how long entering/using the application/ protocol. The possibility to acknowledge the content provided and received by the end-user during the application/protocol usage was not in the scope of this study since this possibility might violate the end-users (children/teenagers) privacy rights.

Type of action	Protocol/Application	Applications used for test	The test was successful (YES) if:
Accessing the Internet Listening/ Watching Online chatting Instant Messaging File sharing	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** concerned, the monitoring test refers as to the tool reporting about the application usage only (and not to the Web streaming)
Contacting people through IM, Chat	IRC; IM	The same as detailed above	The 5 contacts used for test were all blocked

Table 33 - Methodology for functionality test related to monitoring

Managing

Type of action	Type of Test	The test was successful (YES) if:
Managing different users profiles	It was tested on 2 profiles	Both the two profiles worked correctly (shifting from one profile to another)
Customizing content filtering	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 the10 URLs were all blocked or allowed (URL block/white list); if all the 5 keywords (or defined grouped or keywords) were blocked or allowed
Compatibility	The results reported the editors declaration	

Table 34- Methodology for functionality test related to managing

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.

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 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 (being the phone a typically personal device with one user only), the FTP and 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 to verify online gaming and chatting filtering options.
- Differently from PCs and mobile phones, the game consoles provide the PARENTS with a set of integrated (embedded) parental control functionalities that does not include websites filtering. The embedded tool provides with 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 player**
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 35 - 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

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 basing on a subset of criteria as indicated in the dedicated column of 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	Score	Type of actions tested for by-passing the tool (PC)	Mobile/Console subset
Issues that make the tool easily non-operative	0	Using an alternative browser	x
	0	Disabling or uninstalling the software without a password	x
Critical or severe issues	1	Closing the filtering tool trough the Task Manager	
	1	Accessing the Web pages through the Google cache	x
	1	Reaching a website through translation sites (ex. Google translate)	x
Issues requiring some "hacking" skill	2	Using the IP address instead of the URL	x
	2	Using a proxy instead of a direct connection to the Internet	x
Minor issue	3	Changing time and date settings (to overcome time limits usage)	x
No issues identified	4	No issues	
-	No score	Using a Live CD instead of the default Operating system	
-	No score	Formatting the hard disk	

Table 36 - 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	
Changing time and date settings (to overcome time limits usage)		

Table 37 - Methodology for security testing

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 "hacking skill" required (the higher the level the higher is the score)

No score has been associated with the two tests "Using a Live CD instead of the default Operating System" and "Formatting the hard disk". Indeed this test involves by-passing the whole operating system and as a consequence also the software which is installed on the operating systems. We included these tests that no tool is able to pass, as they represent a possible way to circumvent the filtering tools.

Testing activity: effectiveness test

The effectiveness test aims at assessing if a tool is able to block or not a specific harmful page and if at the same time it is able to allow non-harmful pages. The test was carried on a specific **data set** and following 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 **≤ 10** (notably children) and **and/or for ≥ 11 years old** (notably teenagers).

- Content is related to the following topics: adult content, violence, racism, drugs, criminal, self-damage, gambling (see Table 31 – 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 acting like parents.

The chart below shows the data set figures used for this 1st Cycle during the **effectiveness test**. The data set for the effectiveness testing does not include e-mail, chat, FTP, 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			
	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 38 – 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 targeted to measure how much 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 run 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 (≤ 10 years old).
- Having configured the software for a teenager (≥11 years old).

The reason for testing the effectiveness with the 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. Indeed for children (<10) the underblocking is more critical than for teenagers (>11). The weights chosen are the following:

	≤10	≥11
Underblocking	4	3
Overblocking	1	2

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

Score	Criteria
4	**< 10%**
3	**< 20%**
2	**< 30%**
1	**<50%**
0	**>50%**

METHODOLOGY: KEY ISSUES

Testing activity: usability test

The usability tests are aimed at assessing if a tool is easy to install configure and also to use. Within the EU-SIP project Youth Protection Roundtable one result achieved from the work with children's welfare experts and technical specialists was that filter 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 that will lead to bad filtering results.

The usability was assessed by a combination of two different approaches – comprising end users tests and experts reviews. In the first test cycle the results are based on experts' reviews only. Two experts' reviews were carried out independently, the results were then comprised to one final score for each criterion.

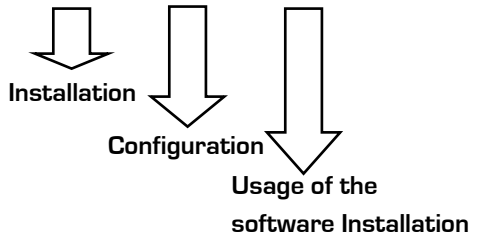
The complete list of criteria comprises 36 questions. These apply to the processes of:

- 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 39–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 tests (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 9 - 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 (≤10 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 (≥11years old)** the functionality are valued as more relevant than for children. Indeed children will mainly have a basic use of the Internet.
- For children, effectiveness is more important than for teenager.

	Weight %	
	≤10	≥11
Effectiveness	64	52
Functionality	8	13
Usability	20	20
Security	8	15

METHODOLOGY: KEY ISSUES

Results disclosure

The results were published in this report and in the webpage also in the format of a queryable database.
The results were mainly provided through tables and graphics. The common scale adopted is a 0 to 4 one. 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

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

GLOSSARY

Download	Downloading is the process of transferring (software, data, character sets, etc.) from a distant to a nearby computer, from a larger to a smaller computer, or from a computer to a peripheral device.
E-mail	"Electronic mail", commonly called email or e-mail, is the method of exchanging digital messages across the Internet or other computer networks.
E-Mail Client	An "email client", "email reader", or more formally "mail user agent" (MUA), is a computer program used to manage a user's email.
File Sharing	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.
Firewall	A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications.
Formatting Hard Disk	It is the initial part of the process for preparing a hard disk or other storage medium for its first use.
FTP	"File Transfer Protocol" is a standard network protocol used to copy a file from one host to another over a Transmission Control Protocol (TCP) / Internet Protocol IP-based network, such as the Internet.
HTTP	The "Hypertext Transfer Protocol" is a networking protocol for distributed, collaborative, hypermedia information systems: it is the foundation of data communication for the World Wide Web.

GLOSSARY

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

GLOSSARY

P2P	"Peer-to-peer" (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes.
Protocols	A "communications protocol" is a formal description of digital message formats and the rules for exchanging those messages in or between computing systems and in telecommunications. Protocols may include signaling, authentication and error detection and correction capabilities.
Proxy	A proxy server is a server (a computer system or an application program) that acts as an intermediary for requests from clients seeking resources from other servers.
Skype	It is a software application that allows users to make voice calls over the Internet.
Temporary Internet Files	Temporary Internet Files is a directory on Microsoft Windows computer systems used by Internet Explorer and other Web browsers to cache pages and other multimedia content, such as video and audio files, from websites visited by the user. This allows such websites to load more quickly the next time they are visited.
Underblocking	It occurs when the tool allows harmful content.
Un-installation	It is the removal of all or parts of a specific application software.
Upload	Uploading is the sending of data from a local system to a remote system with the intent that the remote system should store a copy of the data being transferred.

GLOSSARY

URL	A "Uniform Resource Locator" specifies where an identified resource is available and the mechanism for retrieving it. The best-known example of the use of URLs is for the addresses of Web pages on the World Wide Web, such as http://www.example.com/.
Virus	A computer virus is a computer program that can copy itself and infect a computer.
Web-based email	Email service offered through a web site (a webmail provider) such as Hotmail, Yahoo! Mail, Gmail, and AOL Mail.
Skype	It is a software application that allows users to make voice calls over the Internet.
Whitelist	A list that identifies keywords, URL or website addresses considered safe.

TOOLS LIST

Parental control Tools for PC
Alice (ISP)
Brightfilter Parental Control 2009
CA Internet Security Suite 2010
Cyber Patrol
CyberSieve
Cyber-Sitter
eScan
FilterPak
F-Secure
Internet Security Barrier X6
Kaspersky Internet Security 2011
Mac OS X Parental Controls
McAfee Internet Security 2010
Net Nanny
Norman Security Suite
Norton Internet Security
OpenDNS Basic
Optenet Webfilter
Profil Parental Filter
PureSight PC
Safe Eyes
TIME for kids Internetfilter Plus
Trend micro Internet Security 2011
Vise Parental control
Windows Vista parental control
Zone Alarm Security Suite 2010

Parental Cotrol Tools for Mobile Phones
Safe Eyes Mobile
Security Shield

Parental Control tools for Game Consoles
Astaro (for Wii)
TrendMicroKids Safety (for PS3)
Parental filter embedded with XBox 360 (functionality and usability assessment only)