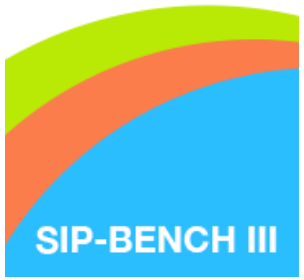


Benchmarking of parental control tools for the online protection of children

Assessment results and methodology: 1st cycle

SAFER INTERNET PROGRAMME

Empowering and Protecting Children Online

SIP Bench is a periodically carried out test of parental control tools. You can find the most up to date test results of parental control tools at **http://sipbench.eu/results**

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

Prepared for: European Commission Directorate General for Communications Networks, Content and Technology

Prepared by: Cybion Srl and Stiftung Digitale Chancen, coordinated by Innova SpA
(hereafter named as “the Consortium”)

NOTICE

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

The opinions expressed in this study are those of the authors and do not necessarily reflect the views of the European Commission.
Although the authors exercised all reasonable efforts to ensure the accuracy and the quality of the content of this publication, the Consortium assumes no liability for any inadvertent error or omission that may appear in this publication.

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

Main references for feedback about the study:

Natalia Mielech
Innova SpA
Via Giacomo Peroni, 386
00131 Rome - Italy

TABLE OF CONTENTS

INTRODUCTION

Objectives

This Report is the first out of 4 reports that will be published on an eight-month basis containing the results of the Study *Benchmarking of parental control tools for the online protection of children SIP-Bench III* 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 according to needs.
- To support the end-users (notably PARENTS) to choose the most appropriate parental control tool that best matches their needs.
- To raise awareness about tools that help protecting children and young people from Internet threats.

The Report aims at guiding the end-users (notably PARENTS) in a clear way through the assorted panorama of parental control tools available on the market.
The results of the study will be also available online in a downloadable version and through a searchable database that allows producing ranking lists adjusted to the PARENTS' specific needs.

What are the parental control tools?

It is important to empower children and young people to use online media safely and responsibly. In addition, there are software and other instruments, that can be used to help protect children. Apart from the clear advantages and opportunities, the Internet carries also threats to CHILDREN/TEENAGERS: from access to inappropriate content (e.g. pornography, violence, self-harm and illicit act incitement) to exposition to online predators and to dangerous behaviors of which they can be victims or authors (e.g., sexting, cyberbullying, pedophilia). Today the market provides PARENTS with numerous instruments to support protection of their CHILDREN/TEENAGERS from such threats. They are known as parental control tools.
It is possible to use a parental control tool in three different ways:

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

Once the tool is operative, PARENTS can:

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

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

The first thing PARENTS should consider is the device used by the CHILDREN/TEENAGERS to access the Internet. Apart from PC, which is still the most common device, mobile phones and game consoles are increasingly used by youngsters to access the Internet.
In this Report the tools are differentiated by device. For this benchmarking cycle we have selected and tested:

- **13 PC/MAC parental control tools.**
- **9 Mobile parental control tools.**
- **3 parental control tools for consoles.**

In addition several alternative tools were assessed, but so far not tested, as the appropriate methodology to test these tools needs to be further developed.

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

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

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

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

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

Typology of NEEDS

In order to have a more detailed overview of the specific testing criteria, users should also read:
- Tools specific and **detailed fiches** (more detailed information is available, especially for functionalities and security).
- The **Methodology** key issues section.

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

NEEDS for functionality

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

NEEDS for Security

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

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, also you might have different sensibility regarding different types of content. You might want to transfer filter configuration between different users or devices. The overall process should be comprehensible, conform with your expectations and be easy to learn.	
USAGE	The alert message in case of blocking should be understandable for children as well as for their parents. You might want to have an option to choose between different reactions in case the tool blocks a website. You might want the tool to support you in your education and help your children understand why the parental control tool is in operation. Not every tool offers a reporting function. Nonetheless, reporting should be easy to handle and understand.	

NEEDS for Usability

RECOMMENDATIONS FOR PARENTS

PC Tools
General

- Filtering tools help you to protect your children. However, it is better to treat them only as a partial solution. The filtering process is still not effective enough. Therefore, in addition to using the tool, you should remember about the importance of direct communication with your children. Discuss with them their activities on the Internet, find out what they like or dislike, organise some Internet-related activities with them and stay up-to-date about the latest trends and threats.
- Parents should keep in mind that filter can be operated at several complementary levels: the operating system (Windows or Mac OS provide some filtering functionalities), the Internet service provider, a software or an app installed on the device, the browser, some websites themselves (eg. Google or Bing offer Safe Search features).
- Some tools are capable of monitoring users' activities in a very detailed way which could violate child's privacy rights. Also, when activating the filtering tool, discuss with your children what kind of filter you want to set up and why.
- When a page is blocked, some filtering tools give children the option to ask parents to unblock the page. If you want to keep the communication open with your children and to increase the tool's effectiveness (as some non-harmful pages are often blocked by error), you should enable this tool option and remember to regularly check and react to your children's requests. Not responding to the requests may be very frustrating for your children.
- Most of the tools provide some customizations features and also the possibility to create several accounts. Be sure that you create one account for each of your children configured according to their needs and age.
- After you have set up the tool or accessed the administration panel of the tool, make sure you log out of the configuration panel or configuration page so that your children cannot access it. Some tools require that the computer be restarted after a configuration (first time or subsequent modifications). To make sure that the tool is working properly, perform a search on Google with a keyword such as "porn" (Not in the presence of your child!). When you try to open the first of the available search results those pages should be blocked.
- Parents should remember to regularly update the tool settings so that they correspond to children age and IT skills.
- Parents should be aware that there are more and more devices to access the web. Apart from PCs, mobile phones and game consoles, there are also tablets. Parents should bear in mind that using a mobile device to access the Internet puts children in a situation where they are usually more often alone than accompanied by an adult who can support them.
- In some cases, it is not the tool itself but the service provider (e.g. browser provider, social network, video website, etc.) that lacks proper content classification. Therefore, parents should remember that parental control tool is complementary to other actions in ensuring their children's safety in the web.

Password protection and security issues

- Make sure that access to the tool configuration is password protected.
- Some tools make use of Windows accounts to manage user profiles and/or require the Windows' admin password to prevent disabling and uninstalling. It is not always evident that this feature is used, so you should check this. In case of doubt, you can create a separate Windows account for your child/teenager and protect your own admin account with a password or software which manages the different profiles linked with the

Windows profile. In this case, you should create a password-protected profile for each teenager/child who can access the Internet. Admin access should be possible only for an adult and be password protected. Be aware that many tools can be bypassed or uninstalled quite easily by children and teenagers. Therefore, check periodically if the filtering tool is still installed and working.

Content filtering

- Be aware that filtering usually does not work well on content related to violence, racism, drugs, self-harm or anorexia. The best options for dealing with such content are education and communication.
- With regards to social networks, check what the tool offers. Does it block access to social networks? Does it filter the content available in social networks? Are there any reporting options that list what the children/teenagers do on social networks?
- If your children/teenagers mostly use the Internet for communicating with others, check the software that they use (e.g. MSN, Skype or Peer-to-Peer software). Then, decide whether you want to filter their communication, for example, filter or block certain actions or limit time spent using the software. In these cases, be aware that there are very few tools that can block/filter communication activities and that their features will differ.

Consoles

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

Mobile phones

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

RECOMMENDATIONS FOR SOFTWARE COMPANIES

General

- Tools should contain a message that provides parents with an explanation of both the capabilities of the tool and its limitations. The message should also motivate parents to engage in Internet activities with their children/teenagers and discuss with them Internet threats.

Usability

- Installation and configuration procedures should be kept simple and explained in plain language.
- The software should:
    - be easy to learn,
    - follow consistent concepts,
    - conform with user expectations about how it works,
    - have an appealing design,
    - provide a good overview on all the features.
- Blocking should be transparent to users.
- Dialogue with the user should be easy to understand and when directed at children should use child sensitive language.
- It is important to inform the users that the tool has some limits, what these limits are and what parents can do with this. This information would give parents a clear picture of what the settings mean in practice and where they should be more careful.

Effectiveness

- Most of the tools are usually not very effective in filtering harmful web content. In any case, adult content is not the only threat to children. Such tools should be more effective with regards to content about violence, racism, self-harm, and, also on user generated content (social networks, blogs, forums, etc.).
- Although not distributed anymore, the AOL filtering tool was satisfactorily effective. Thus, it may serve as a best practice example for other software producers.
- The database containing the black list should be updated at least with every update of the tool.
- Databases should be updated regularly. Weekly update could be a solution reflecting rapid changes in the web.
- Most of the filters filter “old web”, while children and teenagers use web 2.0 (social networks, video-sharing websites). The tools have a low effectiveness on this kind of content. This issue should be better addressed.

Functionality

- Once the installation process is completed, default filtering should be in operation even when the user did not perform or finish a configuration.
- If the creation of user profiles within the filtering tool is linked with the Windows user profile system, parents should be clearly warned (with an alert in a pop-up window or similar) about the need to set up a separate Windows profile and make the admin account password protected. Even better, if there is only one Windows profile, the parent should be guided through the creation of the other profiles.
- Tools should clearly indicate what kind of filtering is performed on the social networks. Is the access to Facebook or similar websites blocked? Is the content filtered? Are interactions with other users filtered or blocked?
- It should be possible, by default or as an option, to make the child/teenager search the web using the safe mode of the three main search engines (Google Safe Search, Bing Safe Search or Yahoo! Safe Search).
- When a page is blocked, the child/teenager should be able to ask the parent to override the blocking when they feel that the blocked content is not harmful.
- Blocking applications: to keep it simple, parents should be provided with a list of applications installed on the computer, for example, in the Windows control panel, instead of having to locate the .exe file on the hard disk.
- Blocking personal data (name, address, phone number) being provided by the child/teenager should be implemented in all tools such as MSN and Skype and also work on websites (blogs, Facebook, webmail).
- Very often blocking categories are based on blocking content in the workplace (i.e. “sports”, “finance”, etc.). Tool providers should consider youth needs when creating the databases for black lists and white lists and provide explanations on what these refer to (to make it more transparent for the parents).
- The reporting of the online activities of the child/teenager and the blocked content should be simple, concise, and provide the relevant information. Sometimes, information provided appears to be designed for business use and not for home or private users.
- Communication between children and parents is the most important issue in youth protection, therefore, the child should always be aware of the monitoring of his/her online activities.
- Tools should be more easy to configure and customize so that they reflect the development of the child.
- Copy of the monitoring report should be automatically sent to the child (at least as an option to be activated). The wording of such reports should be clear and comprehensible.

Security

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

Mobile phones

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

Consoles

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

PARENTAL CONTROL TOOLS FOR PERSONAL COMPUTERS
FINDINGS FOR FUNCTIONALITY, SECURITY, EFFECTIVENESS, USABILITY

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

PC PARENTAL CONTROL TOOLS: Functionality key findings

None of the 13 tested tools reaches the complete functionality coverage. The most complete one covers 77 %. Nine tools are rated under 50 %. The 3 highest scoring products are: PURESIGHT OWL (77 %), NET NANNY (63 %) and TREND MICRO ONLINE GUARDIAN (53 %) .

Customization of Web content filtering
Most of the tools provide the parent with the complete set of customization functionalities (topic and URL black/white lists).
Keywords filtering option is uncommon: only 4 tools offer this option. 11 tools give the possibility to block access to social networks and 10 tools give the possibility to force the user to use the Safe Search functionality of the most common search engines.

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

Management of users profiles Most of the tools enable the parent to create and manage different profiles for users with different needs. One tool can be used only with one profile. Remote Management is possible with 3 tools.

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

Streaming The majority of the tools are able to block Web based streaming provided by YouTube, if not with a specific option, at least by adding it to a black list. Blocking the specific application which allows streaming such as Windows Media Player is possible for 3 tools.

Communication activities 4 tools are able to block Windows Life Messenger and 2 are able to block Skype. If tools are able to block Skype and/or MSN, they block it with respect to the whole application and it is not possible to limit the blocking to Voip or Video chat only.

Monitoring Most of the tools are able to provide the parent with at least basic report on the users’ web activity (visited websites or violations).
4 tools allow remote access to monitoring.

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

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

Area of need	Usage Restriction															
Functionality	Email	P2P		Personal data Provision	Safe search	Skype		Social Networks		Streaming		Web		Windows Life Messenger		
Specific Issue	Block email client and/or webmail access	Block the application	Monitor Downloads	Block	Availability	Block chat	Block video chat	Block Access	Monitor Usage	Block Access	Monitor Access	Block Access	Monitor Access	Block chat	Block video chat	Monitor
F-Secure Internet Security	N	N	N	N	Y	N	N	Y	N	N	N	Y	Y	N	N	N
JusProg	N	N	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N
K9 Web Protection	N	N	N	N	Y	N	N	Y	Y	N	Y	Y	Y	N	N	N
Mac OS X Parental Controls	N	N	N	N	N	Y	N	N	N	N	N	Y	Y	Y	N	N
McAfee All Access	N	Y	N	N	Y	N	N	Y	N	Y	N	Y	Y	Y	N	N
Net Nanny	Y	Y	N	N	Y	N	N	Y	Y	N	N	Y	Y	Y	N	Y
Netintelligence	N	Y	N	N	Y	N	N	Y	N	N	N	Y	Y	N	N	N
Norton Online Family	Y	N	N	Y	Y	N	N	Y	Y	N	N	Y	Y	N	N	N
Optenet PC	Y	Y	N	Y	Y	N	N	Y	N	N	N	Y	Y	N	N	N
Panda	Y	N	N	N	N	N	N	Y	N	N	N	Y	Y	N	N	N
PureSight Owl	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N
Trend Micro Online Guardian	Y	Y	N	Y	N	N	N	Y	Y	Y	Y	Y	Y	N	N	Y
Windows Family Safety	Y	N	N	Y	Y	N	N	Y	N	N	N	Y	Y	N	N	N

% of tools with function	54 %	46 %	8 %	31 %	77 %	15 %	8 %	85 %	38 %	23 %	15 %	100 %	92 %	31 %	8 %	15 %

PC Tools FUNCTIONALITY results and security score

Area of need	Management			Filtering Customisation					Keywords			Time	Blocking Message			Security
Functionality	Management of User profiles	Monitoring	Remote Management	Topics	URLs Black List	URLs White List			Keywords			Time Limit Settings	Type			Score
Specific Issue	Create several profiles	Remote access to monitoring	Manage on various devices	Customisation of Filtering Topics	r i s	Default White List	Modification OR Creation	i n g	U s e r	U s e r	Default Black List	, a m e	o c k i n	Redirect to safe resources	% function coverage	
F-Secure Internet Security	Y	N	N	Y	Y	N	Y	Y1	N	N	N	Y	N	N	33 %	1
JusProg	Y	N	N	N	Y	Y	Y	Y	N	N	N	N	N	Y	27 %	4
K9 Web Protection	N	N	N	Y	Y	N	Y	N	N	N	N	Y	N	N	33 %	3
Mac OS X Parental Controls	Y	N	N	N	Y	Y	Y	Y	N	N	N	Y	N	N	33 %	2
McAfee All Access	Y	N	N	Y	Y	N	Y	N	N	N	N	Y	N	N	40 %	0
Net Nanny	Y	Y	Y	Y	Y	N	Y	Y	Y	N	N	Y	Y	N	63 %	4
Netintelligence	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	N	N	47 %	0
Norton Online Family	Y	Y	Y	Y	Y	N	Y	N	N	N	N	Y	Y	N	50 %	1
Optenet PC	Y	N	N	Y	Y	N	Y	N	Y	Y	N	Y	N	N	47 %	1

Panda	Y	N	N	Y	Y	N	Y	N	N	N	N	N	N	N	27 %	0
PureSight Owl	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	Y	N	N	77 %	4
Trend Micro Online Guardian	Y	N	N	Y	Y	N	Y	N	Y	N	N	Y	N	N	53 %	0
Windows Family Safety	Y	N	N	N	Y	N	Y	Y	N	N	N	Y	N	N	37 %	1
% of tools with function	92 %	31 %	23 %	77 %	100 %	31 %	100 %	54 %	31 %	8 %	8 %	85 %	15 %	8 %		

PC Tools FUNCTIONALITY results and security score

PC PARENTAL CONTROL TOOLS: Effectiveness key findings

	In general, tools have low effectiveness.
Underblocking/Overblocking	The underblocking rate is higher than 30 % for all tested tools.The overblocking rate is low for some tools but in these cases, the underblocking rate is very high. Overblocking and underblocking rates are linked: tools with a low underblocking rate have a high overblocking rate It might be hypothesised that the tools rely mainly on black lists and keywords URL analysis, having the well-known limits associated with these techniques, in particular the difficulty to analyse user-generated content. Less than 20% of the data test set used belongs to the existing black lists and the data test set consists of 4000 items. This may explain why effectiveness results may be lower than the ones proposed by other similar tests.
Age classes	The tools perform quite similarly with a configuration for the two age classes (**≤**12 and **≥** 13). Part of the explanation lies in the fact that many tools do not give a real possibility to create personalised profiles according to the age: • No level of filtering available. • Personalisation by content categories that both applies to children and teenagers. In most of the cases, the tools perform better for the **≥** 13 age class, as it the scoring gives less importance to underblocking for teenagers that for children.
Web and Web 2.0	The tools present lower effectiveness on Web 2.0 content. In particular, the tools which achieve better results than the others have generally higher discrepancy between the underblocking rate on Web and Web 2.0. It is an indicator of the difficulties of tools to deal with user-generated and Web 2.0 content. The web 2.0 is more difficult to filter for several reasons: the content is produced mainly by users and not by identified subjects like companies or institutions; on the website you can find content published by different users, both harmful and not harmful; the content is changing very quickly: a web page that is not harmful could become harmful because of uploaded image; the content may vary according to the user: for instance, each Facebook user's home page is different. Concerning the qualitative tests on web 2.0, all the tools fail.
Topics	The adult content is better filtered than the "other" content categories. On adult content some tools achieve an underblocking lower than 10% which is almost good. On the "other" content categories (except of gambling) only a few tools have an underblocking close to 30%. Most of them have very low effectiveness (more than 70% of underblocking).
Languages	Tools work better on English languages than other languages. Even considering only English content, all the tools have an underblocking rate higher than 20%.

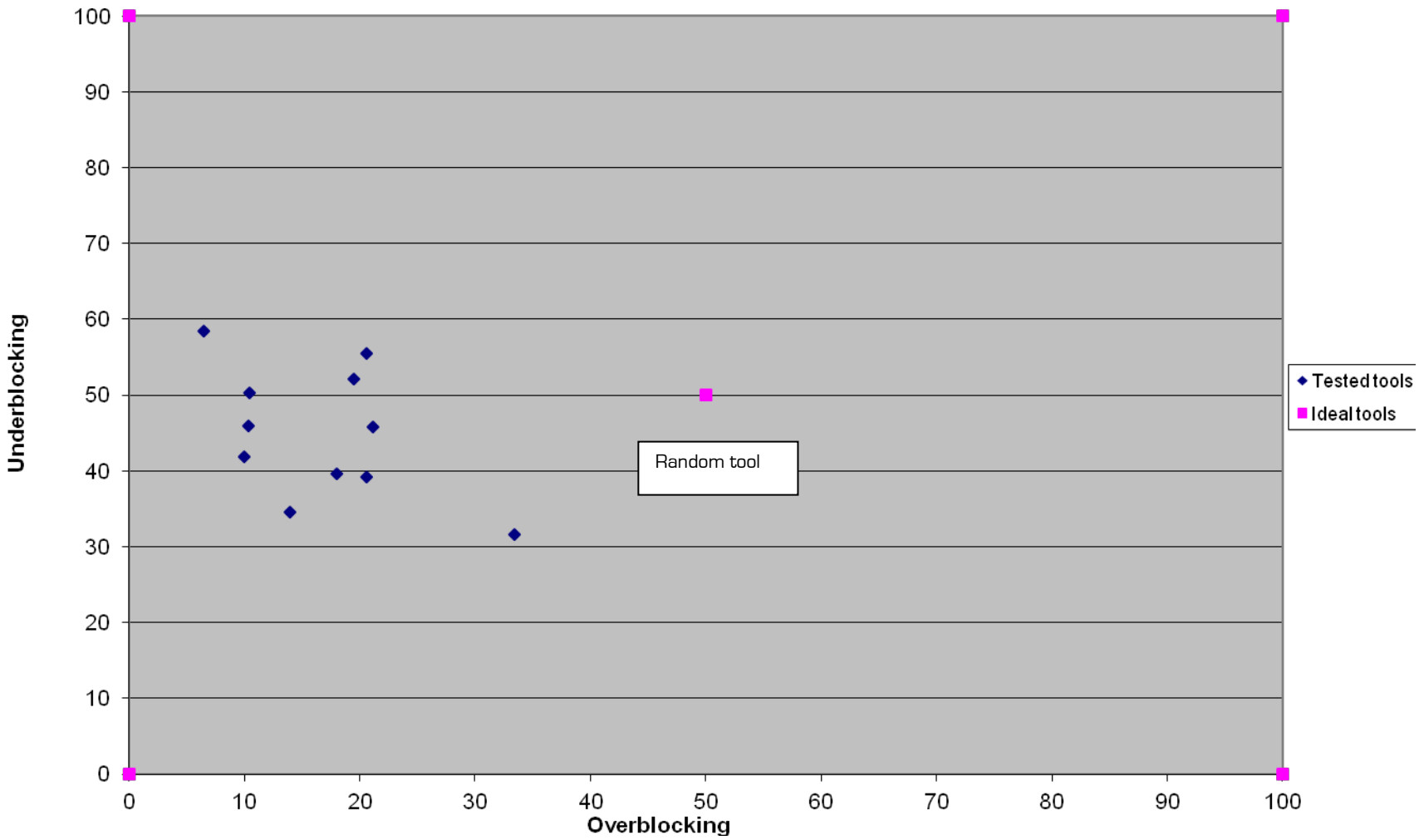
Effectiveness key findings

Note: NetIntelligence has not been tested on effectiveness as it was inoperative as far as effectiveness is concerned.

Tool that allows everything

The worst tool

PU PARENTAL CONTROL TOOLS: Effectiveness performance



A perfect tool

Tool that blocks everything

Each point represents the overblocking and underblocking of a tool.

PC PARENTAL CONTROL TOOLS: Effectiveness (score view)

Effectiveness assessed according to topic and age

Topic	Adult		Other		Overall Score	
	<12	>13	<12	>13	<12	>13
F-SECURE INTERNE	3,0	3,0	0,0	0,0	1,5	1,5
JUSPROG	N/A	1,4	N/A	1,8	N/A	1,6
K9 WEB PROTECT	2,2	2,4	0,0	0,0	1,1	1,2
MAC OS X PARENT	1,8	1,6	0,0	0,0	0,9	0,8
MCAFEE FAMILY P	2,0	2,0	0,0	0,0	1,0	1,0
NET NANNY	3,0	3,0	0,0	0,0	1,5	1,5
NET-INTELLIGENCE	N/A	N/A	N/A	N/A	N/A	N/A
NORTON ONLINE F	3,6	3,2	0,0	0,0	1,8	1,6
OPTENET	1,6	2,2	0,0	0,0	0,8	1,1
PANDA	2,6	2,2	0,0	0,0	1,3	1,1
PURESIGHT OWL	2,0	2,0	1,2	1,4	1,6	1,7
TREND MICRO ON	2,2	2,4	0,0	0,0	1,1	1,2
WINDOWS 8 FAM	3,0	3,0	0,0	0,0	1,5	1,5

PC Tools EFFECTIVENESS results: score view

How to read the table

The table shows how effective the tools are in filtering harmful content. The tool was scored both with reference to the "adult" content and to the "other harmful" content (drugs, violence, racism, etc.) taking into account two different class of age (≤12 years old and ≥13 years old). An overall score was assigned to each age class as **the 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'):

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

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

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

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

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

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

PC PARENTAL CONTROL TOOLS: Effectiveness (over/underblocking)

Underblocking and overblocking

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

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

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

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

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

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

Topic	Adult content		Violence and Crime		Racist		Drugs & Self-Damage		Gambling	
	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking
F-SECURE INTERNET SECURITY 2012	14	13	8	76	6	80	20	44	22	25
JUSPROG	20	37	13	45	12	55	11	52	16	41
K9 WEB PROTECTION	12	23	3	83	14	77	2	56	13	27
MAC OS X PARENTAL CONTROLS	30	21	17	77	10	85	9	69	13	51
MCAFEE FAMILY PROTECTION	22	22	15	63	14	60	8	65	19	41
NET NANNY	12	18	14	87	9	81	11	41	15	23
NET-INTELLIGENCE	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
NORTON ONLINE FAMILY	20	9	2	92	1	90	1	87	0	97
OPTENET	7	47	6	76	7	88	3	65	8	50
PANDA	31	11	30	75	12	82	52	34	49	18
PURESIGHT OWL	20	29	18	62	14	60	31	39	22	37
TREND MICRO ONLINE GUARDIAN FOR FAMILIES	10	25	11	70	9	72	9	85	14	40
WINDOWS 8 FAMILY SAFETY	10	14	6	80	8	78	12	55	17	40

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

How to read the table

The table shows how effective the tools are in blocking content according to the topic.
PARENTS can verify how effective is each tool for the categories they assume are more threatening for their children.
Results in % of overblocked or underblocked content.

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

Language	English		German		Italian		Spanish		French		Polish	
	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking
F-SECURE INTERNET SECURITY 2012	16	23	12	45	11	48	17	45	14	43	12	52
JUSPROG	20	39	15	37	19	50	17	51	23	50	22	52
K9 WEB PROTECTION	12	34	9	48	12	59	6	48	11	43	7	51
MAC OS X PARENTAL CONTROLS	21	27	14	51	16	62	14	71	20	64	29	70
MCAFEE FAMILY PROTECTION	21	25	15	50	18	67	15	70	20	65	31	69
NET NANNY	9	31	15	32	10	52	10	50	9	43	15	42
NET-INTELLIGENCE	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
NORTON ONLINE FAMILY	26	16	21	32	20	38	12	35	13	32	15	35
OPTENET	10	52	6	50	7	68	12	51	5	56	4	70
PANDA	47	31	32	36	29	44	27	39	30	36	31	42
PURESIGHT OWL	19	32	19	43	21	51	23	43	28	36	11	26
TREND MICRO ONLINE GUARDIAN FOR FAMILIES	10	35	8	48	14	62	2	57	18	48	7	63
WINDOWS 8 FAMILY SAFETY	12	40	8	44	11	38	8	50	14	43	8	59

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

How to read the table

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

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

Age	≤12		≥13	
	Overblocking	Underblocking	Overblocking	Underblocking
F-SECURE INTERNET SECURITY 2012	14	36	14	36
JUSPROG	N/A	N/A	17	40
K9 WEB PROTECTION	11	43	10	42
MAC OS X PARENTAL CONTROLS	25	53	17	35
MCAFEE FAMILY PROTECTION	8	39	30	39
NET NANNY	15	35	10	41
NET-INTELLIGENCE	N/A	N/A	N/A	N/A
NORTON ONLINE FAMILY	35	23	17	27
OPTENET	4	72	8	50
PANDA	39	30	38	40
PURESIGHT OWL	25	36	24	35
TREND MICRO ONLINE GUARDIAN FOR FAMILIES	7	46	8	42
WINDOWS 8 FAMILY SAFETY	10	42	17	37

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

How to read the table

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

Note: no results are available for the ≤ 12 age class, as Jusprog offers a white list access for this age class, which is not test with the current methodology.

PC PARENTAL CONTROL TOOLS: Effectiveness related to Web/Web 2.0 (over -/underblocking)

Web Type	Web		Web 2.0	
	Overblocking	Underblocking	Overblocking	Underblocking
F-SECURE INTERNET SECURITY 2012	15	27	11	53
JUSPROG	14	34	20	50
K9 WEB PROTECTION	8	39	15	50
MAC OS X PARENTAL CONTROLS	13	32	26	56
MCAFEE FAMILY PROTECTION	20	43	17	38
NET NANNY	8	22	14	53
NET-INTELLIGENCE	N/A	N/A	N/A	N/A
NORTON ONLINE FAMILY	20	24	21	23
OPTENET	3	53	4	73
PANDA	40	23	19	66
PURESIGHT OWL	18	36	26	49
TREND MICRO ONLINE GUARDIAN FOR FAMILIES	7	36	6	54
WINDOWS 8 FAMILY SAFETY	11	43	11	43

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

How to read the table

The table shows how effective the tools are according to the typology of content, whether it is part of the traditional Web or Web 2.0. The tools were tested both on user generated content or web 2.0 (blogs, social networks, forums) and traditional Web content (pages of website).

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

PC PARENTAL CONTROL TOOLS: Usability key findings

8 out of 13 tools gain better scores for installation and configuration than for usage. No products score less than 2 points, thus not reaching the threshold of 50 % of 4 points, five products range between 2 and 2.50, seven tools between 2.51 and 3. One product scores in the top area and gains 3 points or more.	
General findings	Some of the tools keep the installation and configuration procedures very simple. However, possibilities to customise the tool to one's own needs are poor. Other tools have very extended options to configure the software but then the risk of unwished configuration effects and bad filtering results is high. Only a few products provide additional information about filtering in general and about limitations and restrictions of the filtering procedures. About one third of the tools provide a web- or server-based configuration. This is an increasing number over the last test cycles. Web-based or remote management allows the parents to reconfigure and monitor their children's use from another device, but might consume more time for navigation and storage.
Findings on the installation process	A high percentage of tools keep the installation process very simple. In some cases the installation process runs nearly automatically and is similar to the installation of an App on a smart phone or other mobile device. Some tools merge the installation and first configuration steps into one single process.
Findings on the configuration process	The configuration process is key for the product because of its relevance for an effective use of the filter. For several tools there are very few configuration options. For other tools configuration is very exhaustive and comprises of a lot of functionalities. Some products compensate complexity by good explanations and a well-structured user interface. The range of customisation options is broad. For some tools there can be set only one degree of strength of filtering for all content categories, while others allow to differentiate the strength of filtering between different content categories. Several tools do not explain their filter categories, although some categories are quite unusual with regards to youth protection, i.e. sports or humour.
Findings on the usage of the tools	As most parental control tools work 'in the background', there is less usage than with other computer software. Nonetheless, it is important that parents can easily handle the alert messages and the reporting to keep them involved with the products. Testing of the usage of traditional parental controls refers mainly to the usability of alert messages for blocked web sites. Most tools do not address the alert message to children and youth but to adults only. Most tools do not allow appropriate reaction to the alert message for a blocked web site. Monitoring and reporting functionalities were tested as usage of the tools, where applicable. Reporting ranges from mere log file data to detailed and colourful diagrams. For alternative tools testing of usage covers also the usability for children as they are the user target group of those products.

PC PARENTAL CONTROL TOOLS: Usability table

How to read the table

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

I = Installation

C = Configuration /Re-configuration

U = Usage

Usability Tests	F-SECURE INTERNET SECURITY	JUSPROG	K9 WEB PROTECTION	MAC OS X PARENTAL CONTROLS	MCAFEE ALL ACCESS	NET NANNY	NETINTELLIGENCE	NORTON ONLINE FAMILY	OPTENET PC	PANDA	PURESIGHT OWL	TREND MICRO ONLINE GUARDIAN	WINDOWS FAMILY SAFETY
I	2.35	2.57	2.6	n/a	3.01	2.58	1.74	2.59	2.65	2.83	2.99	2.42	n/a
C	2.52	2.04	3.09	2.63	3	2.65	2.61	3.16	2.58	2.31	3.11	2.92	2.85
U	2.11	2.1	2.31	1.79	2.56	3.07	2.73	3.4	2.42	1.24	2.47	2.73	2.47
Overall score	**2.36**	**2.16**	**2.76**	**2.31**	**2.87**	**2.76**	**2.47**	**3.12**	**2.54**	**2.09**	**2.89**	**2.76**	**2.7**

PC Tools USABILITY result

PARENTAL CONTROL TOOLS FOR MOBILE DEVICES

FINDINGS FOR FUNCTIONALITY, SECURITY, EFFECTIVENESS, USABILITY

Mobile phones and the Internet
Smart phones are one of the most trendy 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 DEVICES PARENTAL CONTROL TOOLS: Functionality key findings

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

iPhone and iPad is equipped with an OS-embedded parental control tool which is able to restrict the usage of some protocols/applications such as Internet accessing by browser or YouTube and e-mail. However, an external parental control tool is necessary to filter web-pages browsing according to the content.
The other operating system, Android, does not provide an embedded tool for mobile phones or tablets. The only way to filter the Internet is to use an external tool.

Web Content Filtering 5 out of 9 tools give the parents the opportunity to personalise the filtering through the choice of filtered topics.
Only MOBIFLOCK, MOBILE PARENTAL FILTER, NET NANNY FOR ANDROID and NORTON ONLINE FAMILY (MOBILE) give the possibility to manage a white or black list of keywords.
Some tools give parents possibility to manage the tool online (from a PC or an other mobile device). For some tools—Norton for exemple—it is possible to manage both the mobile tool and the PC tool (provided that user installed both tools on teenager's devices).

Applications/Protocols and other issues
Concerning usage restriction and monitoring, the tools offer very limited functionalities, in particular for Skype or streaming which are very popular among teenagers.

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

Area of need	Usage Restriction															
Functionality	Email	P2P		Personal data Provision	Safe search	Skype		Social Networks		Streaming		Web		Windows Life Messenger		
Specific Issue	Block email client and/or webmail access	Block the application	Monitor Downloads	Block	Availability	Block chat	Block video chat	Block Access	Monitor Usage	Block Access	Monitor Access	Block Access	Monitor Access	Block chat	Block video chat	Monitor
BSecure	N	N	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N
F-Secure Mobile Security	Y	N	N	N	N	N	N	Y	N	N	N	Y	N	N	N	N
iOS Parental Controls (Mobile)	Y	Y	N	N	N	Y	N	Y	N	N	N	Y	N	N	N	N
K9 Web Protection Browser (Mobile)	N	N	N	N	Y	N	N	N	N	N	N	Y	Y	N	N	N
Mobicip Safe Browser	Y	N	N	N	N	Y	N	Y	N	Y	N	Y	N	N	N	N
Mobiflock	Y	N	N	N	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N	N
Mobile Parental Filter	Y	N	N	N	N	N	N	Y	N	N	N	Y	Y	N	N	N
NetNanny for Android	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	Y	N	N
Norton Online Family (Mobile)	Y	N	N	Y	N	N	N	Y	N	N	N	Y	Y	N	N	N
% of tools with	78 %	11 %	0 %	11 %	44 %	44 %	0 %	67 %	11 %	22 %	11 %	100 %	44 %	11 %	0 %	0 %

function																

MOBILE Tools FUNCTIONALITY results and security score

Area of need	Management			Filtering Customisation					Keywords			Time	Blocking Message			Security
Functionality	Management of User profiles	Monitoring	Remote Management	Topics	URLs Black List	URLs White List			Keywords			Time Limit Settings	Type			
Specific Issue	Create several profiles	Remote access to monitoring	Manage on various devices	Customisation of Filtering Topics	Creation of User's own Black List	Default White List	Modification OR Creation	Restrict Browsing to White List	Creation of a User's Black List	Creation of a User's White List	Default Black List	Set a specific time frame or web access duration	Ask for unblocking by parents	Redirect to safe resources	% function coverage	Score
BSecure	N	N	N	N	N	N	N	N	N	N	N	N	N	N	7 %	0
F-Secure Mobile Security	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	13 %	1
iOS Parental Controls (Mobile)	N	N	N	N	N	N	N	N	N	N	N	N	N	N	17 %	3
K9 Web Protection Browser (Mobile)	N	N	N	N	N	N	N	N	N	N	N	N	N	N	10 %	1
Mobicip Safe Browser	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N	23 %	0
Mobiflock	N	Y	Y	Y	Y	N	Y	N	N	N	N	Y	N	N	50 %	1
Mobile Parental	N	Y	Y	Y	Y	N	Y	N	N	N	N	Y	Y	N	37 %	1

Filter																
NetNanny for Android	Y	N	Y	Y	Y	N	Y	N	N	N	N	Y	Y	N	40 %	0
Norton Online Family (Mobile)	Y	Y	Y	Y	Y	N	Y	N	N	N	N	N	N	N	37 %	0
% of tools with function	33 %	33 %	56 %	56 %	44 %	0 %	44 %	0 %	0 %	0 %	0 %	33 %	22 %	0 %		

MOBILE Tools FUNCTIONALITY results and security score

MOBILE DEVICES PARENTAL CONTROL TOOLS: Effectiveness key findings

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

MOBILE PHONES PARENTAL CONTROL TOOLS – Effectiveness key findings

MOBILE PHONES PARENTAL CONTROL TOOLS: Effectiveness (score view)

MOBILE PHONES Tools EFFECTIVENESS results – Score view

Topic	Adult		Other		Overall Score	
	<12	>13	<12	>13	<12	>13
BESECURE	0,8	1,6	0,0	0,0	0,4	0,8
F-SECURE MOBILE	3,0	3,0	0,0	0,0	1,5	1,5
K9 WEB PROTECT	2,2	2,4	0,0	0,0	1,1	1,2
MOBICIP SAFE BR	2,2	2,4	0,0	0,0	1,1	1,2
MOBIFLOCK	0,6	1,2	0,0	0,0	0,3	0,6
MOBILE PARENTA	2,2	2,4	0,0	0,0	1,1	1,2
NETNANNY FOR A	1,4	1,8	0,0	0,0	0,7	0,9
NORTON ONLINE F	3,0	3,0	0,0	0,0	1,5	1,5

How to read the table
The table shows how effective the tools are in filtering harmful content. The tool was scored both with reference to the "adult" content and to the "other harmful" content (drugs, violence, racism, etc.) taking into account two different class of age (≤12 years old and ≥13 years old). An overall score was assigned to each age class as **the 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'):
0 Very weak - The tool is less effective than a random tool.
1 Weak - The tool has a low effectiveness and answers very partially to parents needs.
2 Fair - The tool has a fair lever of filtering, nonetheless a non small part of the content is not correctly filtered.
3 Good - The tool offers a good level of filtering but a part of the content is not correctly filtered.
4 Excellent - The tool offers a very good level of filtering and satisfy the parents' needs in terms of effectiveness.

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

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

Underblocking and overblocking

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

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

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

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

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

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

MOBILE DEVICES PARENTAL CONTROL TOOLS: Effectiveness (over -/underblocking)

Topic	Adult content		Violent and crime		Racist		Drugs and self-damage		Gambling	
	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking
BESECURE	8	50	8	85	7	87	6	80	14	70
F-SECURE MOBILE SECURITY	13	15	7	70	8	82	17	48	21	29
K9 WEB PROTECTION BROWSER	11	25	6	81	12	79	5	51	10	35
MOBICIP SAFE BROWSER	10	21	8	76	6	81	10	70	18	45
MOBIFLOCK	14	53	9	70	11	64	8	72	8	78
MOBILE PARENTAL FILTER	10	28	16	50	11	69	17	60	21	50
NETNANNY FOR ANDROID	16	40	6	84	14	79	40	49	36	43
NORTON ONLINE FAMILY MOBILE	19	13	4	90	2	85	5	84	2	96

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

Language	English		German		Italian		Spanish		French		Polish	
	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking	Overblocking	Underblocking
BESECURE	10	80	9	82	7	60	8	82	13	79	12	82
F-SECURE MOBILE SECURITY	12	14	10	74	8	81	16	50	17	30	12	53
K9 WEB PROTECTION BROWSER	14	35	11	42	10	55	9	46	10	45	7	51
MOBICIP SAFE BROWSER	20	42	42	59	33	59	31	58	36	60	41	61
MOBIFLOCK	7	80	14	83	18	79	12	72	10	79	15	52
MOBILE PARENTAL FILTER	13	41	17	64	13	56	10	50	19	60	25	73
NETNANNY FOR ANDROID	27	42	17	64	14	65	31	51	14	63	14	67
NORTON ONLINE FAMILY MOBILE	26	16	21	32	20	38	12	35	13	32	15	35

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

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

Web type	Web		Web 2.0	
	Overblocking	Underblocking	Overblocking	Underblocking
BESECURE	10	72	12	77
F-SECURE MOBILE SECURITY	15	27	11	53
K9 WEB PROTECTION BROWSER	8	40	15	50
MOBICIP SAFE BROWSER	35	51	39	64
MOBIFLOCK	16	42	14	63
MOBILE PARENTAL FILTER	15	42	14	63
NETNANNY FOR ANDROID	20	51	20	60
NORTON ONLINE FAMILY MOBILE	20	24	20	23

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

Age	≤12		≥13	
	Overblocking	Underblocking	Overblocking	Underblocking
BESECURE	11	78	9	71
F-SECURE MOBILE SECURITY	13	36	14	36
K9 WEB PROTECTION BROWSER	11	43	10	42
MOBICIP SAFE BROWSER	44	61	40	66
MOBIFLOCK	10	73	10	67
MOBILE PARENTAL FILTER	16	56	15	49
NETNANNY FOR ANDROID	19	53	13	54
NORTON ONLINE FAMILY MOBILE	32	23	18	27

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

MOBILE PHONES PARENTAL CONTROL TOOLS: Usability key findings

The scores for the mobile tools range between 1.42 and 2.87.

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

MOBILE PHONES PARENTAL CONTROL TOOLS: Usability table

Usability Tests	F-SECURE MOBILE SECURITY	IOS PARENTAL CONTROLS (MOBILE)	K9 WEB PROTECTION BROWSER (MOBILE)	MOBICIP SAFE BROWSER	MOBIFLOCK	MOBILE PARENTAL FILTER	NETNANNY FOR ANDROID	NORTON ONLINE FAMILY (MOBILE)
I	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
C	2.73	2.42	1.65	2.42	2.52	2.32	2.66	2.91
U	1.42	0.99	1.02	1.09	1.86	1.92	2.39	2.81
Overall score	**2.24**	**1.89**	**1.42**	**1.92**	**2.27**	**2.17**	**2.56**	**2.87**

MOBILE PHONES Tools USABILITY results

Note: BSecure works as a background software only. There are no customisation options to adjust the filter to parent's needs. Therefore, the tool could not be tested with regards to usability.

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 widely used to access the Internet. They are mainly used for online gaming, chatting with other players and downloading content.

GAME CONSOLES PARENTAL CONTROL TOOLS: Functionality key findings

The functionalities of the tools for consoles are very limited compared to other devices.
There are only basic 'enable' or 'disable' functions or irregular working filtering functionalities for websites.
The OS-embedded tools are focused on the control of other online activities: online gaming and content downloading/purchasing (apart from a series of offline activities filtering).

Web browsing and Content filtering
Trend Micro and Astaro claim to filter webpages. However, filtering does not work in neither of them. Astaro blocks all web access through browser, also all non-harmful pages. Trend Micro shows a short time harmful pages before fading in a blocking message.

Access to the Internet
All the consoles enable the PARENTS to switch off the access to the Internet.

Monitoring
None of the tools is able to monitor the online child/teenager activity.

Area of need	Usage Restriction															
Functionality	Email	P2P		Personal data Provision	Safe search	Skype		Social Networks		Streaming		Web		Windows Life Messenger		
Specific Issue	Block email client and/or webmail access	Block the application	Monitor Downloads	Block	Availability	Block chat	Block video chat	Block Access	Monitor Usage	Block Access	Monitor Access	Block Access	Monitor Access	Block chat	Block video chat	Monitor
Astaro - Parental	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N

Control for Wii*																
Microsoft Live Safety	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
Trend Micro Kids Safety - PS3	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
% of tools with function	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	100 %	0 %	0 %	0 %	0 %

GAME CONSOLES Tools FUNCTIONALITY results and security score

Area of need	**Management**			**Filtering Customisation**					**Keywords**			**Time**	**Blocking Message**			Security
Functionality	**Management of User profiles**	**Monitoring**	**Remote Management**	**Topics**	**URLs Black List**	**URLs White List**			**Keywords**			**Time Limit Settings**	**Type**			
Specific Issue	**Create several profiles**	**Remote access to monitoring**	**Manage on various devices**	**Customisation of Filtering Topics**	**Creation of User's own Black List**	**Default White List**	**Modification OR Creation**	**Restrict Browsing to White List**	**Creation of a User's Black List**	**Creation of a User's White List**	**Default Black List**	**Set a specific time frame or web access duration**	**Ask for unblocking by parents**	**Redirect to safe resources**	**% function coverage**	**Score**
Astaro - Parental Control for Wii	N	N	N	N	N	N	N	N	N	N	N	N	N	N	0 %	N/A
Microsoft Live Safety	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	7 %	N/A
Trend Micro Kids Safety - PS3	N	N	N	N	N	N	N	N	N	N	N	N	N	N	3 %	2

% of tools with function	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	33 %	0 %	0 %		

GAME CONSOLES Tools FUNCTIONALITY results and security score

* Astaro blocks all web access through browser. Filtering does not work and Astaro refuses Internet connection with different error messages. According to Nintendo's Support, Astaro for Wii has been discontinued.

GAME CONSOLES PARENTAL CONTROL TOOLS: Effectiveness key findings

There are only few tools for consoles providing Web filtering functionalities. A tool for PS3 has been tested: it offers similar but slightly lower results compared to the product for PC produced by the same company. A tool for Wii was tested but the filtering functionality was not effective. The Xbox default tool offers only the possibility for the parent to block or allow the access to the Internet.Therefore, it was not possible to access the Internet.	
Underblocking/Overblocking	We can assume that PS3 TREND MICRO operates on the basis of a URLs blacklist and allows all pages not present in its black list, for that reason the overblocking is very low while the underblocking is high.
Age classes	The tool performs quite similarly with a configuration for the two age classes (≤12 and ≥ 13). 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. • No possibility of choosing content categories to be filtered or not.
Web and Web 2.0	Web 2.0 filtering performance is lower than on traditional Web. Concerning the qualitative tests on web 2.0, all tools fail.
Topics	Concerning topics, both TREND MICRO performs better filtering on adult content rather than other categories of content. For PS3, some categories are completely ignored like Crime or Self-damage while other non-adult content categories are badly filtered.
Languages	The tool filters better on English content than on other languages.

GAME CONSOLES PARENTAL CONTROL TOOLS – Effectiveness key findings

Note: Microsoft Live Safety has not yet been tested against effectiveness criterion. As a parent you can only activate or deactivate Internet access, there is no filter option. Astaro is not working and it was not possible to test effectiveness.

GAME CONSOLES PARENTAL CONTROL TOOLS: Effectiveness (score view)

Topic	Adult		Other		Overall Score	
	≤12	≥13	≤12	≥11	≤12	≥13
ASTARO (Wii)	N/A	N/A	0,0	0,0	**0,0**	**0,0**
TREND MICRO SAFETY (PS3)	1,4	1,8	0,0	0,0	**0,7**	**0,9**
MICROSOFT LIVE SAFETY (XBOX)	N/A	N/A	N/A	N/A	**N/A**	**N/A**

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, etc.) taking into account two different classes of age (≤12 years old and ≥13 years old). An overall score was assigned to each age class as the results of the average performance of the two content topic types. The scoring scale considers both the underblocking (harmful pages which are not blocked) and overblocking (non harmful pages which are blocked). For a comprehensive understanding of the assessment, please read the 'Methodology key issues'.

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

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 CONSOLES PARENTAL CONTROL TOOLS: Effectiveness

Underblocking and overblocking

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

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

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

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

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

GAME CONSOLES PARENTAL CONTROL TOOLS: Effectiveness

Topic		ASTARO (Wii)	TREND MICRO KIDS SAFETY (PS3)	MICROSOFT LIVE SAFETY (XBOX)
Adult content	Overblocking	N/A	12	N/A
	Underblocking	N/A	32	N/A
Violent and crime	Overblocking	N/A	5	N/A
	Underblocking	N/A	81	N/A
Racist	Overblocking	N/A	4	N/A
	Underblocking	N/A	78	N/A
Drugs and self-damage	Overblocking	N/A	3	N/A
	Underblocking	N/A	69	N/A
Gambling	Overblocking	N/A	22	N/A
	Underblocking	N/A	56	N/A

GAME CONSOLES Tools EFFECTIVENESS

results for topics: % of over -/underblocked content

Language		ASTARO (Wii)	TREND MICRO KIDS SAFETY (PS3)	MICROSOFT LIVE SAFETY (XBOX)
English	Overblocking	N/A	13	N/A
	Underblocking	N/A	47	N/A
Italian	Overblocking	N/A	16	N/A
	Underblocking	N/A	50	N/A
German	Overblocking	N/A	6	N/A
	Underblocking	N/A	56	N/A
Spanish	Overblocking	N/A	5	N/A
	Underblocking	N/A	61	N/A
French	Overblocking	N/A	13	N/A
	Underblocking	N/A	48	N/A
Polish	Overblocking	N/A	14	N/A
	Underblocking	N/A	68	N/A

GAME CONSOLES Tools EFFECTIVENESS

results for languages: % of over -/underblocked content

GAME CONSOLES PARENTAL CONTROL TOOLS: Effectiveness

Web type		ASTARO (Wii)	TREND MICRO KIDS SAFETY (PS3)	MICROSOFT LIVE SAFETY (XBOX)
Web	Overblocking	N/A	13	N/A
	Underblocking	N/A	53	N/A
Web 2.0	Overblocking	N/A	3	N/A
	Underblocking	N/A	69	N/A

GAME CONSOLES Tools EFFECTIVENESS

Each table shows how effective the tools are in blocking content with reference to the **age and Web types** (Web/Web 2.0).
With regards to the web types, the tools were tested both on user generated content or Web 2.0 (blogs, social networks, forums) and traditional web content (pages of websites).
PARENTS can verify how effective is each tool in relation to the topic they are more interested in. Results in % of content overblocked or underblocked.

GAME CONSOLES PARENTAL CONTROL TOOLS: Usability key findings

Compared to parental control tools for PCs, those for game consoles seem to be less known by parents. Nonetheless, they can be useful but the configuration of game consoles can be difficult for parents.	
Installation	It is a challenge for parents to learn about and to decide on the need to install an additional parental control tool on game consoles. ASTARO for Wii, MICROSOFT LIVE SAFETY and TREND MICRO for PS3 serve as applications installed nearly automatically with the download. Therefore, there is no installation process to be handled by the user.
Configuration	All tools provide barely any option for configuration, MICROSOFT LIVE SAFETY allows only to activate or deactivate Internet access. The process might be unfamiliar for parents and is not well supported. Some parts are difficult to understand.
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 to keep them involved with the products. The tools do not address the alert message for a blocked web site to children and youth but to adults only. Also no appropriate option for reaction to the alert message is provided. No reporting is offered.*

GAME CONSOLES PARENTAL CONTROL TOOLS: Usability key findings

*During the testing cycle it was not possible to connect with the ASTARO server. As a result, the filtering functions were not operating and alert messages occured. Therefore, the assessment of the alert message is related to the previous testing cycles.

GAME CONSOLES PARENTAL CONTROL TOOLS: Usability table

GAME CONSOLES Tools USABILITY results

Usability Console	ASTARO - PARENTAL CONTROL FOR WII	MICROSOFT LIVE SAFETY	TREND MICRO KIDS SAFETY - PS3
I	n/a	n/a	n/a
C	1.37	2.29	0.69
U	0.51	0.87	1.23
Overall score	**1.05**	**1.76**	**0.89**

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 is aimed at assessing the tools according to various features: functionality, effectiveness, usability, configurability, transparency, and security for the European users. Four benchmarking cycles are foreseen, each cycle every 8 months. The results of each benchmarking cycle consist in:

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

The assessment activity was based on a specific methodology. The Report and the methodology described herein refer to the 1st **Cycle.**

Users' Needs

The definition of the users' needs was a starting point of the study activity and is key to reading of the Report: It oriented the testing activity providing some criteria for the tools selection and for the dataset creation, the parameters for the tool testing and the key to the presentation of the results.
The analysis of users' needs was carried out starting from a literature of existing studies and reports and complemented by our experience in the field in terms of the Internet and digital threats. The users' needs with regard to usability have been identified in a first place based on previous experiences derived from the work with children's welfare organizations and other experts in the field, esp. at the Youth Protection Roundtable.

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

METHODOLOGY: KEY ISSUES

The analysis resulted in:

• The identification of 3 main **devices** used to access the Internet: **PC, mobile devices (phones and tablets) and game consoles.**

• The identification of the actions performed by the CHILDREN/TEENAGERS that might expose the children/teenagers to risks**:**
- **Visualizing** content present on websites, including content available in streaming and on the Internet through blogs, social networks and forums.
- **Communicating online** by means of e-mail and social networking and Instant Massaging including video chat, VoIP and chat section available in gaming.
- **Uploading/downloading and sharing** files (like applications and video) through the Web or Peer to Peer applications.

• The definition of the **needs in terms of functionality/security/effectiveness/usability** as reported in the tables 2, 3, 4 and 5 of this Report.

• The identification of **three types of activities** that the PARENTS would require the tool to be able to perform:
- Filtering web-pages according to content topics (including the advertising present on web pages).
- Blocking the usage of a protocol/application including the control of spending amount through mobile devices.
- Monitoring the application/protocol usage and the Web content accessed.

• The selection of the **applications/protocols** or more generally the specific **Internet spheres** mainly used for these activities.

METHODOLOGY: KEY ISSUES

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

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

USERS' NEEDS: topics parents are concerned with

METHODOLOGY: KEY ISSUES

Selection of tools to be tested

There are numerous filtering solutions. **25 tools** have been considered in this test. The selection was aimed at covering the parents' needs in terms of devices (PCs, Mobile Phones, Consoles), operating systems (Windows, Mac, Android), languages, type of solutions (default systems like Microsoft Live family safety or, client software,) and capacity to meet their needs.
The selection of filtering and parental control tools that are the subject of testing and benchmarking activity is carried out in parallel with the analysis of users' needs.

- Functions achieved by the tools which can address one or several among the following ones:

- Interface in several EU languages: the filtering tools shall have multilingual user interfaces that cover most of the EU languages.

- Filter regardless of the language: the filtering tools should be able to filter multilingual content, at least in one EU language and, preferably, in several EU languages.

- Cover the main devices: the filtering tools have a version that can be executed on the main hardware devices and software systems offering Internet access to the users.
- Type of tools: stand-alone solutions, server solutions, ISP service provided with Internet connection, service provided by phone companies and default tools provided by software manufacturers or embedded in operating systems. Support the main Operating Systems: the filtering tools shall be supported on the main Operative Systems available on selected devices:
- Support the main browsers:
- the filtering tools shall support the main web browsers: Internet Explorer, Firefox, Google Chrome, Safari.

- Filtering methods (blacklist of URLs, white list of URLs, word lists, text analysis, image analysis)

The group of tools will always include the main players (market share relevancy criterion) and also some interesting "outsiders" and tools which interface and filtering capacity cover some less popular EU languages (for instance, Slovenian) as far as they are also available in English language for testing. If available at least one free tool will be included for each main device.
Some alternative tools (walled gardens, child safe browsers) will be also tested.

METHODOLOGY: KEY ISSUES

Testing strategy for Usability and Functionality (Capability)

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

Functionality test by experts

Firstly, the tools will be checked against an open-ended list of standardised functionalities one would expect from a parental control tool, like customising content filtering, allowance of remote management or settings for the provision of personal data.

Functionalities not available will be marked, but not followed further. Functionalities that are available will be reviewed with regards to their usability by experts in the laboratory. In case the usability reviews reveal further functionalities not detected earlier, these will also be reviewed regarding their usability. By this strategic approach, it can be ensured that the whole range of functionalities available is attributed to the product and reviewed with regards to usability.

Area of Need	**Functionality / Capability**	**Specific Issue**
Management	Management of User profiles	Create several profiles
	Remote Management	Manage on various devices
	Monitoring	Remote access to monitoring
Filtering Customisation	Topics	Customisation of Filtering Topics
	URLs White List	Restrict Browsing to White List

		Default White List
		Modification OR Creation
	URLs Black List	Creation of User's own Black List
Keywords	Keywords	Default Black List
		Default White List
		Creation of a User's Black List
		Creation of a User's White List
Time	Time Limit Settings	Set a specific time frame or web access duration Monitor / observe the time spent online
Blocking Message	Type	Ask for unblocking by parents
		Redirect to safe resources
Usage Restriction	Web	Block Access
		Monitor Access
	Safe search	Availability
	Social Networks	Block Access
		Monitor Usage
	Personal data Provision	Block
	Streaming	Bloack Access
		Monitor Access
	P2P	Block the application

		Monitor Downloads
	Skype	Block chat
		Block video chat
		Monitor
		Prevent new Contact
	Windows Life Messenger	Block chat
		Block video chat
		Monitor
		Prevent new Contact
	Email	Block email client and/or webmail access

List of functionalities to be checked prior to usability test

Usability tests

Usability of filtering software is crucial for its effectiveness. Therefore, it is necessary to pay attention to the usability of the tools tested in the benchmarking. 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 software products often do not unfold their full potential due to usability deficiencies. If the users are not able to adjust the products to their needs and maintain the software on their own system, the filtering results are poor. Deficiencies in usability shall be detected in the benchmarking by expert reviews.

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

Usability review in laboratory

For each filtering tool a usability review will be accomplished in parallel by two experts in a usability laboratory. Thus. it will be ensured that usability of the products is tested and in a standardised manner to achieve comparable and consolidated results.
Usability testing will consider the relevant usability aspects including installation, configuration/customisation, general user experience, documentation, supported operating systems and updating capabilities.

The criteria tested in SIP Bench III are:

Usability:

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

Configurability:

- Parameter configuration
- Setting up classes of users (e.g. age, cultural background)

- Customising filtering criteria
- Possibility to manage and / or limit the time spent online and online purchases (such as app downloads etc.)

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

The critera catalogue is arranged into the following seven sub-categories according to DIN ISO standards :

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

Criteria catalogue

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

Results from the usability review in laboratory

The usability analysis report will include description of the functionalities available and numerical evaluation and comments and recommendations on the usability of the tools. The numerical evaluation of the usability will be based on the expert reviews. By answering to the

questionnaire, experts will have to choose between answers corresponding to numerical values. Following the testing, the two experts consolidate their results to achieve integrity and balance. It will be possible to have a numerical assessment of the usability of the various tools.

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

Testing activity: security test

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

Peculiarities for Mobile Phones and Game Consoles
The test was carried out with reference to the external tools and based on a subset of criteria as indicated in the table below.

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

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

Description of the score	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 (e.g., Google Translate)	x
	1	Renaming a blocked application	
Issues requiring some computer skills	2	Using the IP address instead of the URL	x
	2	Using a proxy instead of a direct connection to the Internet	x
	2	Changing time and date settings (to overcome time limits usage)	x
Minor issues	3	Starting the computer in Safe Mode	x
No issues identified	4	No issues	

Set of criteria and scoring for security

METHODOLOGY: KEY ISSUES

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

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

Methodology for Security Testing

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

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

METHODOLOGY: KEY ISSUES

Testing activity: effectiveness test

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

Data used to test the tools
A sample of 4000 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 **≤ 12** (notably children) and **and/or for ≥ 13 years old** (notably teenagers).

Tests of user generated content filtering

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

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

Content that is evolving over time

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

Content that is personalised by the user

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

Platforms hosting massively user generated content

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

Multimedia content with little textual information

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

Outbound content

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

For each one of these kind of contents Cybion will assess the tools with qualitative tests.

METHODOLOGY: KEY ISSUES

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

The chart below shows the data set figures used for 1st cycle during the **effectiveness test**. The data set for the effectiveness testing does not include e-mail, chat, P2P or VOIP content. With relation to these type of data, the tools were tested only from a functional point of view (functionality test), i.e. in terms of the potentiality of the tool to BLOCK or MONITOR the application/protocol usage, see **Ethical Issues** paragraph below. Each Web page has been manually reviewed to assess the harmfulness and the topic related. Data according to web type/ Data according to content type and appropriateness.

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

Data set composition

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

METHODOLOGY: KEY ISSUES

Methodology for effectiveness assessment

The test is aimed at measuring how effectively each tool blocks harmful content and allows non-harmful content. The test was carried out according to: language, age, topic and Web type (Web / Web 2.0).
For each tool an **automatic test** was carried out to see if each page was blocked or not. This test was performed with the default configuration of the software.

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

The tools effectiveness 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 content will be rarely blocked.

METHODOLOGY: KEY ISSUES

Global rating issues

	Weight %	
	<12	>13
Effectiveness	65	55
Usability	25	25
Security	10	20

METHODOLOGY: KEY ISSUES

Results disclosure

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

Ethical and legal issues

The content/pages covered by authentication procedure or generally related to the user's personal private communication (social network, chat, Instant Messaging, emailing) was excluded from the data set used to test the tool effectiveness due to the EC commitment to respect the children's privacy rights.
The exchange on material protected by copyrights, which constitutes the most of material exchanged to Peer to Peer networks, was also excluded from the data set used to test the tool effectiveness.

GLOSSARY

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

Configuration	It is an arrangement of functional units according to their nature, number, and chief characteristics. Often, configuration pertains to the choice of hardware, software, firmware, and documentation and affects system function and performance.
Cookie	Also known as a "Web cookie", "browser cookie", and "HTTP cookie", it is a piece of text stored by a user's Web browser.
Download	Downloading is the process of transferring (software, data, character sets, etc.) from a distant to a nearby computer, from a larger to a smaller computer, or from a computer to a peripheral device.
E-mail	"Electronic mail", commonly called email or e-mail, is the method of exchanging digital messages across the Internet or other computer networks.
E-Mail Client	An "email client", "email reader", or more formally "mail user agent" (MUA), is a computer program used to manage user's email.
File Sharing	File sharing is the practice of distributing or providing access to digitally stored information, such as computer 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.

HTTP	The "Hypertext Transfer Protocol" is a networking protocol for distributed, collaborative, hypermedia information systems: it is the foundation of data communication for the World Wide Web.
Installation	Installation (or setup) of a program is the act of putting the program onto a computer system so that it can be executed.
Instant Message	Instant messaging (IM) is a form of real-time direct text-based communication between two or more people using personal computers or other devices, along with shared software clients. The user's text is conveyed over a network, such as the Internet..
ISP (Internet Service Provider)	Also referred to as an "Internet access provider" (IAP), it is a company that offers its customers access to the Internet.
Instant Message	Instant messaging (IM) is a form of real-time direct text-based communication between two or more people using personal computers or other devices, along with shared software clients. The user's text is conveyed over a network, such as the Internet.
Messenger	MSN Messenger (now named Windows Live Messenger) is an instant messaging client created by Microsoft.
Online chatting	It refers to direct one-on-one chat or text-based group chat (also known as "synchronous conferencing"), using tools such as instant messengers, Internet Relay Chat, talkers and possibly Multi-User Domains..

Operating System	An operating system (OS) is a software, consisting of programs and data, that runs on computers and manages the computer hardware and provides common services for efficient execution of various application software. Windows, Mac OS or Linux are operating systems
Overblocking	It occurs when the tool blocks non-harmful content.
P2P	"Peer-to-peer" (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-topeer 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 and chat over the Internet.
Social network	A social network is an online service, platform, or site where people share ideas, activities, events, and interests within their individual or shared networks. Facebook is a social network.

Temporary Internet Files	Temporary Internet Files is a directory on Microsoft Windows computer systems used by Internet Explorer and other Web browsers to cache pages and other multimedia content, such as video and audio files, from websites visited by the user. This allows such websites to load more quickly the next time they are visited.
Underblocking	It occurs when the tool allows harmful content.
Uninstallation	It is the removal of all or parts of a specific application software.
Upload	Uploading is the sending of data from a local system to a remote system with the intent that the remote system should store a copy of the data being transferred.
URL	A "Uniform Resource Locator" specifies where an identified resource is available and the mechanism for retrieving it. The best-known example of the use of URLs is for the addresses of Web pages on the World Wide Web, such as http://www.example.com/.
Virus	A computer virus is a computer 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.
Whitelist	A list that identifies keywords, URL or website addresses considered safe.

TOOLS LIST

Parental control tools for PCs:

- F- SECURE INTERNET SECURITY
- JUSPROG
- K9 WEB PROTECTION
- MAC OS X PARENTAL CONTROLS
- MC AFEE ALL ACCESS
- NET NANNY
- NORTON ONLINE FAMILY
- PURESIGHT OWL
- TREND MICRO ONLINE GUARDIAN
- WINDOWS 8 LIVE FAMILY SAFETY
- NET-INTELLIGENCE
- PANDA
- OPTENET

Parental control tools for Mobile Devices:

- BSECURE
- F-SECURE MOBILE SECURITY
- iOS Parental Controls
- K9 WEB PROTECTION
- MOBICIP SAFE BROWSER
- MOBIFLOCK
- MOBILE PARENTAL FILTER
- NET NANNY FOR ANDROID
- NORTON ONLINE FAMILY MOBILE

Parental Control Tools for Game Consoles:

- ASTARO
- MICROSOFT LIVE SAFETY
- TREND MICRO