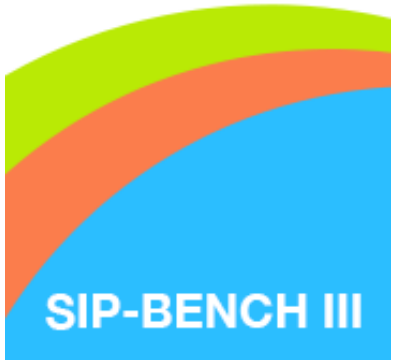

Benchmarking of parental control tools for the online protection of children

SIP-Bench III

4th CYCLE STUDY REPORT

Assessment results

(v.6)

SAFER INTERNET PROGRAMME

Empowering and Protecting Children Online

March 2017

The Study is Funded by the European Union, through the “Safer Internet Programme” 2008-2012 http://ec.europa.eu/saferinternet

The Study Report has been prepared by INNOVA Srl in collaboration with Cybion Srl and Stiftung Digitale Chancen (hereafter named as “the Consortium”) for the European Commission Directorate General for Communications Networks, Content and Technology – DG CONNECT.

The document reports the results of the 4th benchmarking testing cycle carried out during the period July-December 2016.

Main contact for the Study:

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

Table of content

INTRODUCTION 3
1. WHAT ARE PARENTAL CONTROL TOOLS? 4
2. SIP-BENCH III TESTING CONTEXT 5
3. THE 4th SIP BENCH III TESTING CYCLE 6
4. PARENTS CONCERNS AND AREAS OF TOOLS' PERFORMANCE 7
5. ELEMENTS ASSESSED DURING THE BENCHMARKING TESTS 10
6. OVERVIEW OF THE 4TH BENCHMARKING TESTING CYCLE RESULTS 11
7. PARENTAL CONTROL TOOLS FOR PERSONAL COMPUTERS 16
7.1. PC PARENTAL CONTROL TOOLS FUNCTIONALITY: key findings 17
7.2. PC PARENTAL CONTROL TOOLS EFFECTIVENESS: key findings 21
7.3. PC PARENTAL CONTROL TOOLS USABILITY: key findings 28
7.4. PC PARENTAL CONTROL TOOLS SECURITY: key findings 30
8. PARENTAL CONTROL TOOLS FOR MOBILE DEVICES 31
8.1. MOBILE PHONES PARENTAL CONTROL TOOLS FUNCTIONALITY: key findings 31
8.2. MOBILE PHONES PARENTAL CONTROL TOOLS EFFECTIVENESS: key findings 36
8.3. MOBILE PHONES PARENTAL CONTROL TOOLS USABILITY: key findings 43
8.4. MOBILE PHONES PARENTAL CONTROL TOOLS SECURITY: key findings 45
9. ALTERNATIVE TOOLS 46
9.1. 9.1. ALTERNATIVE TOOLS FUNCTIONALITY: key findings 46
9.2. ALTERNATIVE TOOLS EFFECTIVENESS: key findings 51
9.3. ALTERNATIVE TOOLS USABILITY: key findings 52
9.4. ALTERNATIVE TOOLS SECURITY: key findings 54
10. PARENTAL CONTROL TOOLS FOR GAME CONSOLES 55
11. RESULTS DISCLOSURE AND ETHICAL/LEGAL ISSUES 57
12. CONCLUSIONS 59
ANNEXES 61
ANNEX 1 - TOOLS LIST 62
ANNEX 2 - GLOSSARY 63

INTRODUCTION

The present document is the 4th report produced in the framework of the project *SIP-Bench III* – "*Benchmarking of parental control tools for the online protection of children"*, funded by the European Commission in the framework of the Safer Internet Programme 2008-2012.

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

- Raise awareness on tools that help protecting CHILDREN/TEENAGERS from Internet threats;
- Provide the end-users (notably PARENTS) with an overview of the existing parental control tools benchmarked according to end-users' identified needs;
- Support the end-users in the selection of the most appropriate parental control tools that best match their specific needs.

The report aims to present results of the 4th benchmarking testing cycle conducted in the period July-December 2016 on a set of 25 parental control tools available on the market. The testing cycle has assessed some main areas of performance of tools (Functionality, Usability, Effectiveness and Security).

The report is intended as support guidance to PARENTS in the selection of the most suitable tool according to specific needs and requirements.

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 through awareness raising initiatives and by fighting illegal and harmful online content and conduct.

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

The results of the Study are also available online through a searchable database on the project website http://sipbench.eu/ that allows extracting ranking lists of tools to help and guide users in the decision making process.

1. WHAT ARE PARENTAL CONTROL TOOLS?

One of the biggest concerns PARENTS have about the Internet is the type of websites their CHILDREN/TEENAGERS are browsing and the content they may be viewing. 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 behaviours of which they can be victims or authors (e.g., sexting, cyberbullying, and paedophilia).

It is therefore important to empower CHILDREN/TEENAGERS using online media safely and responsibly. Today, the market provides PARENTS with numerous tools to support their CHILDREN/TEENAGERS 'protection' from such threats. Such tools are known as '*PARENTAL CONTROL TOOLS*' and may have **four different functions**:

- Block addresses – to avoid access to specific Internet addresses (URLs or IP addresses);
- Filter content – to identify inappropriate content accessed;
- Manage usage – to limit Internet access by setting time limits and time quotas;
- Monitor activities – to check, through alerts and reporting, CHILDREN/TEENAGERS activity on Internet.

There are **different** ways to make **use** of a PARENTAL CONTROL TOOL:

- ☞ Install a software on the PC or download an app on the mobile device;
- ☞ Subscribe to an online filtering service offered by an Internet Service Provider (ISP);
- ☞ Combine both solutions;
- ☞ Parental control tools features may be embedded inside the Operating System (OS), or embedded in internet browsers (such as Chrome, Firefox..) and embedded in online services (safe search, social networks settings, online platforms settings).

Once the tool is operative, PARENTS can:

- ✓ Customise Web content filtering: ask the tool to block or show content or set a level of filtering (low, medium, high)
- ✓ Block the usage: block the usage of some applications (for instance, Skype or Peer to Peer applications)
- ✓ Monitor: track location and activity when the devices are used.

2. SIP-BENCH III TESTING CONTEXT

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

From simple content filters to robust home network solutions, new PARENTAL CONTROL TOOLS offer a range of different media-management options. Within the SIP-BENCH III Study **four** different **categories of tools** have been considered:

- Parental control tools for PC/MAC (**PC tools**): tools that may be executed or installed on PC/MAC;
- Parental control tools for mobile devices (**Mobile tools**): tools that may be executed or installed on mobile devices (such as smartphones, tablets, etc.);
- Parental control tools for **Game consoles:** tools that may be executed on console machines to be used for online gaming, chatting with other players and downloading content;
- **'Alternative tools'**, such as tools based entirely on white lists (so called "walled gardens"), or child safe browsers, which are usually designed to create a safe environment for very young children.

The parental control tools for game consoles were considered separately from PC tools since their primary use is not Web surfing but game and online game (including chatting).

By the second SIP Bench III cycle, however, the parental control tools for game consoles category was skipped as no new or improved versions of previously tested tools for game consoles were found available on the market.

To conduct the tests a **large data set test** has been used (more than 4,000 items) considering different categories of content (**adult content, other harmful content, non-harmful content). The data set test** included about 30 % of **user-generated content** (blogs, chat, multimedia content, personal pages) to better analyse features, strength and weaknesses of each tested tool.

3. THE 4th SIP BENCH III TESTING CYCLE

The 4th SIP BENCH III benchmarking cycle has been conducted on a list of **25 selected tools** segmented according to the access device as it follows:

- **10 PC/MAC parental control tools**
- **10 parental control tools for mobile devices**
- **5 Alternative parental control tools.**

The complete list of benchmarked tools is included in ANNEX 1 to this report.

4. PARENTS CONCERNS AND AREAS OF TOOLS' PERFORMANCE

The criteria guiding PARENTS in the selection of the most appropriate tool are different according to the specific concerns they have (avoid CHILDREN/TEENAGERS viewing/producing inappropriate content, being a victim/author of a harmful communication, spending too much time on the Internet or using certain applications/protocols).

SIP-BENCH III has identified **four** main **areas of tools performance** (**Functionality, Security, Effectiveness, and Usability**) that can be linked to the specific PARENTS' needs. The benchmarking testing exercise has been focused on the four areas as shown In Table 1 below.

Table 1 – AREAS OF PERFORMANCE FOR BENCHMARKING TESTS

AREA OF PERFORMANCE	TESTING PURPOSE	QUESTIONS BY USERS TO BE ADDRESSED
FUNCTIONALITY	To assess which functionalities the tool provides	Does the tool offer the required functionality? Is there a functionality to block the access to social networks? Is it possible to have a different level of filtering for a 7-year-old daughter and a 16-year-old son?
EFFECTIVENESS	To measure 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 visiting suitable websites?
USABILITY	To assess if the tool can be easily installed, configured, used and maintained by average users	Will it be easy/difficult/almost impossible to install and configure the tool?
SECURITY	To assess the tool resistance to attempts to by-pass it by means of specific actions	Is it easy or difficult for the CHILD/TEENAGER to uninstall or by-pass the tool and access the Internet freely?

In the following tables, the users' needs have been identified and segmented in relation to the four areas of performance.

Table 2 - FUNCTIONALITY NEEDS

Type of Need	Need Description
COMPATIBILITY	If the device is already available, check if the tool is compatible with the operating system (e.g., Windows, Mac OS, Linux) and the related version (e.g. Vista, 7, 8).
DIFFERENT USERS	If the access to the device is open to more than one user with different filtering requirements, there is a need to manage specific and customised features.
CUSTOMISATION OF FILTERING	If there are specific needs with regards to content to be filtered (topics, specific URLs white and black list). This might be useful when there is a particular concern by certain topics, wish to restrict CHILDREN/TEENAGERS navigation to safe websites and block the others.
KEYWORDS	If there is a particular concern on words that CHILDREN/TEENAGERS may find in the webpages and communication messages.
TIME RESTRICTION	If there is concern about the time CHILDRENT/TEENAGERS spend in the Internet (browsing, playing or communicating).
USAGE RESTRICTIONS	If there is interest 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 to control such protocols/applications. The type of control considered for the test is: block/monitor. There could be interest in blocking 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 represents one of the PARENTS increasing concerns. Communication/networking tools are an opportunity for CHILDREN/TEENAGERS to share their opinions and find new friends but they imply also a risk: CHILDREN/TEENAGERS could easily come in contact with malicious or potentially dangerous people that profit from the anonymity granted by the username; they could be actors/victims of bullying, sexting or malicious actions. In this case it can be useful to block or monitor the access to applications/protocols that allow for: chatting and sending instant messaging or email to specific contacts – e.g. Skype, Live Messenger (Instant Messaging), email client (e.g. Outlook, Thunderbird) or webmail provider, (e.g. Yahoo!, Gmail).

Table 3 - EFFECTIVENESS NEEDS

Type of Need	Need Description
CONTENT	Different needs may emerge among parents in terms of topics to be filtered.
UNDERBLOCKING/ OVERBLOCKING	Each tool faces two problems: 1) blocking non-harmful pages (over-blocking); 2) allowing harmful pages (under-blocking). Parent may decide to give more importance to over-blocking or under-blocking. For instance, for a CHILD it can be preferable to ensure a good filtering of harmful content even if a lot of non-harmful content is blocked, while for a TEENAGER it could be preferable to give him/her a wider access to Internet even if more harmful content is not blocked.
AGE	According to the age (CHILDREN or TEENAGERS) different needs may emerge in terms of content to be filtered. Some tools may have a different effectiveness addressing such need.
LANGUAGE	The interface of the tool needs to be available in a language the parent is 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. While configuring the tool, parents should be aware of the kind of content that is mostly accessed by CHILDREN/TEENAGERS.

Table 4 - USABILITY NEEDS

Type of Need	Need Description
INSTALLATION	A short installation process, or no installation at all, options could be useful. PARENTS should be able to understand and manage the installation process (i.e. installation for beginners or for advanced users).
CONFIGURATION	PARENTS may be interested to set up different degrees of filtering or to transfer filter configuration between different users or devices. They may also have different sensibility on different types of content. The overall process should be comprehensible, conform with parents’ expectations and easy to learn.
USAGE	The alert message in case of blocking should be understandable for CHILDREN as well as for their parents. PARENTS might want to have an option to choose between different reactions in case the tool blocks a website. PARENTS might want that the tool support them in the education and help their CHILDREN understand why the parental control tool is in operation. Not all tools offer a reporting function. Nonetheless, reporting should be easy to handle and understand.

Table 5 - SECURITY NEEDS

Type of Need	Need Description
SECURITY	Tools may be by-passed or uninstalled. Today, this happens especially among TEENAGERS. Depending on the computer skills, parents may choose the tool according to its resistance to various type of violations, such as: o By-pass the tool accessing the prohibited pages by: using the IP address, proxy websites, online translation service (e.g., Google Translate), the Google Cache or other such services like the Internet Archive, an alternative browser. o By-pass the tool: changing the time settings (if time limit usage restriction is applied).

5. ELEMENTS ASSESSED DURING THE BENCHMARKING TESTS

- Two main different classes of age have been taken into consideration (≤12 years old and ≥13 years old)
- A functionality coverage has been measured considering the number of functionalities offered by each tool
- To support the users more appropriately in their decision making process a list of functionalities has been checked.
- Effectiveness has been measured with reference to: topic of the content, age, language, Web type, and social media used.
- The tools' effectiveness has been assessed in terms of their performance in blocking harmful content and allowing non-harmful content and measured against the following performance features:
  - **Sensitivity** – Under-blocking (% of missed bad content)
  - **Specificity** – Over-blocking (% of dropped good content)
- Usability has been measured considering installation and configuration processes and usage.
- Security: the tools have been tested to check if they prevent the user from by-passing or disabling the filter through a specific set of actions (e.g. using an alternative browser, disabling or uninstalling the software without a password, closing the filtering tool trough the Task Manager, accessing pages through the Google Cache, etc.).

6. OVERVIEW OF THE 4TH BENCHMARKING TESTING CYCLE RESULTS

Scoring method

The tests conducted in the 4th cycle on the 25 selected tools produced results for tools' performance against the four investigated areas: Functionality, Effectiveness, Usability and Security.

As for **Functionality**, SIP-BENCH III has not assigned an overall score to each tool as a final result, but checked the availability of a set of functionalities for each analysed tool. Therefore, for this performance area, given a set number of functionalities checked by SIP-BENCH III, for each tested tool it is indicated how many functionalities are covered by that specific tool. The information is provided in % of functionalities covered by the tool against the total number of functionalities tested. Results for this area of performance are presented in paragraphs 7.1., 8.1 and 9.1 of this report.

As for **Effectiveness**, **Usability** and **Security**, Table 6 below shows the 4th benchmarking cycle results. Tools are grouped per device used. The list is not a ranking. It just gives an overview of results obtained by testing the tools and **marks (in bold) the tool in each group that reached the highest score in each performance area.**

As regards the scoring, the following criteria have been applied for each performance area.

Effectiveness

The scope of the tests is to assess how effective is each tool in filtering harmful content. Each tool is scored with reference to both "adult" and "other harmful" content taking into account two different classes of age (≤12 years old and ≥13 years old).

An overall score is assigned to each age class as the result of the average performance of the two content topic types. The scoring scale considers both the **under blocking** (harmful pages which are not blocked) and **over blocking** (non-harmful pages which are blocked).

The overall score ranges from 0 (Very weak) to 4 (Excellent) as it follows:

- 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 level of filtering, nonetheless a non-small part of the content is not correctly filtered
- 3 = Good: the tool offers a good level of filtering, but part of the content is not correctly filtered.
- 4 = Excellent: the tool offers a very good level of filtering and satisfies the parents' needs in terms of effectiveness.

Usability

Results refer to three different processes: Installation (I), Configuration/Re-configuration (C) and Usage (U). For each process a set of criteria was applied to the tool. The scores are scaled from 0 (worst performance) to 4 points (best performance).

Security

Security is measured in terms of capacity of the tool to prevent the user from by-passing or disabling the filter through a specific set of actions. The assessment has been carried out through a binary model: 'Yes' the tool prevents the user from by-passing; 'No' the tool does not prevent the user from by-passing. The score is assigned to the tool according to the issues raised while testing:

0 = Issues making the tool easily non operative

1 = Critical or severe issues

2 = Issues requiring some computer skills

3 = Minor issues

4 = No issues identified

Table 6 – PERFORMANCE OVERVIEW OF PARENTAL CONTROL TOOLS FOR PERSONAL COMPUTERS AND MOBILE DEVICES

Device	Tool Name	Effectiveness		Usability	Security
		≤12	≥13		
PC / MAC	ContentBarrier X9	1.8	1.8	2.84	1
	F-Secure Internet Security	2.2	2.2	2.67	1
	Kaspersky Safe Kids	2.0	2.0	3.03	1
	Mac Os X Parental Controls[1]	1.8	1.8	3.03	**4**
	McAfee Total Protection	2.0	2.0	2.90	1
	Netintelligence Online Child Safety	2.2	2.1	2.63	1
	Norton Family Premier	2.1	2.0	**3.52**	1
	Panda Global Protection (2016)	1.6	1.6	2.47	1
	Qustodio_Qustodio Premium	**2.3**	**2.3**	2.91	1
	Witigo Parental Filter	1.7	1.5	2.43	1
Mobile	Curbi	1.7	1.7	2.13	1
	Familoop	1.9	1.9	2.57	1
	F-Secure Mobile Security	2.2	2.2	2.51	1
	Mobicip Safe Browser	2.0	2.0	2.51	**4**
	Norton Family parental control	**2.4**	**2.4**	**2.90**	1
	Parentsaround (mobile)	1.6	1.6	2.69	1
	Qustodio (mobile)	1.8	1.8	2.87	1
	Surfie Kids	2.5	2.5	2.86	1
	WebProtectMe Safe Browser	2.1	2.1	3.04	1
	Xooloo (mobile)	n/a	n/a	2.21	**4**
Alternative Tools	JumpTo Secure Kids	**2.5**	**2.5**	1.20	**4**
	Magic Desktop	**2.5**	**2.5**	**2.10**	**4**
	Maxthon Kid-Safe Browser	n/a	n/a	1.60	**4**
	Surfgarten	n/a	n/a	**2.10**	**4**
	Zoodles Premium	n/a	n/a	**2.10**	2

[1] The same system is implemented in iOS (iPad, iPhone).

Summary of the main findings of the 4th benchmarking cycle

- **A single perfect tool does not exist**: each PARENT should look for the tool that best matches with his/her needs and that adequately balance the areas of performance.
- Test results on the four areas of **performance vary substantially** among the different tools, even within the same device category.
- **None** of the 25 tested tools **scores better in two or more areas of performance** against the other tools.
- Not **any** of the tested tools reaches the **complete functionality** tested. The highest coverage percentage is 67 % for PC tools, 60 % for Mobile tools and only 43 % for Alternative tools. To make a suitable selection of the tool addressing specific needs, it would be useful to check all the functionalities offered and the related results achieved with the tests. Through the YES/NO list provided in the overview tables it is possible to check how many functionalities each tool is able to offer or how many tools offer a specific functionality.
- Some functionalities are embedded in the operating system (iOS for example).
- The overall **effectiveness**, in general, is **low**. Over blocking and under blocking rates perform oppositely: tools with a low over blocking rate have a high under blocking rate where, in principle, the lower the level of both under-blocking/over-blocking, the better is the tool.
- The **adult content** is better filtered than the other categories. It is the most common category included by default in each tested tool.
- **User-generated content** (Social Media and Web 2.0) is very badly filtered by almost all tools with traditional techniques (black list and URL filtering) since it is provided on an encoded basis, it is difficult to categorise and it is not always included in the black lists.
- **English** is the language the tools work better with.
- Not all the tools tested provide filtering settings in according to the age and the sex of the child. This explains why **Effectiveness** among the two **classes of age** is quite **similar**.
- **Security scores** almost **the same** for PC and mobile devices tools. Higher scores are registered for Alternative tools, and this is obvious given the nature of these tools working as a ‘protected’ environment.
- **Usability** scores are **higher** for **PC and mobile tools** than for Alternative tools.

7. PARENTAL CONTROL TOOLS FOR PERSONAL COMPUTERS

FINDINGS FOR
FUNCTIONALITY, EFFECTIVENESS, USABILITY AND SECURITY

PCs and the Internet

The PCs are still a common way to access the Internet, even if mobile devices are overtaking in terms of usage in particular among youngsters. PCs allow CHILDREN/TEENAGERS to access Web pages, share experiences and contents through social networks and communicate with people.

7.1. PC PARENTAL CONTROL TOOLS FUNCTIONALITY: key findings

The table below shows an overview of the tests performed on FUNCTIONALITY of PC TOOLS

Table 7 – OVERVIEW FOR FUNCTIONALITY RESULTS OF PC TOOLS

TOOL	% FUNCTION COVERAGE
ContentBarrier X9	**67 %**
Norton Family Premier	**57 %**
Kaspersky Safe Kids	**53 %**
Qustodio_Qustodio Premium	**50 %**
Mac Os X Parental Controls	47 %
Netintelligence Online Child Safety	47 %
McAfee Total Protection	40 %
F-Secure Internet Security	37 %
Witigo Parental Filter	37 %
Panda Global Protection (2016)	33 %

- **None** of the 10 tested tools reaches the **complete functionality** tested in SIP Bench III. It is not possible for a tool to gain 100 % functionality coverage due to contradicting functionalities (either/or-decision). PARENTS should check the list of functionalities as displayed in the functionality tables in order to find tools that best fit their individual functionality needs.
- The **most complete tool covers 67 %**.
- The PC tools tested in the 4th cycle provide a **broader range of functionalities** than tools tested in previous cycles. The functionality coverage is also higher than the one resulting for tested tools for mobile devices.
- The **highest scoring products** are:
  - Content Barrier X9 (67 %)
  - Norton Family Premier (57 %)
  - Kaspersky Safe Kids (53 %)
  - QUSTODIO_Qustodio Premium (50 %)
- All **other products** score **less than 50 %** functionality coverage.

Table 8 and 9 below show in more detail the functionality coverage of the 10 tested PC tools.

Table 8 – TESTS DETAILED RESULTS FOR FUNCTIONALITY OF PC TOOLS (1)

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
ContentBarrier X9	Y	Y	N	N	N	Y	N	Y	N	Y	N	Y	Y	Y	N	Y
F-Secure Internet Security	N	N	N	N	Y	N	N	Y	N	N	N	Y	N	N	N	N
Kaspersky Safe Kids	Y	Y	N	N	Y	Y	Y	Y	N	N	N	Y	Y	N	N	N
Mac Os X Parental Controls	Y	N	N	N	N	Y	Y	N	N	N	N	Y	Y	N	N	N
McAfee Total Protection	Y	Y	N	N	N	N	N	Y	N	Y	N	Y	N	N	N	N
Netintelligence Online Child Safety	Y	Y	N	N	N	N	N	Y	N	N	N	Y	Y	N	N	N
Norton Family Premier	Y	N	N	Y	Y	N	N	Y	Y	Y	N	Y	Y	N	N	N
Panda Global Protection (2016)	Y	Y	N	N	Y	N	N	Y	N	N	N	Y	Y	N	N	N
Qustodio_Qustodio Premium	Y	N	N	N	Y	N	N	Y	Y	N	N	Y	Y	N	N	N
Witigo Parental Filter	Y	N	N	N	Y	N	N	Y	N	N	N	Y	N	N	N	N
% of tools with function	90 %	50 %	0 %	10 %	60 %	30 %	20 %	90 %	20 %	30 %	0 %	100 %	70 %	10 %	0 %	10 %

Table 9 – TESTS RESULTS FOR FUNCTIONALITY OF PC TOOLS (2)

Area of need	Management			Filtering Customisation					Keywords			Time	Blocking Message		% function coverage
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	
ContentBarrier X9	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y	67 %
F-Secure Internet Security	Y	N	N	Y	Y	N	Y	Y	Y	Y	N	Y	N	N	37 %
Kaspersky Safe Kids	Y	Y	Y	Y	Y	N	Y	N	N	N	N	Y	N	Y	53 %
Mac Os X Parental Controls	Y	N	Y	N	Y	Y	Y	Y	N	N	N	Y	Y	Y	47 %
McAfee Total Protection	Y	N	Y	Y	Y	N	Y	N	N	N	N	Y	N	Y	40 %
Netintelligence Online Child Safety	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y	N	N	47 %
Norton Family Premier	Y	Y	Y	Y	Y	N	Y	N	N	N	N	Y	Y	Y	57 %
Panda Global Protection (2016)	Y	N	N	Y	Y	N	Y	N	N	N	N	N	N	N	33 %
Qustodio_Qustodio Premium	Y	Y	Y	Y	Y	N	Y	Y	N	N	N	Y	N	Y	50 %
Witigo Parental Filter	Y	Y	Y	N	Y	N	Y	N	N	N	N	Y	Y	N	37 %
% of tools with function	100 %	50 %	80 %	80 %	100 %	30 %	100 %	50 %	20 %	10 %	0 %	90 %	40 %	60 %	

In the table below the main findings on specific issues of functionality are summarised.

Table 10 – MAIN FINDINGS ON FUNCTIONALITY OF PC TOOLS

Area of Functionality	Findings
Customisation of Web content filtering	▪ Most of the tools provide PARENTS with the complete set of customisation functionalities (topic and URL black/white lists). ▪ Keywords filtering (filtering by words or content categorised as inappropriate) is uncommon: only two tools offer this option. ▪ Nine tools give the possibility to block access to social networks; only two tools allow PARENTS to monitor social network usage. ▪ Six tools give the possibility to force the user to use the Safe Search functionality of the most common search engines, which however provides only a limited protection (e.g.: deny access to google translate, google cache).
Filtering Topics	▪ There are eight tools that are able to filter web content via topics.
Protocols and Applications	▪ The tools rarely provide the option to block an entire protocol whereas blocking applications are more common.
Management of users' profiles	▪ All tools enable the PARENT to create and manage different profiles for users with different needs.
Remote Management	▪ Remote Management is possible in eight tools. For some tools (Norton and Qustodio for example) it is possible to manage both the PC tool and the mobile tool (provided that both are installed and used). In this case user profiles can be transferred between devices.
Restricting Web access	▪ All tools enable PARENTS to block the access specifically to the Internet (whether using a specific functionality or using the "time restrictions").
Streaming	▪ Only three tools block web-based streaming as a functionality. If this specific option is not available, sites that offer streaming can at least be added to a black list.
Communication activities	▪ One tool is able to block Windows Live Messenger and three are able to block Skype. If tools are able to block Skype and/or MSN, they block it to the whole application and it is not possible to limit the blocking to Voice Over IP (VoIP) or Video chat only.
Monitoring	▪ Most of the tools are able to provide the PARENT with at least a basic report on the user's web activity (visited websites or violations). ▪ Five tools allow remote access to monitoring and eight tools allow remote management on various devices.
Language Interface	▪ English is the most frequent language, whereas the choice of tools is limited for many other European languages.

7.2. PC PARENTAL CONTROL TOOLS EFFECTIVENESS: key findings

Table 11 – PC TOOLS EFFECTIVENESS RESULTS: score view

TOOL	Overall Score	
	≤ 12	≥ 13
ContentBarrier X9	1.8	1.8
F-Secure Internet Security	2.2	2.2
Kaspersky Safe Kids	2	2
Mac Os X Parental Controls	1.8	1.8
McAfee Total Protection	2	2
Netintelligence Online Child Safety	2.2	2.1
Norton Family Premier	2.1	2
Panda Global Protection (2016)	1.6	1.6
Qustodio_Qustodio Premium	**2.3**	**2.3**
Witigo Parental Filter	1.7	1.5

How to read the table

The table shows how effective the tools are in filtering harmful content. Each tool is scored with reference to both "adult" and "other harmful" content (drugs, violence, racism, etc.) taking into account two different classes of age (≤12 years old and ≥13 years old).

An overall score is assigned to each age class as **the result of the average performance of the two content topic types.** The scoring scale considers both the under blocking (harmful pages which are not blocked) and over blocking (non-harmful pages which are blocked).

Effectiveness Score. The overall score ranges from 0 to 4. The scores provide measurement as it follows:

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 level of filtering, nonetheless a non-small part of the content is not correctly filtered

3 = Good: the tool offers a good level of filtering, but part of the content is not correctly filtered.

4 = Excellent: the tool offers a very good level of filtering and satisfies the parents' needs in terms of effectiveness.

Note: The overall effectiveness score provides only a synthetic view of the tests results. Before choosing one tool, it would be useful to check all the functionalities tested and the results (over blocking, under blocking, etc.), to select the tools which better address the specific needs.

Table 12 - EFFECTIVENESS OF PC TOOLS RELATED TO TOPIC (OVERBLOCKING/UNDERBLOCKING)

TOOL	Adult content		Violence and Crime		Racist		Drugs & Self-Damage		Gambling	
	over blocking	under blocking	over blocking	under blocking	over blocking	under blocking	Over blocking	under blocking	over blocking	under blocking
ContentBarrier X9	27 %	34 %	7 %	61 %	12 %	47 %	17 %	47 %	28 %	34 %
F-Secure Internet Security	10 %	25 %	4 %	54 %	6 %	52 %	15 %	35 %	16 %	24 %
Kaspersky Safe Kids	5 %	64 %	3 %	67 %	4 %	66 %	4 %	62 %	7 %	61 %
Mac Os X Parental Controls	23 %	38 %	6 %	61 %	6 %	64 %	12 %	61 %	9 %	68 %
McAfee Total Protection	4 %	50 %	1 %	62 %	1 %	65 %	2 %	54 %	8 %	51 %
Netintelligence Online Child Safety	9 %	27 %	4 %	63 %	7 %	59 %	9 %	50 %	13 %	36 %
Norton Family Premier	11 %	18 %	15 %	57 %	12 %	51 %	10 %	37 %	19 %	21 %
Panda Global Protection (2016)	26 %	22 %	26 %	45 %	22 %	44 %	35 %	27 %	34 %	24 %
Qustodio_Qustodio Premium	5 %	34 %	1 %	68 %	1 %	67 %	6 %	46 %	18 %	28 %
Witigo Parental Filter	28 %	24 %	20 %	44 %	18 %	44 %	23 %	33 %	21 %	30 %

How to read the table

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

Over blocking occurs when the tool blocks non-harmful content.

Under blocking occurs when the tool allows harmful content.

PARENTS can verify how effective is each tool against the categories they assume are the most threatening for their CHILDREN/TEENAGERS.

Results are provided in % of over blocked or under blocked content.

An effective tool has a low over blocking and a low under blocking. The lower the level of both under blocking and over blocking, the better the tool is.

Table 13 - EFFECTIVENESS OF PC TOOLS RELATED TO LANGUAGE

TOOL	English		German		Italian		Spanish		French		Polish	
	over blocking	under blocking	over blocking	under blocking	over blocking	under blocking	over blocking	under blocking	over blocking	under blocking	over blocking	under blocking
ContentBarrier X9	27 %	44 %	19 %	41 %	12 %	41 %	28 %	45 %	27 %	32 %	10 %	39 %
F-Secure Internet Security	12 %	28 %	13 %	34 %	10 %	40 %	9 %	40 %	9 %	32 %	6 %	39 %
Kaspersky Safe Kids	4 %	68 %	13 %	60 %	1 %	61 %	5 %	64 %	5 %	58 %	1 %	64 %
Mac Os X Parental Controls	11 %	60 %	8 %	54 %	24 %	45 %	24 %	49 %	17 %	47 %	7 %	48 %
McAfee Total Protection	3 %	58 %	4 %	54 %	8 %	56 %	3 %	55 %	4 %	48 %	1 %	52 %
Netintelligence Online Child Safety	10 %	35 %	12 %	46 %	4 %	44 %	7 %	48 %	13 %	39 %	3 %	45 %
Norton Family Premier	11 %	28 %	13 %	31 %	19 %	40 %	15 %	34 %	9 %	30 %	14 %	30 %
Panda Global Protection (2016)	31 %	28 %	32 %	31 %	29 %	30 %	26 %	35 %	28 %	27 %	21 %	28 %
Qustodio_Qustodio Premium	5 %	45 %	10 %	46 %	7 %	44 %	6 %	48 %	6 %	41 %	3 %	41 %
Witigo Parental Filter	19 %	33 %	27 %	31 %	19 %	40 %	27 %	40 %	24 %	29 %	29 %	18 %

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 the language/s of interest. Results are provided as % of over blocked or under blocked content.

Table 14 - EFFECTIVENESS OF PC TOOLS RELATED TO AGE

TOOL	≤ 12		≥ 13	
	over blocking	under blocking	over blocking	under blocking
ContentBarrier X9	22 %	42 %	22 %	41 %
F-Secure Internet Security	10 %	35 %	11 %	34 %
Kaspersky Safe Kids	5 %	65 %	5 %	64 %
Mac Os X Parental Controls	15 %	54 %	16 %	53 %
McAfee Total Protection	4 %	56 %	4 %	55 %
Netintelligence Online Child Safety	9 %	42 %	9 %	41 %
Norton Family Premier	13 %	32 %	14 %	31 %
Panda Global Protection (2016)	28 %	30 %	29 %	29 %
Qustodio_Qustodio Premium	6 %	46 %	6 %	44 %
Witigo Parental Filter	24 %	33 %	26 %	32 %

How to read the table

The table shows how effective the tools are with respect to the age of the CHILDREN/TEENAGERS.

Each tool has been configured for each class of age and tested.

Results are provided in % of over blocked or under blocked content.

Table 15 - EFFECTIVENESS OF PC TOOLS RELATED TO WEB TYPE: WEB/WEB 2.0

Topic	Web (websites pages)		Web 2.0 (blogs, forums)	
	over blocking	under blocking	over blocking	under blocking
ContentBarrier X9	22 %	37 %	20 %	50 %
F-Secure Internet Security	11 %	27 %	10 %	47 %
Kaspersky Safe Kids	3 %	63 %	9 %	66 %
Mac Os X Parental Controls	14 %	52 %	16 %	55 %
McAfee Total Protection	4 %	50 %	2 %	63 %
Netintelligence Online Child Safety	7 %	36 %	11 %	50 %
Norton Family Premier	16 %	25 %	7 %	43 %
Panda Global Protection (2016)	30 %	24 %	24 %	38 %
Qustodio_Qustodio Premium	6 %	37 %	6 %	57 %
Witigo Parental Filter	26 %	27 %	20 %	42 %

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 (websites pages) or Web 2.0 (blogs, forums).

In this table Web 2.0 does not include user-generated content on social network (which is instead included in Table 16 below), but includes user generated content and media on personal blogs or webpages.

The tools have been tested both on traditional Web content and user generated content or web 2.0.

PARENTS can verify how effective each tool is, according to the type of content mostly accessed by their CHILDREN/TEENAGERS in blocking harmful/bad content.

Results are provided in % of over blocked or under blocked content.

Table 16 - EFFECTIVENESS OF PC TOOLS RELATED TO SOCIAL MEDIA

TOOL	Tumblr	YouTube	Vine	Pinterest	Twitter	Facebook
ContentBarrier X9	100 %	99 %	100 %	99 %	91.7 %	80.6 %
F-Secure Internet Security	100 %	99 %	100 %	99 %	83.4 %	77.4 %
Kaspersky Safe Kids	100 %	99 %	100 %	99 %	91.7 %	80.6 %
Mac Os X Parental Controls	100 %	99 %	100 %	99 %	91.7 %	80.6 %
McAfee Total Protection	100 %	99 %	100 %	100 %	91.7 %	80.6 %
Netintelligence Online Child Safety	100 %	99 %	100 %	99 %	91.7 %	67.7 %
Norton Family Premier	100 %	99 %	100 %	99 %	91.7 %	71 .0%
Panda Global Protection (2016)	100 %	99 %	100 %	99 %	91.7 %	80.6 %
Qustodio_Qustodio Premium	100 %	99 %	100 %	99 %	91.7 %	71.0 %
Witigo Parental Filter	100 %	99 %	100 %	100 %	9.7 %	67.7 %

How to read the table

The table shows how effective the tools are in terms of their operation with the main social media platforms.

PARENTS can verify how effective each tool is with content exchanged in each of the six most accessed and popular social media platforms.

Results are provided in % of under-blocked content.

Table 17 – EFFECTIVENESS KEY FINDINGS

Topic	The over blocking rate is below the 30 % in almost all cases, but the under blocking rate is higher than 30 % for almost all tested tools. In general, effectiveness is low. Over blocking and under blocking rates, in fact, perform oppositely: tools with a low over blocking rate have on the contrary a high under blocking rate. It might be assumed that the tools rely mainly on black lists and keywords URL analysis, and are limited by these techniques. In particular the difficulty in analysing user-generated content. Less than 20 % of the data test set used belongs to the existing black lists and the data test set consists of 4,000 items. This may explain why effectiveness results may be lower than the ones proposed by other similar tests. The adult content is better filtered than the "other" content categories. On adult content some tools achieve an over blocking lower than 10 %. On the "other" content categories (except gambling) only a few tools have an under blocking close to 30 %. Most of them have very low effectiveness (more than 50 % of under blocking).
Age classes	The tools perform quite similarly with a configuration for the two age classes (≤12 and ≥ 13). This can be ascribed to the fact that many tools do not give a real possibility to create personalised profiles according to the age.
Web and Web 2.0	The tools present lower effectiveness on Web 2.0 content. In particular, the tools which achieve better results show generally a higher discrepancy between the under-blocking rate on Web and Web 2.0. It is an indicator of the difficulties of the tools to deal with user-generated and Web 2.0 content. The web 2.0 is more difficult to filter for several reasons: (i) the content is produced mainly by users and not by identified entities (like companies, institutions, etc.); (ii) on the website the content is published by different users and this implies that the content varies according to the user (e.g. on Facebook); (iii) the content changes very quickly (e.g. a web page that is not harmful could become harmful because of uploaded images). In this sense, the traditional blacklist filtering is not enough fast with respect to the quick and numerous content changes. Furthermore, most social media services provide their content on an encoded basis (HTTPS). Filtering of individual content via deep links (like profiles or single videos) is not possible, since the deep link URLs are encoded themselves and usually not readable by filters.

7.3. PC PARENTAL CONTROL TOOLS USABILITY: key findings

Table 18 – OVERVIEW FOR USABILITY RESULTS OF PC TOOLS

TOOL	Content Barrier X9	F-Secure Internet Security	Kaspersky Safe Kids	Mac Os X Parental Controls	McAfee Total Protection	Netintelligence Online Child Safety	Norton Family Premier	Panda Global Protection (2016)	Qustodio_ Qustodio Premium	Witigo Parental Filter
I	2,62	3	3,3	n/a	2,84	1,9	3,52	2,98	2,73	1,44
C	3,26	2,68	3,27	3,3	3,12	3,14	3,57	2,77	3,11	2,79
U	2,29	2,42	2,47	2,58	2,59	2,28	3,42	1,61	2,71	2,49
overall	2,84	2,67	**3,03**	**3,03**	2,90	2,63	**3,52**	2,47	2,91	2,43

- The overall score for the PC tools range between 2.43 and 3.52.
- None of the tools score less than 2 points, thus not reaching the threshold of 50 % of 4 possible points, two tools range between 2 and 2.50, and five tools from 2.50 up to 3.
- Three tools (**Norton Family Premier, Kaspersky Safe Kids, Mac Os X Parental Controls**) score in the top area and gain 3 points or more.
- Nine out of ten tools gain better scores for installation and/or configuration than for usage.

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 tool. The detailed test results are available in individual tool fiches and in a both database available online.

I = Installation

C = Configuration /Reconfiguration

U = Usage

Table 19 – MAIN FINDINGS ON USABILITY OF PC TOOLS

Area of Usability	Findings
General findings	Some of the tools keep the installation procedures very simple. The configuration process varies greatly for the different tools. However, possibilities to customise the tool to one's own needs are generally poor. Some tools have very extended options to configure the software but then the risk of unwanted configuration effects and bad filtering results is high. Only a few tools provide additional information about filtering in general and about limitations and restrictions of the filtering procedures.
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 devices. Some tools merge the installation and first configuration steps into one single process.
Findings on the configuration process	The configuration process is crucial for the tool because of its relevance for an effective use of the filter. Most tools offer the possibility of an initial (default) configuration, which can later be adjusted. Some tools offer a configuration that comprises a lot of functionalities and can therefore be exhaustive. A number of products compensate complexity by good explanations and a well-structured user interface. The range of customisation options is broad. For some tools, only one degree of strength of filtering for all content categories is allowed, while for others the strength of filtering between different content categories can be differentiated. 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 specifically address the alert message to CHILDREN/TEENAGERS but rather to adults. Some tools offer an appropriate reaction to the alert message for a blocked web site, for example the redirection to safe resources or the possibility to ask for unblocking. Monitoring and reporting functionalities were tested as usage of the tools where applicable. Reporting ranges from mere long file data to detailed and colourful diagrams.

7.4. PC PARENTAL CONTROL TOOLS SECURITY: key findings

Table 20 – TESTS RESULTS OVERVIEW FOR SECURITY OF PC TOOLS

TOOL	SCORE	SECURITY ISSUES	MITIGATION
ContentBarrier X9	1	Access to harmful content through Google translate	Black list google translate website
F-Secure Internet Security	1	Access to harmful content through Google translate, and web cache sites. Uninstalled without asking credentials or pin	Black list google translate website and the web cache sites Restrict access on Windows Control panel
Kaspersky Safe Kids	1	Access to harmful content through Google translate	Black list google translate website
Mac Os X Parental Controls	**4**	No major issues	
McAfee Total Protection	1	Access to harmful content through Google translate Uninstalled without asking credentials or pin	Black list google translate website. Restrict access on Windows Control panel
Netintelligence Online Child Safety	1	Access to harmful content through Google translate, and web cache sites. Uninstalled without asking credentials or pin	Black list google translate website and the web cache sites Restrict access on Windows Control panel
Norton Family Premier	1	Access to harmful content through web cache sites. Does not filters pages inside an iframe	Black list web cache sites. No mitigation for iframe problem.
Panda Global Protection (2016)	1	Access to harmful content through Google translate site Uninstalled without asking credentials or pin	Black list google translate website Restrict access on Windows Control panel
Qustodio_Qustodio Premium	1	Access to harmful content through Google translate	Black list google translate website
Witigo Parental Filter	1	Access to harmful content through Google translate	Black list google translate website

How to read the table

Security is measured in terms of capacity of the tool to prevent the user from by-passing or disabling the filter through a specific set of actions. The assessment has been carried out through a binary model: (Yes) the tool prevents the user from by-passing; (No) the tool does not prevent the user from by-passing.

The score is assigned to the tool according to the issues raised while testing:

0 = Issues making the tool easily non operative

1 = Critical or severe issues

2 = Issues requiring some computer skills

3 = Minor issues

4 = No issues identified

For each tool, major issues identified are briefly indicated in the third column, while potential actions are suggested to mitigate security issues in the fourth column.

8. PARENTAL CONTROL TOOLS FOR MOBILE DEVICES

FINDINGS FOR
FUNCTIONALITY, EFFECTIVENESS, USABILITY AND SECURITY

Mobile phones and the Internet

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

8.1. MOBILE PHONES PARENTAL CONTROL TOOLS FUNCTIONALITY: key findings

The table below shows an overview of the tests performed on FUNCTIONALITY of tools for MOBILE DEVICES

Table 21 – OVERVIEW FOR FUNCTIONALITY RESULTS OF MOBILE TOOLS

TOOL	% of FUNCTION COVERED
Surfie Kids	**60 %**
Qustodio (Mobile)	**57 %**
Norton Family parental control	**50 %**
Parentsaround (Mobile)	43 %
Familoop	40 %
F-Secure Mobile Security	30 %
WebProtectMe Safe Browser	37 %
Curbi	27 %
Xooloo parental control (Mobile)	23 %
Mobicip Safe Browser	17 %

- None of the ten tested tools reaches the complete functionality tested in SIP Bench III. It is not possible for a tool to gain 100% functionality coverage due to contradicting functionalities (either/or-decision). PARENTS should check the list of functionalities as displayed in the functionality tables in order to find tools that best fit their individual functionality needs.
- The **most complete** one covers **60 %**. However, the mobile tools tested in the 4th cycle provide a broader range of functionalities than previously tested tools. Over the years, in fact, mobile tools have integrated more functionalities.
- **The highest scoring tools are:**
  - Surfie Kids (60 %)
  - Qustodio Mobile (57 %)
  - Norton Family parental control (50 %)
- All **other products** score **less than 50 %** functionality coverage.

Table 22 – TESTS DETAILED RESULTS FOR FUNCTIONALITY OF MOBILE TOOLS (1)

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
curbi	Y	N	N	N	Y	N	N	Y	N	N	N	Y	N	N	N	N
Familoop	Y	N	N	N	Y	N	N	N	N	N	N	Y	Y	N	N	N
F-Secure Mobile Security	Y	N	N	N	Y	Y	N	Y	N	N	N	Y	N	N	N	N
Mobicip Safe Browser	N	N	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N
Norton Family parental control	Y	N	N	Y	Y	Y	Y	Y	Y	N	N	Y	Y	N	N	N
Parentsaround (Mobile)	Y	N	N	N	Y	Y	Y	N	N	N	N	Y	Y	N	N	N
Qustodio (Mobile)	Y	N	N	N	Y	Y	Y	Y	Y	N	N	Y	Y	N	N	N
Surfie Kids	Y	Y	Y	N	Y	Y	N	Y	Y	N	N	Y	Y	N	N	N
WebProtectMe Safe Browser	Y	N	N	N	Y	N	N	Y	N	N	N	Y	N	N	N	N
Xooloo (Mobile)	Y	N	N	N	N	Y	Y	N	N	N	N	N	N	N	N	N
% of tools with function	90 %	10 %	10 %	10 %	90 %	60 %	40 %	60 %	30 %	0 %	0 %	90 %	50 %	0 %	0 %	0 %

Table 23 – Tests detailed results for FUNCTIONALITY of MOBILE TOOLS (2)

Area of need	Management			Filtering Customisation					Keywords			Time	Blocking Message		% function coverage
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	
curbi	N	Y	Y	N	Y	N	N	N	N	N	N	Y	N	N	27 %
Familoop	Y	Y	Y	N	Y	N	Y	N	N	N	N	Y	Y	Y	40 %
F-Secure Mobile Security	N	N	N	Y	N	N	N	N	N	N	N	Y	Y	Y	30 %
Mobicip Safe Browser	Y	N	Y	N	N	N	N	N	N	N	N	N	Y	N	17 %
Norton Family parental control	Y	Y	Y	N	Y	N	Y	N	N	N	N	Y	N	N	50 %
Parentsaround (Mobile)	Y	Y	Y	N	Y	N	N	N	N	N	N	Y	Y	Y	43 %
Qustodio (Mobile)	Y	Y	Y	Y	Y	N	Y	Y	N	N	N	Y	N	Y	57 %
Surfie Kids	Y	Y	Y	Y	Y	N	Y	Y	N	N	N	Y	N	Y	60 %
WebProtectMe Safe Browser	N	Y	Y	N	Y	Y	Y	N	Y	Y	N	N	N	N	37 %
Xooloo (Mobile)	Y	N	N	N	Y	Y	N	N	N	N	N	Y	N	N	23 %
% of tools with function	70 %	70 %	80 %	30 %	80 %	20 %	50 %	20 %	10 %	10 %	0 %	80 %	40 %	50 %	

In the table below the main findings on specific issues of functionality are summarised.

Table 24 – Main findings on FUNCTIONALITY of MOBILE TOOLS

Area of Functionality	Findings
Customisation of Web content filtering	▪ Most of the tools allow PARENTS to create their own blacklist. Only three tools allow the customisation of filtering topics. ▪ Keywords filtering is very uncommon: only one tool offers this option. ▪ Six tools give the possibility to block access completely to social networks; only three tools allow the PARENTS to monitor social network usage. ▪ Most tools give the possibility to force the user to use the Safe Search functionality of the most common search engines.
Filtering Topics	▪ There are fewer tools for mobile devices than tools for PC able to filter web content via topics. Only three mobile tools offer this option.
Protocols and Applications	▪ The tools rarely provide the option to block an entire protocol whereas blocking applications are more common.
Management of users' profiles	▪ Seven tools enable PARENTS to create and manage different profiles for users with different needs.
Remote Management	▪ Remote Management is possible for eight tools. For some tools – Norton and Qustodio for example - it is possible to manage both the mobile tool and the PC tool (provided that both are installed and used). In this case user profiles can be transferred between devices.
Restricting Web access	▪ All tools enable PARENTS to block the access specifically to the Internet (whether using a specific functionality or using the "time restrictions").
Streaming	▪ None of the tools block web-based streaming. If this specific option is not available, sites that offer streaming can at least be added to a black list or streaming Apps can be blocked.
Communication activities	▪ Five tools are able to block Skype chat and only three tools block video chat.
Monitoring	▪ Most of the tools are able to provide PARENTS with at least a basic report on the user's web activity (visited websites or violations). Seven tools allow remote access to monitoring and eight tools allow remote management on various devices.
Language Interface	▪ English is the most frequent language, whereas the choice of tools is limited for many other European languages.

8.2. MOBILE PHONES PARENTAL CONTROL TOOLS EFFECTIVENESS: key findings

Table 25 – MOBILE TOOLS EFFECTIVENESS RESULTS: score view

TOOL	Overall Score	
	≤ 12	≥ 13
curbi	1.7	1.7
Familoop	1.9	1.9
F-Secure Mobile Security	2.2	2.2
Mobicip Safe Browser	2	2
Norton Family parental control	**2.4**	**2.4**
Parentsaround (Mobile)	1.6	1.6
Qustodio (Mobile)	1.8	1.8
Surfie Kids	**2.5**	**2.5**
WebProtectMe Safe Browser	2.1	2.1
Xooloo (Mobile)[2]	n/a (*)	n/a

How to read the table

The table shows how effective the tools are in filtering harmful content. The tool is scored with reference both to the "adult" and to "other harmful" content (drugs, violence, racism, etc.) taking into account two different classes of age (≤12 years old and ≥13 years old). An overall score is assigned to each age class as the result of the average performance of the two types of content. The scoring scale considers both the over blocking (non-harmful pages which are blocked) and under blocking (harmful pages which are not blocked).

(*) At the start of the 4th benchmarking cycle 'Xooloo' was included in the list of tested tools as a mobile tool. During the testing phase, however, the mobile tool version has been deprecated, so it was not possible to test it anymore for the specific purpose here indicated. The Alternative tool version works in a "walled garden" environment and the measurement of effectiveness, in this case, is not significant.

Effectiveness Score. The overall score ranges from 0 to 4 as it follows:

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 level of filtering, nonetheless a non-small part of the content is not correctly filtered

3 = Good: the tool offers a good level of filtering, but part of the content is not correctly filtered.

4 = Excellent: the tool offers a very good level of filtering and satisfies the parents' needs in terms of effectiveness.

[2] Xooloo has been tested in both versions: as tool for mobile devices (cycles 3 and 4) and Alternative tool cycle 3). The two versions of the tools work differently.

Table 26 - EFFECTIVENESS of MOBILE TOOLS RELATED TO TOPIC (OVERBLOCKING/UNDERBLOCKING)

TOOL	Adult content		Violence and Crime		Racist		Drugs & Self-Damage		Gambling	
	over blocking	under blocking	over blocking	under blocking	over blocking	under blocking	over blocking	under blocking	over blocking	under blocking
Curbi	17 %	20 %	12 %	53 %	18 %	51 %	18 %	58 %	15 %	55 %
Familoop	11 %	39 %	8 %	62 %	8 %	63 %	8 %	59 %	10 %	59 %
F-Secure Mobile Security	9 %	27 %	6 %	57 %	3 %	53 %	12 %	41 %	14 %	31 %
Mobicip Safe Browser	13 %	36 %	2 %	68 %	1 %	69 %	1 %	67 %	1 %	72 %
Norton Family parental control	15 %	8 %	18 %	53 %	16 %	42 %	13 %	27 %	22 %	15 %
Parentsaround (Mobile)	29 %	11 %	29 %	45 %	26 %	46 %	33 %	31 %	28 %	38 %
Qustodio (Mobile)	15 %	36 %	14 %	56 %	13 %	56 %	16 %	44 %	16 %	45 %
Surfie Kids	6 %	27 %	2 %	51 %	2 %	47 %	4 %	57 %	9 %	29 %
WebProtectMe Safe Browser	9 %	46 %	4 %	65 %	2 %	67 %	5 %	63 %	3 %	70 %
Xooloo (Mobile)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

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 against the categories they assume are the most threatening for their CHILDREN/TEENAGERS.

Results are provided in % of under blocked or over blocked content.

Table 27 - EFFECTIVENESS OF MOBILE TOOLS RELATED TO LANGUAGE

TOOL	English		German		Italian		Spanish		French		Polish	
	over blocking	under blocking	over blocking	under blocking	over blocking	under blocking	over blocking	under blocking	over blocking	under blocking	over blocking	under blocking
Curbi	17 %	38 %	12 %	46 %	12 %	43 %	15 %	40 %	23 %	31 %	11 %	44 %
Familoop	10 %	52 %	9 %	52 %	7 %	49 %	13 %	57 %	11 %	45 %	7 %	54 %
F-Secure Mobile Security	11 %	32 %	10 %	42 %	6 %	40 %	9 %	43 %	6 %	34 %	6 %	43 %
Mobicip Safe Browser	11 %	58 %	2 %	54 %	4 %	54 %	5 %	57 %	8 %	51 %	1 %	51 %
Norton Family parental control	13 %	18 %	16 %	25 %	19 %	24 %	16 %	28 %	12 %	24 %	17 %	27 %
Parentsaround (Mobile)	32 %	25 %	25 %	33 %	25 %	30 %	27 %	35 %	34 %	18 %	16 %	31 %
Qustodio (Mobile)	19 %	44 %	15 %	49 %	13 %	44 %	15 %	43 %	13 %	38 %	9 %	50 %
Surfie Kids	2 %	41 %	5 %	35 %	5 %	38 %	7 %	41 %	11 %	31 %	1 %	35 %
WebProtectMe Safe Browser	5 %	60 %	4 %	54 %	6 %	57 %	2 %	63 %	10 %	53 %	3 %	57 %
Xooloo (Mobile)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

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 the language/s of their interest.

Results are provided as % of over blocked or under blocked content.

Table 28 - EFFECTIVENESS OF MOBILE TOOLS RELATED TO AGE

TOOL	≤ 12		≥ 13	
	over blocking	under blocking	over blocking	under blocking
Curbi	16 %	41 %	16 %	40 %
Familoop	9 %	53 %	10 %	52 %
F-Secure Mobile Security	8 %	39 %	9 %	37 %
Mobicip Safe Browser	6 %	56 %	7 %	55 %
Norton Family parental control	15 %	24 %	16 %	23 %
Parentsaround (Mobile)	28 %	29 %	29 %	28 %
Qustodio (Mobile)	15 %	46 %	15 %	44 %
Surfie Kids	5 %	39 %	5 %	38 %
WebProtectMe Safe Browser	5 %	59 %	6 %	58 %
Xooloo (Mobile)	n/a	n/a	n/a	n/a

How to read the table

The table shows how effective the tools are with respect to the age of the CHILDREN/TEENAGERS.

Each tool has been configured for each category of age and tested.

Results are provided in % of over blocked or under blocked content.

Table 29 - EFFECTIVENESS OF MOBILE TOOLS RELATED TO WEB TYPE: WEB/WEB 2.0

Topic	Web (websites pages)		Web 2.0 (blogs, forums)	
	over blocking	under blocking	over blocking	under blocking
Curbi	13 %	40 %	20 %	39 %
Familoop	11 %	50 %	7 %	54 %
F-Secure Mobile Security	8 %	32 %	9 %	47 %
Mobicip Safe Browser	6 %	52 %	6 %	60 %
Norton Family parental control	17 %	16 %	11 %	34 %
Parentsaround (Mobile)	29 %	25 %	24 %	33 %
Qustodio (Mobile)	13 %	44 %	17 %	45 %
Surfie Kids	5 %	31 %	5 %	49 %
WebProtectMe Safe Browser	6 %	56 %	4 %	61 %
Xooloo (Mobile)	n/a	n/a	n/a	n/a

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, forums) and traditional Web content (websites pages).

Results do not refer to user-generated content exchanged on social networks, but user generated content and media on personal blogs or webpages. Tools' performance with the most popular social networks among youngsters is shown in the next Table 30.

PARENTS can verify how effective each tool is, according to the kind of content mostly accessed by their CHILDREN/TEENAGERS.

Results are provided in % of over blocked or under blocked content.

Table 30 - EFFECTIVENESS OF MOBILE TOOLS RELATED TO SOCIAL MEDIA

TOOL	Tumblr	YouTube	Vine	Pinterest	Twitter	Facebook
curbi	99 %	3.0 %	99 %	99 %	91.7 %	67.7 %
Familoop	100 %	99.0 %	100 %	99 %	91.7 %	77.4 %
F-Secure Mobile Security	100 %	99.0 %	100 %	99 %	83.3 %	77.4 %
Mobicip Safe Browser	100 %	99.0 %	100 %	100 %	9.7 %	80.6 %
Norton Family parental control	100 %	96.0 %	100 %	99 %	91.7 %	71.0 %
Parentsaround (Mobile)	100 %	93.9 %	99 %	99 %	83.3 %	74.2 %
Qustodio (Mobile)	100 %	98.0 %	99 %	99 %	91.7 %	77.4 %
Surfie Kids	100 %	90.9 %	99 %	99 %	91.7 %	80.6 %
WebProtectMe Safe Browser	100 %	99.0 %	99 %	100 %	91.6 %	80.5 %
Xooloo (Mobile)	n/a	n/a	n/a	n/a	n/a	n/a

How to read the table

The table shows how effective the tools are in terms of their operation with the main social media platforms.

PARENTS can verify how effective each tool is with content exchanged in each of the six most accessed and popular social media platforms.

Results are provided in % of under-blocked content.

Table 31 – EFFECTIVENESS KEY FINDINGS

Topics	The tools perform better on adult content. 'Other content' is badly filtered, with a under blocking higher than 50 % for almost all tools.
Languages	The tools perform better with English content than with other languages.
Age classes	The tools show similar results for CHILDREN and TEENAGERS. Indeed, the results of under blocking 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 in terms of under blocking.

8.3. MOBILE PHONES PARENTAL CONTROL TOOLS USABILITY: key findings

Table 32 – TESTS RESULTS OVERVIEW FOR USABILITY OF MOBILE TOOLS

TOOL	curbi	Familoop	F-Secure Mobile Security	Mobicip Safe Browser	Norton Family parental control	Parentsaround (Mobile)	Qustodio (Mobile)	Surfie Kids	WebProtect Me Safe Browser	Xooloo (Mobile)
I	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
C	2,66	2,95	2,76	3,07	3,23	3,02	3,07	3,29	3,38	2,67
U	1,24	1,94	2,08	1,58	2,36	2,14	2,55	2,14	2,48	1,44
overall	2,13	2,57	2,51	2,51	2,9	2,69	**2,87**	**2,86**	**3,04**	2,21

How to read the table

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

The scores are scaled from 0 to 4 points.

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

I = Installation

C = Configuration /Reconfiguration

U = Usage

- The **overall score** for the mobile tools range **between 2.13 and 3.04**
- **General findings.** Most tools provide web-based configuration and reporting mechanisms, but most of the tools do not address the CHILDREN appropriately to communicate the objectives of the parental control tool. In some tools, the issue that most CHILDREN consider their mobile phone as a very personal item is not sufficiently reflected in tools' functionalities (i.e. PARENTS often need to take the device from their CHILDREN for monitoring their usage and to access the reporting).
- **Findings on the installation process.** The tools tested are applications that are installed nearly automatically with the download. Therefore, there is no installation process to be handled by the user and installation was not tested.
- **Findings on the configuration process.** The complexity of the configuration process differs among the tools:
  - most tools provide a web-based configuration as well as options within the tool;
  - some tools offer a second application(configuration and monitoring), which can either be installed on the same device or on a second (parent) device;
  - 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 mobiles devices;
  - information on how to proceed after the installation is sometimes missing or badly linked within the smartphone application.
- **Findings on usage.** As most parental control tools work 'in the background' of the mobile phones, there is less usage than with other computer software. Nonetheless, it is important that PARENTS can easily handle the alert messages and the reporting to keep them involved with the tools. Most tools do not specifically address the alert message to CHILDREN/TEENAGERS but rather to adults. Some tools offer an appropriate reaction to the alert message for a blocked web site, for example the redirection to safe resources or the possibility to ask for unblocking. The reporting function is comprehensible for most tools and the amount of information is adequate.

8.4. MOBILE PHONES PARENTAL CONTROL TOOLS SECURITY: key findings

Table 33 – TESTS RESULTS OVERVIEW FOR SECURITY OF MOBILE TOOLS

TOOL	SCORE	SECURITY ISSUES	MITIGATION
Curbi	1	Access to harmful content through Google translate, and web cache sites.	Black list google translate website and the web cache sites. Disallows access to App store
Familoop	1	Access to harmful content through Google translate, and web cache sites. Uninstalled without asking credentials or pin	Black list google translate website and the web cache sites. Disallows access to App store
F-Secure Mobile Security	1	Access to harmful content through web cache sites and Google Translate. Does not filter pages inside an iframe	Black list web cache sites and Google Translate. No mitigation for iframe problem.
Mobicip Safe Browser	**4**	No issues found	
Norton Family parental control	1	Access to harmful content through web cache sites and Google Translate. Does not filter pages inside an iframe	Black list web cache sites and Google Translate. No mitigation for iframe problem.
Parentsaround (Mobile)	1	Access to harmful content through Google Translate. Does not filter pages inside an iframe	Black list Google Translate. No mitigation for iframe problem
Qustodio (Mobile)	1	Access to harmful content through web cache sites and Google Translate. Uninstalled without pin	Black list google translate website and the web cache sites. Disallows access to App store
Surfie Kids	1	Access to harmful content through web cache sites and Google Translate.	Black list google translate website and the web cache sites.
WebProtectMe Safe Browser	1	Access to harmful content through web cache sites and Google Translate. Uninstalled without pin	Black list google translate website and the web cache sites. Disallows access to App store
Xooloo (Mobile)	**4**	No issues found	

How to read the table

Security is measured in terms of capacity of the tool to prevent the user from by-passing or disabling the filter through a specific set of actions. The assessment has been carried out through a binary model: (Yes) the tool prevents the user from by-passing; (No) the tool does not prevent the user from by-passing.

The score is assigned to the tool according to the issues raised while testing:

0 = Issues making the tool easily non operative

1 = Critical or severe issues

2 = Issues requiring some computer skills

3 = Minor issues

4 = No issues identified

For each tool, major issues identified are briefly indicated in the third column, while potential actions are suggested to mitigate security issues in the fourth column.

9. ALTERNATIVE TOOLS

FINDINGS FOR
FUNCTIONALITY, EFFECTIVENESS, USABILITY AND SECURITY

Alternative tools

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

9.1. ALTERNATIVE TOOLS FUNCTIONALITY: key findings

The table below shows an overview of the tests performed on FUNCTIONALITY of ALTERNATIVE TOOLS

Table 34 – OVERVIEW FOR FUNCTIONALITY RESULTS OF ALTERNATIVE TOOLS

TOOL	% of FUNCTION COVERED
Surfgarten[3]	**43 %**
Zoodles Premium	**37 %**
Magic Desktop	**30 %**
JumpTo Secure Kids	23 %
Maxthon Kid-Safe Browser	10 %

- None of the five tested tools reaches the complete functionality tested in SIP Bench III. It is not possible for a tool to gain 100% functionality coverage due to contradicting functionalities (either/or-decision). PARENTS should check the list of functionalities as displayed in the functionality tables in order to find tools that best fit their individual functionality needs.
- The most complete one covers 43 % of functions. However, the alternative tools tested in the 4th cycle provide a broader range of functionalities than previously tested tools.
- **The highest scoring products are:**
  - Surfgarten (43 %)
  - Zoodles Premium (37 %)
  - Magic Desktop (30 %)

[3] The tool 'Surfgarten' uses a whitelist for younger children, but also provides blacklisting for older children/youngsters. For the 2nd benchmarking cycle it was selected among the 'Alternative tools' since, at that stage, it was one of the available tools showing more features owned by these types of tools. For comparison purposes, it was then tested as 'Alternative tool' also in subsequent benchmarking cycles.

Table 35 – TESTS RESULTS OVERVIEW FOR FUNCTIONALITY OF ALTERNATIVE TOOLS (1)

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
JumpTo Secure Kids	N	N	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N
Magic Desktop	Y	N	N	N	Y	N	N	N	N	N	N	Y	N	N	N	N
Maxthon Kid-Safe Browser	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Surfgarten	Y	N	N	N	Y	N	N	Y	N	N	N	Y	N	N	N	N
Zoodles Premium	Y	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N
% of tools with function	60 %	0 %	0 %	0 %	60 %	0 %	0 %	20 %	0 %	0 %	0 %	60 %	20 %	0 %	0 %	0 %

Table 36 – TESTS RESULTS OVERVIEW FOR FUNCTIONALITY OF ALTERNATIVE TOOLS (2)

Area of need	Management			Filtering Customisation					Keywords			Time	Blocking Message		% function coverage
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	
JumpTo Secure Kids	Y	Y	Y	N	N	Y	N	N	N	N	N	Y	N	N	23 %
Magic Desktop	Y	N	N	N	Y	Y	Y	Y	N	N	N	Y	N	N	30 %
Maxthon Kid-Safe Browser	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	10 %
Surfgarten	Y	N	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y	43 %
Zoodles Premium	Y	Y	Y	N	Y	Y	Y	Y	N	N	N	Y	N	Y	37 %
% of tools with function	80 %	40 %	40 %	20 %	60 %	100 %	80 %	80 %	0 %	0 %	0 %	80 %	20 %	40 %	

In the table below the main findings on specific issues of functionality are summarised.

Table 37 – MAIN FINDINGS ON FUNCTIONALITY OF ALTERNATIVE TOOLS

Area of Functionality	Findings
Customisation of Web content filtering	▪ All tools are white-list based and only allow a limited access to the Internet. Therefore, specific restriction functionalities are usually not necessary ▪ Three tools allow additionally the PARENT to create their own blacklist ▪ Only one tool allows the customisation of filtering topics
Management of users' profiles	▪ All except one tool enable the PARENT to create and manage different profiles for users with different needs
Remote Management and Monitoring	▪ Remote Management and Monitoring is possible for two tools
Language Interface	▪ English is the most frequent language whereas the choice of tools is limited for many other European languages

9.2. ALTERNATIVE TOOLS EFFECTIVENESS: key findings

Table 38 – TESTS RESULTS OVERVIEW FOR EFFECTIVENESS FOR ALTERNATIVE TOOLS

TOOL	Overall Score	
	≤ 12	≥ 13
JumpTo	**2.5**	**2.5**
SurfGarten	**2.5**	**2.5**
Magic Desktop (*)	n/a	n/a
Maxthon Kid-Safe Browser (*)	n/a	n/a
Zoodles Premium (*)	n/a	n/a

(*) Walled garden or walled-garden-like tools for which effectiveness tests are not meaningful since they will result in 100 % over-blocking and 0 % under-blocking

How to read the table

The table shows how effective the tools are in filtering harmful content. The tool is scored with reference both to the "adult" and to "other harmful" content (drugs, violence, racism, etc.) taking into account two different classes of age (≤12 years old and ≥13 years old).

An overall score is assigned to each age class as the result of the average performance of the two types of content. The scoring scale considers both the over blocking (non-harmful pages which are blocked) and under blocking (harmful pages which are not blocked).

Effectiveness Score. The overall score ranges from 0 to 4. The scores provide measurement as it follows:

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 level of filtering, nonetheless a non-small part of the content is not correctly filtered

3 = Good: the tool offers a good level of filtering, but part of the content is not correctly filtered.

4 = Excellent: the tool offers a very good level of filtering and satisfies the parents' needs in terms of effectiveness.

9.3. ALTERNATIVE TOOLS USABILITY: key findings

Table 39 – TESTS RESULTS OVERVIEW FOR USABILITY FOR ALTERNATIVE TOOLS

TOOL	JumpTo Secure Kids	Maxthon Kid-Safe Browser	Zoodles Premium	Magic Desktop	Surfgarten
I	2,84	n/a	2,81	3,76	n/a
C	2,42	2,45	2,73	3,32	2,75
U	1,24	1,48	1,9	1,69	2,37
Usability	1,2	1,5	1,8	1,7	2,4
Hedonic Quality	1,1	1,8	2,7	3,0	1,7
overall UX / Usability	1,2	1,6	**2,1**	**2,1**	**2,1**

Usability Alternative	Overall Score
Zoodles Premium	**2,1**
Surfgarten	**2,1**
Magic Desktop	**2,1**
Maxthon Kid-Safe Browser	1,6
JumpTo Secure Kids	1,2

How to read the table

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

I = Installation

C = Configuration /Reconfiguration

U = Usage

UX = User Experience

- Three of the tested tools were PC tools (JumpTo, Zoodles, Magic Desktop) while two were for mobile devices (Maxthon, Surfgarten).
- In the "classical" usability rating Surfgarten reaches the highest score (2.4), followed by Zoodles Premium (1.8), Magic Desktop (1.7), Maxthon Kid-Safe Browser (1.5) and JumpTo Secure Kids (1.2).
- Looking at the Hedonic Quality, Magic Desktop (3.0) and Zoodles Premium (2.7) reach higher scores than the other three tools.
- In the overall usability test, the highest score (2.1) is reached by Surfgarten, Magic Desktop and Zoodles Premium, while scores for the other two tools are considerably lower.

Figure 1 – ALTERNATIVE TOOLS USABILITY SCORING

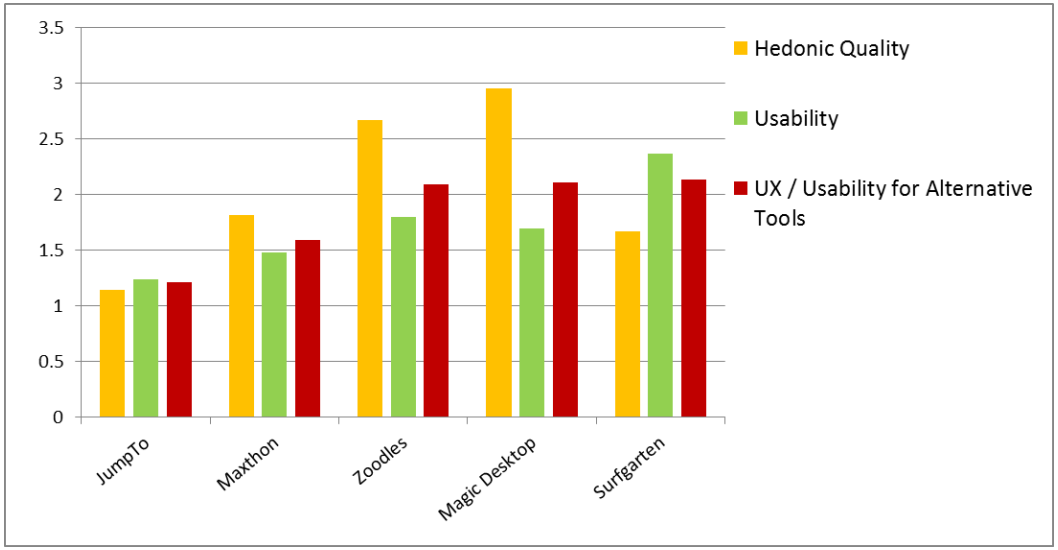

Figure 1 shows the performance of the five Alternative tools according to the Usability criterion, the Hedonic Quality and the overall UX/Usability. Apart from traditional usability, joy of use has also been tested via an additional instrument: the scale “Hedonic Quality” of the AttrakDiff[4] inventory. This scale has two subscales: ‘Hedonic Quality – Stimulation’ and ‘Hedonic Quality – Identity’.

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

9.4. ALTERNATIVE TOOLS SECURITY: key findings

Table 40 – TESTS RESULTS OVERVIEW FOR SECURITY FOR ALTERNATIVE TOOLS

Tool	Score	Security issues	Mitigation
JumpTo Secure Kids	**4**	The users can logout easily disabling all filters. If you choose this tool configure correctly your OS, disabling the access to other browser and permitting only the use of JumpTo builtin browser	
Magic Desktop	**4**	No issues found	
Maxthon Kid-Safe Browser	**4**	It is a walled garden. If you choose this tool make sure to limit the access to the Google Play Store and do not install other browsers. The tool can be a good choice in conjunction with the XooLoo tool. Be careful if you put Google in 'favourite' since this action will introduce the ability to access to harmful content via Google translate and Google Cache. You can use a safe search engine http://www.kidrex.org/ to give some freedom to your child.	
Surfgarten	**4**	Be sure to disable access to Safari, Apple Store and to other browsers. It can be uninstalled without pin.	Disallow access to App store
Zoodles Premium	2	It's too easy to exit from the application killing it from task manager or pressing ALT+TAB selecting the app from the task bar and closing it. A presence of a PARENT is required.	

10. PARENTAL CONTROL TOOLS FOR GAME CONSOLES

Game consoles and the Internet

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

Game consoles were not tested in the 4th benchmarking cycle since no major updates have been identified in the market with respect to tools tested in the 1st benchmarking cycle conducted in 2014.

Results from that cycle showed limited functionalities of the tools for game consoles compared to other devices and the limit for PARENTS to monitor the online CHILD/TEENAGER activity on such devices, while being able to switch off the access to the Internet.

Some developments may occur in the market during 2017, but it will be out of the SIP-BENCH III Study period.

According to the results of the SIP-BENCH III 1st cycle it has been considered less important to measure performance of game consoles and benchmarking tests on such devices have been left.

Furthermore, as the statistics show in the last years, global sales of current generation game consoles have decreased from 2008 to 2016.

The results of SIP-BENCH III tests for game consoles are available on the SIP-BENCH III web site in the 1st cycle report at the link: http://www.sipbench.eu/phase6.cfm.

11. RESULTS DISCLOSURE AND ETHICAL/LEGAL ISSUES

Results disclosure

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

The results are mainly provided through tables and graphics. The common scale adopted is 0 to 4. In case of effectiveness, a % view of the results is provided: % of the webpages over blocked or under blocked.

The figures' rationale is explained under each table with an "How to read the table" box.

Ethical and legal issues

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

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

12. CONCLUSIONS

- Parental control tools are only a **part of the ecosystem** for children safety.
- Parental control tools work best when used **openly** and **honestly in partnership with kids**, not as a stealth spying method.
- Parental controls tools should be understood as **facilitators** for parent-child discussions on what entails appropriate and inappropriate content and behaviours.
- **Parents' involvement** in the tool **configuration** process is **crucial**.
- The tools testing process is designed considering a **virtual scenario** in which the user can access directly to any remote website; however this is something difficult in the real context.
- Each **tool**, if properly chosen and configured, is **good for a specific purpose**.
- **A single perfect tool does not exist**: **none**, in fact, of the 25 tools tested in the 4th benchmarking cycle **scores better in two or more areas of performance** against the other tools.
- Each PARENT should look therefore for the tool that best matches his/her own needs. A balance should be found in the tool selection process among needs, taking into account results achieved with the tests in the four areas of performance.
- The main challenge for future applications is to **ensure filtering of user-generated content and Web 2.0 content** and improve performance of parental control tools in this area.
- A focus should be put on enhancing children's opportunities on the Internet, while coping with their **improved and growing skills and resilience** to potential harm.

ANNEXES

ANNEX 1 - TOOLS LIST

Device	Tool Name (Version)	Company	System
PC/Mac	Witigo Parental Filter	Witigo/Profil Technology	Linux
	Mac Os X Parental Controls	Apple	Mac OS X
	ContentBarrier X9	intego	Mac OS 10.8
	McAffee Total Protection	McAfee Inc	Win 7 and up
	F-Secure Internet Security (2016)	F-Secure GmbH	Win7
	Norton Family Premier	Symantec Corporation	Win 7 and up
	Netintelligence Online Child Safety	iomart Cloud Services Ltd 2016	Win XP, Vista, 7
	Panda Global Protection (2016)	Panda Security	Win 7 and up
	Qustodio/Qustodio Premium	Qustodio LLC	Win 7 and up
	Kaspersky Safe Kids	Kaspersky	Win XP and up
Mobile	Qustodio (Mobile)	Qustodio LLC	iOS 7 and up
	Curbi (2.0.2)	Systemic Pty Ltd	iOS 9.2 and up
	WebProtectMe Safe Browser	DigiTar Inc.	iOS 8.1 and up
	Familoop (iOS 2.3 (updated May 2016)	Familoop	iOS 8.0 and up
	Norton Family parental control	NortonMobile	Android 4.0 and up
	F-Secure Mobile Security (16.3.012820 - June 2016)	F-Secure Corporation	Android 4.0 and up
	Mobicip Safe Browser (Android (updated June 2016)	Mobicip LLC	Android 2.3 and up
	Parentsaround (Mobile) (Android 2.604 (updated June 2016)	ARS Nova Systems	Android 2.3 and up
	Xooloo Parental Control (Android 1.2.0 (updated February 2015)[5]	Xooloo SAS	Android 4.2 - 5
	Surfie Kids (1.05576)	Puresight Technologies Ltd.	Android 2.3 and up
Alternative	Magic Desktop (9)	Easybits Software AS	Win 7 and up
	Surfgarten (1.0.1)[6]	Dt. Telekom AG	iOS 5 and up
	Zoodles	Inquisitive Minds, Inc.	Windows; Mac OS X; Android 1.6 and up;
	Maxthon Kid-Safe Browser	Maxthon (Asia) Ltd.	Android 2.2 and up
	JumpTo Secure Kids	Jumpto Media Inc.	Win 7 and up

[5] The new Version 2.5.09 of Xooloo has become available only in February 2017, after the closure of the 4th SIP-BENCH III benchmarking cycle.

[6] As of December 2016, Dt. Telekom does not longer provide Surfgarten. For further information please refer to https://itunes.apple.com/de/app/surfgarten/id660667553?mt=8

ANNEX 2 - GLOSSARY

Anti-virus	The anti-virus software is used to prevent, detect, and remove computer viruses, worms, and Trojan horses.
Application	An application software, also known as an “application” or an "app", is a computer software designed to help the user to perform singular or multiple related specific tasks.
Blacklist	A list that identifies dangerous keywords, URL or website addresses that are blocked by the tool.
Blog	As an abbreviation for "Web blog" is a type or a part of a website usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics, music or video.
Browser	A "Web browser" or "Internet browser" is a software application for retrieving, presenting, and traversing information resources on the World Wide Web.
Cache	A file stored on the hard drive of computers in which the Internet browser stores previously accessed data so that future requests for that data can be processed more quickly.
Configuration	It is an arrangement of functional units according to their nature, number, and chief characteristics. Often, configuration pertains to the choice of hardware, software, firmware, and documentation and affects system function and performance.
Cookie	Also known as a "Web cookie", "browser cookie", and "HTTP cookie", it is a piece of text stored by a user's Web browser.
Download	Downloading is the process of transferring (software, data, character sets, etc.) from a distant to a nearby computer, from a larger to a smaller computer, or from a computer to a peripheral device.
E-mail	"Electronic mail", commonly called email or e-mail, is the method of exchanging digital messages across the Internet or other computer networks.
E-Mail Client	An "email client", "email reader", or more formally "mail user agent" (MUA), is a computer programme used to manage user's email.

File Sharing	File sharing is the practice of distributing or providing access to digitally stored information, such as computer programmes, multi-media (audio, video), documents, or electronic books.
Firewall	A firewall is a part of a computer system or network that is designed to block unauthorised access while permitting authorised communications.
HTTP	The "Hypertext Transfer Protocol" is a networking protocol for distributed, collaborative, hypermedia information systems: it is the foundation of data communication for the World Wide Web.
Installation	Installation (or setup) of a program is the act of putting the program onto a computer system so that it can be executed.
Instant Message	Instant messaging (IM) is a form of real-time direct text-based communication between two or more people using personal computers or other devices, along with shared software clients. The user's text is conveyed over a network, such as the Internet.
ISP (Internet Service Provider)	Also referred to as an "Internet access provider" (IAP), it is a company that offers its customers access to the Internet.
Instant Message	Instant messaging (IM) is a form of real-time direct text-based communication between two or more people using personal computers or other devices, along with shared software clients. The user's text is conveyed over a network, such as the Internet.
Keywords filtering	Keyword Filtering allows to block pages which may contain inappropriate content. This is made through the set-up of rules that filter content with particular keywords or a combination of keywords.
Messenger	MSN Messenger (now named Windows Live Messenger) is an instant messaging client created by Microsoft.
Online chatting	It refers to direct one-on-one chat or text-based group chat (also known as "synchronous conferencing"), using tools such as instant messengers, Internet Relay Chat, talkers and possibly Multi-User Domains.
Operating System	An operating system (OS) is a software, consisting of programmes and data, that runs on computers and manages the computer hardware providing common services for efficient execution of various application software. Windows, Mac OS or Linux are operating systems.
Over blocking	It occurs when the tool blocks non-harmful content.

P2P	"Peer-to-peer" (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes.
Protocols	A "communications protocol" is a formal description of digital message formats and the rules for exchanging those messages in or between computing systems and in telecommunications. Protocols may include signalling, authentication and error detection and correction capabilities.
Proxy	A proxy server is a server (a computer system or an application program) that acts as an intermediary for requests from clients seeking resources from other servers.
Skype	It is a software application that allows users to make voice calls and chat over the Internet.
Social network	A social network is an online service, platform, or site where people share ideas, activities, events, and interests within their individual or shared networks. Facebook is a social network.
Temporary Internet Files	Temporary Internet Files is a directory on Microsoft Windows computer systems used by Internet Explorer and other Web browsers to cache pages and other multimedia content, such as video and audio files, from websites visited by the user. This allows such websites to load more quickly the next time they are visited.
Under blocking	It occurs when the tool allows harmful content.
Uninstallation	It is the removal of all or parts of a specific application software.
Upload	Uploading is the sending of data from a local system to a remote system with the intent that the remote system should store a copy of the data being transferred.
URL	A "Uniform Resource Locator" specifies where an identified resource is available and the mechanism for retrieving it. The best-known example of the use of URLs is for the addresses of Web pages on the World Wide Web, such as http://www.example.com/.
Virus	A computer virus is a computer programme that can copy itself and infect a computer.
Web-based email	Email service offered through a web site (a webmail provider) such as Hotmail, Yahoo! Mail, Gmail, and AOL Mail.
Whitelist	A list that identifies keywords, URL or website addresses considered safe.