European Commission

Benchmarking of parental control tools for the online protection of children

SIP-BENCH III

FINAL REPORT

A study prepared for the European Commission DG Communications Networks, Content & Technology by:

INNOVA Technology Transfer & Valorisation

CYBION Online Business Intelligence

stiftung digitale-chancen

Digital Single *Market*

This study was carried out for the European Commission by:

INNOVA Srl (Italy)
Ms. Antonella Vulcano
a.vulcano@innova-eu.net

CYBION Srl (Italy)
Ms. Rina Angeletti
angeletti@cybion.it

Stiftung Digitale Chancen (Germany)
Dr. Carola Croll
ccroll@digitale-chancen.info

Internal identification

Contract number: 30-CE-0528769/00-05

SMART number: 2012/0044

DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission’s behalf may be held responsible for the use which may be made of the information contained therein.

ISBN 978-92-79-70499-4

doi:10.2759/80227

© European Union, 2017. All rights reserved. Certain parts are licensed under conditions to the EU.

Reproduction is authorised provided the source is acknowledged.

ABSTRACT

Today, accessing the Internet has become an essential part of our daily lives. From an early age, children live in a digital environment and grow up using a wide range of interconnected devices for various activities (learning, entertainment, communication with family and friends, pastimes).

Apart from opportunities and advantages, the Internet also carries threats to children and youths, from access to inappropriate content (e.g. pornography, violence, self-harm) to exposure to online predators or dangerous behaviour which they can be either victims or authors of (e.g. sexting, cyberbullying).

In this framework, parents' supervision and monitoring of online activity of their children and youngsters is essential. The market offers a broad range of parental control systems able to block or filter content, manage the use, monitor activities, set time limits and quotas.

SIP-BENCH III is a benchmarking study procured by the European Commission's DG CONNECT under the Safer Internet Programme1. The study has been conducted as a benchmarking exercise on a selected list of parental control tools available in the market to raise awareness, provide users (parents and carers) with an overview of the existing parental control tools and support them in the selection of tools that best match their needs.

[1] Decision No 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 establishing a multiannual Community programme on protecting children using the Internet and other communication technologies, published in the Official Journal L 348 of 24.12.2008, p.118.

Table of Contents

Introduction

Children and youths are becoming one of the main user groups[2] of online and mobile technologies in Europe. In 2015, the Internet Governance Forum (IGF) recognised the potential of the Internet and other ICTs to improve children's access to learning, information, health, participation and play. However, it also aroused the concern that Internet access increases the risks to children, resulting in calls for their protection[3].

The EU has supported and promoted a safer use of the Internet through the Safer Internet programmes since 1999, with the aim of educating users (particularly children, parents and carers), and to fight against illegal content and harmful conduct online. Within the framework of the Digital Single Market, several key actions address children and youths online through the European Strategy for a Better Internet for Children[4], which was adopted in 2012. Over the years, the initiatives covered increased awareness of child online safety and the implication of the use of new technologies by young people.

In the actual context, in addition to setting rules and actively talking with children, parents rely on technical filtering, parental control tools or interpersonal monitoring strategies[5]. In the market the range of products (parental control tools) available to ensure filtering or monitoring is quite diversified and is gradually increasing.

SIP-BENCH III – 'Benchmarking of parental control tools for the online protection of children' is a study procured by the European Commission's DG CONNECT within the framework of the Safer Internet Programme 2008-2012. The purpose of the study was to implement a benchmarking exercise of parental control tools available in the market and help end-users (notably parents and child carers) to choose the most appropriate parental control tool that best fits their specific needs. The benchmarking exercise was implemented through eight-monthly testing cycles on a number of parental control tools, allowing parents/carers to monitor their children/teenagers' activity on the Internet accessed through PCs, mobile devices and game consoles. Each cycle concluded with a summary of tests results showing the performance of the benchmarked parental control tools. Results are publicly available online on the SIP-BENCH III web site (http://www.sipbench.eu/).

The present report provides an overview of the whole benchmarking study conducted over the period December 2012-February 2017. Following an introduction which explains what parental control tools are and what the specific market segment is (Chapter 1), the report provides a description of the methodology applied in conducting the study (Chapter 2). The main results and findings of the testing cycles are then presented (Chapter 3). Chapter 4 reports on dissemination activities carried out to publicise the study results. Chapters 5, 6 and 7 report on the effectiveness of the available products on the market, the emerging market trends, and the pricing policy. Finally, the report provides recommendations to users (parents/carers), tool providers and policy makers to give inputs on how to better align the products to users' needs and suggest policy strategies and initiatives in line with market trends.

[2] "Being young in Europe today - digital world", EUROSTAT - Statistics Explained, February 2017 (http://ec.europa.eu/eurostat/statistics-explained/index.php/Being_young_in_Europe_today_-_digital_world)

[3] "One in Three: Internet Governance and Children's Rights", Global Commission of Internet Governance, Sonia Livingstone, John Carr and Jasmina Byrne, PAPER SERIES: NO. 22 — November 2015

[4] https://ec.europa.eu/digital-single-market/en/news/communication-european-strategy-make-internet-better-place-kids

[5] EU Kids Online III, "Findings, methods, recommendations", KU Leuven, Belgium, February 2016

1. Parental control tools and the overall context

Children and youths connect to the entire world using the Internet. They are usually more online than adults. Internet use by children/youths does not only entail watching videos, but also reading webpages, interacting on social networks, chatting, etc. According to the EU Kids Online survey[6]:

- 9-16-year-old Internet users spend 88 minutes per day online, on average;
- The most common location for Internet use is the home (87 %), followed by school (63 %);
- 33 % go online via a mobile phone or handheld device;
- 22 % of 9- to 10-year-olds and 53 % of 11- to 12-year-olds are on Facebook
- Among social network users, 26% have public profiles.

The **content** that children and youths may encounter while accessing the Internet is one of the main problems, namely sites promoting violence, racism, sites full of hate, pornographic sites, etc. Public anxiety often focuses on pornography, “sexting”, bullying and meeting strangers, especially for young children. But there are also other risks that worry children, including many teenagers, especially those associated with user-generated content (e.g. hate speech, pro-anorexia, self-harm, drug-taking or suicide). Some of the content or conduct may be illegal, such as hate speech, while others may not be illegal, but nevertheless potentially harmful for children.

The results from a survey commissioned by ESET®[7] in May-June 2015, using Google Consumer Survey and conducted with 2,000 parents in the UK and USA, shows that **88 % parents worry about what children can access on the Internet** (81 % worry about their children visiting inappropriate web pages; 71 % are concerned about their kids giving their personal details to strangers online; 61 % worried that their children spent too much time on a device).

Other problems related to the access to the Internet by young people is the time spent, for example, or their conduct.

It is obviously not possible to control and supervise everything while minors are surfing the Web on a PC, much less on a smartphone or a tablet. Children cannot be left to their own devices, especially when their devices are Wi-Fi enabled.

Parents and carers should be provided with the **necessary resources and competencies** enabling them to be in a better position to make sure that their children/teenagers (youngsters/minors) are not exposed to harmful content. In the new connected world, the parents’ role in protecting and empowering children is both fundamental and more demanding. But this role can be affected by the level of awareness and technology equipment the parents have. There is, in fact, a risk of **“protection divide”** where children with well-educated, technology-savvy parents might be better protected than those with less prepared parents.

[6] EU Kids Online is a multinational research network that uses multiple methods to map children's and parents' experience of the internet, in dialogue with national and European policy stakeholders. The EU Kids Online survey is the result of a unique, detailed, face-to-face survey in homes with 9-16-year-old Internet users from 25 countries conducted by the EU Kids Online network. 25,142 children and their parents were interviewed during 2010. EU Kids Online. Finding, methods, recommendations. 2014 (https://lsedesignunit.com/EUKidsOnline/index.html?r=64)

[7] https://www.eset.com/int/about/newsroom/products/88-of-parents-concerned-about-what-children-can-access-online-reveals-survey/

That is where parental control software comes in, with the ability to filter out unwanted content, limit screen time, and, in some cases, monitor social media interactions.

Such tools cannot, of course, replace the direct communication of parents/carers with youngsters regarding the concerns they have about the Internet, but they can be useful supporting tools to monitor online activity and to filter the access to harmful content, while respecting minors' privacy.

Despite the potential of parental control tools, according to the ESET® survey conducted in UK and USA, **only 34 % of parents have installed a parental control app** to help manage their kids' online experiences and only 37 % do not have any security running on their mobile or tablet to protect their kids while using their device. According to the EU Kids Online study conducted in 2014 in 25 EU countries, only **25 %** of parents use parental controls or other means to keep track of the websites visited by their children or block/filter some types of websites.

This is a big gap since parental control tools can support parents in their efforts to keep their children/youths' Internet experiences safe, fun, and productive.

Parental control tools 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 (words or images, if the respective URLs are blacklisted)
- ➢ Manage usage – to limit Internet access by setting time limits and time quotas;
- ➢ Monitor activities – to check, through alerts and reporting, youngsters' activity on Internet.

There are **three** different **ways to use** a parental control tool:

- ✓ Install software on the PC, use a pre-installed tool, for example on a Mac PC or iOS device, or download an app on the mobile device;
- ✓ Subscribe to an online filtering service offered by an Internet Service Provider -ISP;
- ✓ Combine both solutions.

From simple content filters to robust home network solutions, parental controls offer a wide range of options and solutions that are available in the market.

Conducting a benchmarking exercise on the different systems requires a selection of tools and the identification of specific areas of tools' performance that is worth investigating. This is at the root of the rationale of the SIP-BENCH III Study, as will be illustrated in the following pages.

2. The SIP-BENCH III Benchmarking Study

2.1. The Study framework

THE FUNDING FRAMEWORK

The SIP-BENCH III benchmarking study builds on the methodological approach and the results achieved in a previous similar study 'SIP-BENCH II' conducted under the same EU programme (more details on results of the SIP-BENCH II study can be found at http://sipbench.eu/index.cfm/secid.6).

THE STUDY OBJECTIVES

The success and efficacy of parental control products largely vary. There is a need, therefore, for a **rigorous and neutral expert review of parental control tools**.

The Study has been commissioned with the aim of:

- raising awareness of tools that protect children and youths from harm online;
- providing users (notably parents and carers) with an overview of the existing parental control tools;
- supporting users in the selection of the parental control tool that best matches their needs.

THE TOOLS TESTED

In each of the four cycles, the study analysed, on average, **25 parental control tools**. The selection of the tools to be tested was made by SIP-BENCH III experts, according to the type of access device:

- Parental control tools for **PC/MAC**;
- Parental control tools for **mobile devices** (such as smartphones, tablets, etc.);
- Parental control tools for **game consoles** (only in the 1st cycle) to use for online gaming, chatting with other players and downloading content;

In the four SIP-BENCH III cycles Mac OS for parental controls were tested in PC tools. In the 1st and 2nd SIP-BENCH III cycles built-in iOS tools have been tested in mobile tools.

The parental control tools for game consoles were considered separately from PCs since their primary use is not Web surfing but gaming and online gaming (including chatting). Game consoles provide parents with a set of integrated (embedded) parental control functionalities. However, these do not include website filtering, even though the Web can be accessed from the game console. The embedded tool provides functionalities for filtering online chat, online gaming and content downloading.

The testing of parental control tools for game consoles was skipped in SIP-BENCH III after the first cycle, as no updated tools for game consoles were available on the market at that stage.

By the second cycle, a further segment of tools had been included, namely the **Alternative tools**. These are parental control tools based entirely on white lists (so-called "walled gardens"), or children-safe browsers, which are usually designed to create a safe environment for very young children. These tools were assessed using a different methodology, as they function in a very different way from other tools.

THE GROUPS OF USERS AND AGE DIFFERENTIATION

Within the SIP-BENCH III study, a users' needs identification has been made referring to two major groups of users, namely **parents** and **child carers** as direct users, and **children** and **youngsters** as indirect beneficiaries of the tools. In the following, the indirect beneficiaries are referred to as "youngsters".

The youngsters were classified into two age groups: children aged 12 years and younger (≤ 12 years old) and young people aged 13 years and older (≥13 years old).

THE ASSESSMENT AREAS

The testing cycles have been conducted to assess **four areas of performance** of each tool:

- **Functionality -** To assess functionalities offered by the tool; for example, to check if the tool is compatible with the operating systems (e.g. Windows, Linux, Mac OS), if it filters web content according to keywords, topics, URLs or if it can block or monitor access to the internet, e-mails, chats, instant messaging tools. A list of 'desirable' functionalities has been pre-defined and 'functionality coverage' has been measured, taking into account the number of functionalities offered by each tool.

- **Effectiveness -** To check to what extent each tool blocks harmful content and allows non-harmful content. The extent of under-blocking (can the tool block websites with unsuitable material for children or can these sites still be accessed?) and over-blocking have been analysed (does the tool block non-harmful content?). Furthermore, it has been assessed on whether the tool is available in languages users are confident with and if it can properly filter blogs, forums and social networking sites. Effectiveness has been measured with regard to topics of the content, age, language, Web type, and social media used.

- **Usability -** to measure ease of installation and configuration processes and usage (Can both beginners and advanced users install the tool on their computer? Is the installation process too complex? Is it easy for the parent and child to understand when a website is blocked?).

- **Security -** to check if the tool can be easily disabled or bypassed by technology-savvy youngsters.

For each of the above areas, a tailored approach was developed by the consortium partners and applied in the testing cycles, as laid down in Chapter 3 of this report.

The choice of the areas of performance is strictly linked to the specific concerns that parents may have on the youngsters' access on the Internet (e.g.: avoid youngsters viewing/producing inappropriate content, being a victim/author of a harmful communication, spending too much time on the Internet or using certain applications/protocols). In the table below, the testing purpose linked to each area of performance is outlined, together with the users' most common questions, relating to that area of performance, which will need to be addressed. As for the identification of needs, please see the below sub-paragraph 2.2.1 which illustrates the methodology and criteria applied.

Table 1 - Areas of performance measured and purpose of the 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 bypass it by means of specific actions	Is it easy or difficult for the CHILD/TEENAGER to uninstall or bypass the tool and access the Internet freely?

The online activities most frequently undertaken by youngsters have been identified by the SIP-BENCH III experts. Several studies were analysed regarding usage of the Internet. The findings can be shortly summarised as it follows:

- ever-younger children go online;
- increasing usage, in general, of different devices;
- children are using personal devices more often;
- increasing usage when children are on their own;
- children are using mobile devices more often;
- more children are using social networking sites.

Activities have been then replicated by the SIP-BENCH III researchers to test the performance of the tools in the four main areas and the results have been recorded.

In the following paragraph, a more detailed description of the methodology applied is provided.

The parents' needs and the online activities of youngsters formed the framework of analysis for the SIP-BENCH III benchmarking study.

2.2. The Methodology applied

The methodology for the SIP-BENCH III benchmarking study assumes **interdependencies** between the **effectiveness** and the **usability** of parental control tools. Within the EU-SIP project *"Youth Protection Roundtable"*[8], one result achieved from the work with children's welfare experts and technical specialists was that filtering software products often do not live up to their full potential due to usability deficiencies. If the users are not able to adjust the products to their needs and maintain the software on their own system, this will lead to poor filtering results.

[8] The 'Youth Protection Roundtable' is a project funded in the framework of the Safer Internet Action Plan of the European Commission from November 2006 till April 2009 whose mission was to establish an inter-communicable socio-technical approach to youth protection.

2.2.1. Users of parental control tools: needs, risks and threats

USER NEEDS ANALYSIS IN REGARD TO PARENTAL CONTROL TOOLS

As explained in the previous chapter, the departure point for the assessment process was an analysis of users' needs, based on existing studies and reports that describe and detail the typical requirements of users in need of protection from web-based harmful content. Based on the findings of the SIP Bench II study[9], the following main needs of parents and child carers, as users of parental control tools, were stated:

- easy to understand;
- fast and simple installation and configuration procedures;
- good overview about the functionalities and options; and
- appropriate wording of messages to parents and children.

ANALYSIS OF RISKS AND THREATS

In addition, for the SIP-BENCH III study, the users' needs were identified, based on an analysis of the risks and threats young users might be confronted with when accessing the Internet. The risks were identified through:

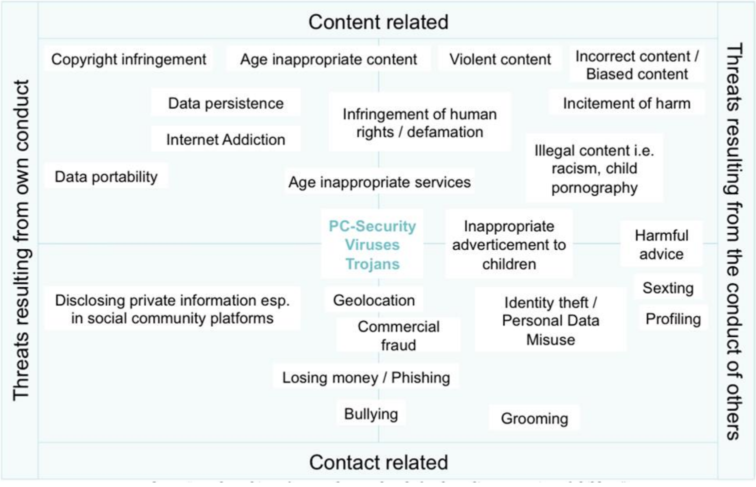
- an understanding of the new emerging trends;
- a portrait of the current situation regarding youngsters' access to the Internet and their usage;
- an overview of the parents' main concerns;
- an analysis of the implications of the youngsters' role in the information flow and their position in the interaction process (information recipient/information provider).

The knowledge of the risks and threats that should be addressed by parental control tools is based both on recent research findings and on the consortium's know-how acquired in the specific field.

The assumption made by the SIP-BENCH III consortium on risks and threats to youngsters on the Internet was based on an updated version of the '*Matrix of Risks and Threats*' developed at the 'Youth Protection Roundtable' in 2008.

[9] 'SIP-BENCH II' is a benchmarking study conducted within the same Safer Internet Programme in the period 2010-2012.

Figure 1 - Matrix of Risks and Threats


Content related
Contact related
Threats resulting from own conduct
Threats resulting from the conduct of others
Copyright infringement
Age inappropriate content
Violent content
Incorrect content / Biased content
Data persistence
Internet Addiction
Infringement of human rights / defamation
Incitement of harm
Illegal content i.e. racism, child pornography
Data portability
Age inappropriate services
PC-Security Viruses Trojans
Inappropriate advertiecement to children
Harmful advice
Sexting
Profiling
Disclosing private information esp. in social community platforms
Geolocation
Commercial fraud
Identity theft / Personal Data Misuse
Losing money / Phishing
Bullying
Grooming

Source: Youth Protection Roundtable, 2008

IDENTIFICATION OF NEEDS

According to the analysis made and assumptions taken, the SIP-BENCH III experts identified **parents' needs** in relation to **four main areas of performance** as is illustrated in the following tables.

Table 2 - FUNCTIONALITY parents' 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 about certain topics and a wish to restrict children/teenagers' navigation to safe websites whilst blocking others.
KEYWORDS	If there is a particular concern about words that children/teenagers may find in the webpages and communication messages.
TIME RESTRICTION	If there is concern about the time children/teenagers spend on 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 the control of 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:

	○ Surfing the Web (Web access). ○ Watching/listening to video/images/music in streaming (streaming through the Web). ○ 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 encounter 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 parents' 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 may 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 the 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 differing efficacies in addressing such needs.
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 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 of children/teenagers coming into contact with inappropriate material produced by "unchecked" sources increased. While configuring the tool, parents should be aware of the kind of content that is mostly accessed by children/teenagers.

Table 4 - USABILITY parents' needs

Type of Need	Need Description
INSTALLATION	The options of either a short installation process, or no installation at all, 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 in setting up different degrees of filtering or transferring filter configurations between different users or devices. They may also have different sensibilities on different types of content. The overall process should be easy to understand, conform with parents' expectations and easy to learn.
USAGE	The alert message in case of blocking should be clear 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 and might want the tool to support them in educating and helping 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 parents' needs

Type of Need	Need Description
SECURITY	Tools may be bypassed 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: ○ Bypass 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. ○ Bypass the tool: changing the time settings (if time limit usage restriction is applied).

2.2.2. Selection of Tools

Following the identification of users' needs, a selection of tools has been made, taking into account the main findings of the previously conducted SIP Bench II study and addressing the below requirements:

- Tools should run on different devices;
- They should filter user-generated content;
- They should allow monitoring and control of time spent online.

Within each cycle, the selection of tools was made ensuring that they could cover, as far as possible, the following features:

- **Limitation and/or prevention of certain types of Internet usage** by youngsters, e.g. accessing or creating inappropriate content on the Internet; harmful contact or conduct between minors (cyber-bullying); harassment and unwanted solicitation of minors on the Internet; disclosure of personal data; spending money without parental consent on the Internet; excessive time-consumption with Internet-related activities.

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

- **Filtering regardless of the language:** the filtering tools should be able to filter multilingual content in at least one EU language and, preferably, in several EU languages. Tools have been tested with reference to **six languages**: English, French, German, Italian, Polish and Spanish.

- **Coverage of the main devices:** the filtering tools versions can be executed on the main hardware devices and software systems offering Internet access to the users. The devices that have been considered are: personal computers, mobile devices (phones and tablets) and game consoles.

- **Type of tools:** stand-alone solutions, server solutions, ISP service provided with Internet connection, service provided by phone companies and default tools provided by software manufacturers or embedded in operating systems, and location of the user interface (on the device or web-based).

- **Support on the main Operating Systems.** The filtering tools should be supported on the main Operation Systems available on selected devices:

    - **For computers:** Windows (XP, Vista, Seven, 8), Mac OS (Tiger, Leopard, Snow Leopard, Lion, Mountain Lion), Linux (Ubuntu);

    - **For Mobile phones:** Android, iOS, Windows 8;

    - **For games consoles:** Nintendo (DS Lite, DS, Wii), Sony (PSP and PlayStation 3, PlayStation 4), Xbox (Xbox 360 and then Xbox 720)[10].

- **Support within the main browsers**: Internet Explorer, Firefox, Google Chrome, and Safari.

- **Filtering methods:** black list of URLs, white list of URLs, word lists, text analysis, and image analysis.

The tools selection included the **main players** (market share relevancy criterion) as well as some **niche products and tools**, whose interface and filtering capacity cover some less prevalent EU languages, as far as they are also available in English language for testing. At least one free tool was included in each cycle.

In addition, starting from the second cycle, **Alternative tools** (walled garden tools, child-safe browsers) were also tested.

It is worth noting here that some tools provide different editions which are available in the market (for example basic, gold, premium, etc.). This variety of edition types has developed further over the benchmarking four cycles and made it more difficult to compare the results the tools achieved in the tests.

[10] This category was skipped after the first cycle in SIP-BENCH III, as no updated tools for game consoles were available on the market at that stage.

2.2.3. Data test set creation and renewal

The data test set used in the effectiveness tests comprised 4,000 relevant data containers with one of the following elements: *URLs, images, videos,* etc., representing the diversity of harmful content to which children and teenagers might be exposed.

Specific **categories of harmful content** that the selected tools should be able to filter, have been selected:

- Adult content
- Violent content and criminal skills/activity that could incite damage to others
- Racist and hate material
- Illegal drug-taking and the promotion of illegal drug use
- Content that could incite youngsters to hurt themselves
- Gambling

A detailed list for each of the above categories is provided in **Annex 1** to this report.

As for the dataset creation, not only home pages of websites were considered (typically www.website.com), but also some deeper links, for instance www.website.com/page1.html and www.website.com/page123.html. An automated data collection and extraction process was carried out based on specific selection criteria determining the choice of specific keywords and examples of inappropriate content, and completed by manual retrieval of data and by a set of raw data with a first possible categorisation. The collected data were afterwards reviewed by the SIP-BENCH III experts to verify whether they were consistent with the selection and categorisation criteria.

All adult harmful content and Web 2.0 content was renewed for each cycle.

The other harmful content and non-harmful content was kept stable for all the cycles, as it is more static and often difficult to find.

2.2.4. Categorisation of the data test set

The data test set was created taking into account the following categories of content, which also represent the macro-categories according to which the data was classified:

- **Adult content data containers** (on average 33-35 % of the total data set). Content covered: adult, sexually explicit content that could impair children' and young adults' sexual development.
- **Other harmful content data containers** (on average 33-35 % of the total data set). Content covered included the following categories:
    - Violent content that could impair children' and young adults' moral and social development and could cause damage to others (e.g. weapons and bombs). Criminal skills/activity that could incite harming themselves or another.
    - Racist and hate material that could cause damage to another or another's freedom and rights.
    - Incitement to self-damaging attitudes, such as: illegal drug-taking, the promotion of illegal drug use, or anorexia/bulimia.
    - Gambling, content that could cause damage to people's lives.

- **Non-harmful content** (on average 30-35 % of the total data set). The tools were also tested for *false positives*, i.e. content that should not be filtered, but that is filtered anyway (over-blocking). For each of the macro-categories a set of non-harmful content was chosen, whose themes are close to harmful content (e.g. sex-education content, historical content on racism and genocides, journalistic information on terrorism), to test the over-blocking performance of the tools.

The following table presents how the data set test was split between the categories of content. Figures in the table include both appropriate and inappropriate content. For each category, two-thirds of the data set test were related to inappropriate content and one-third to appropriate content.

A large part of data test set is constituted by Web 2.0, which includes user-generated content. The choice was made due to the growing relevance of this type of content.

Table 6 - Distribution of data test set by content (figures expressed in number of data containers)

	Content Category			
	Harmful Adult content	Other harmful content	Non-harmful sexual related content	Non-harmful content related to other categories
Web	800	800	400	400
Web 2.0	530	530	270	270
Total	1,330	1,330	670	670

2.2.5. Database creation

The data test set was stored in a database which included the following information for each data container:

Table 7 - Database fields description

Field	Value type	Comments
URL	URL	If applicable, the URL of the resource to be accessed
Content language	Text (one language)	One of the following languages: English, German, Italian, Spanish, French and Polish
Harmful ≤ 12	Yes/No	Harmful/Non-harmful for '12 years old and below' users
Harmful ≥ 13	Yes/No	Harmful/Non-harmful for '13 years old and above' users
Category of content	One Category	In case of more than one possible associable category, the prevailing one was chosen (e.*g. adult content, violent content)*

The database was used during the whole process of creating and reviewing the data set test, and later during the tools tests.

Access to the database was possible only during the reviews and validation sessions. The database was only accessible to specific authorised IP addresses and secured by a login and a password, to ensure that no unauthorised access to the harmful content in the data test set was possible.

2.2.6. Assessment of the tools: Functionality tests

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

The table below shows the list of functionalities checked in relation to each area of need.

Table 8 - List of Functionalities to be checked prior to Usability Test

Area of Need	Functionality / Capability	Specific Issue
Management	Management of User profiles	Create several profiles
	Remote Management	Manage on various devices
	Monitoring	Remote access to monitoring
Filtering Customisation	Topics	Customisation of Filtering Topics
	URLs White List	Restrict Browsing to White List
		Default White List
		Modification OR Creation
	URLs Black List	Creation of User's own Black List
Keywords	Keywords	Default Black List
		Default White List
		Creation of a User's Black List
		Creation of a User's White List
Time	Time Limit Settings	Set a specific time frame or web access duration
Blocking Message	Type	Ask for unblocking by parents
		Redirect to safe resources
Usage Restriction	Web	Block Access
		Monitor Access
	Safe search	Availability
	Social Networks	Block Access

		Monitor Usage
	Personal data Provision	Block
	Streaming	Block Access
		Monitor Access
	P2P	Block the application
		Monitor Downloads
	Skype	Block chat
		Block video chat
		Monitor
		Prevent new Contact
	Windows Life Messenger[11]	Block chat
		Block video chat
		Monitor
		Prevent new Contact
	Email	Block email client and/or webmail access

Functionalities not available were marked, but not followed further. Functionalities available were reviewed by the SIP-BENCH III experts with regard to their usability.

If the usability reviews revealed further functionalities not detected earlier, they were reviewed with regard to their usability. With this strategic approach, it was ensured that the whole range of available functionalities was attributed to the product and reviewed with regard to usability.

2.2.7. Assessment of the tools: Effectiveness tests

The effectiveness tests were carried out in a testing laboratory adapted to the needs of the study. The testing lab consisted of the following **infrastructure:**

- **database server**: hosts the database that contains the data set test and the results of the test;
- **DNS server**: a DNS server is used to redirect the clients' requests to the content when closed Internet is used;
- **content server:** to provide copies of the content provided through the closed Internet;

[11] The application was tested as long as it was available.

- **connection:** a dedicated Internet connection, with a firewall and ADSL connection;
- **servers**: to install and test server-based filtering products;
- **desktop computers**: to install personal filtering products and to run tests;
- **game consoles**: to test filtering tools;
- **mobile phones and tablets**: to test filtering tools.

How the tests were performed

The effectiveness tests were carried out based on the data test set. They were performed on the default configuration of the tools. The test procedure followed a certain number of steps:

1) The data set test database was screened.

2) Information related to each data container was extracted and the test for that data container was performed, for instance, to visualise a web page.

3) The response of the filtering tools was to block or not to block the content. This response was stored in data test database. Along with the request, the expected response was also stored according to data test.

4) The response provided by the filtering tool was compared to the expected result (whether the content should be blocked according to the data test set).

5) Additional manual verification through spot-checks ensured accuracy and validity of the test results. The statistical analysis then calculated the percentage of missed harmful content (false negatives) and non-harmful content (false positives) according to the typology of the data test (with criteria regarding languages, type of harmful content).

How the tests were automated

Some scripting tools were used to automate the tests as much as possible. Basically, the scripts were to:

1) extract data from the data set test and for each data container;

2) launch the related tools;

3) access the resources;

4) store the outcomes of the tests in the database.

How the "*Closed Internet*" worked

To test the full spectrum of characteristics of the filtering tools, a "*Closed Internet*" was built to emulate the real-life Internet in a controlled way. This provided test predictability and ensured that the content was the same during all tests for all filtering tools, so that all tools could be compared more accurately.

Content was retrieved from the Internet and stored on the content server. The request of a resource (a web page for instance) was intercepted by the DNS server and redirected to one of the "*Closed Internet*" content servers. The content server responded to the request as if it were the true (and original) Internet server. The response was intercepted by the filtering tool activated for the test and it decided to block, erase or pass on the content. Since the original Internet addresses were kept, URL-based filtering was not affected.

Tests of user-generated content filtering

Part of the data set test was dedicated to user-generated content (Web 2.0). Some additional capability tests were performed to assess the capacity of the tools to filter: outbound content (e.g. by publishing content on Facebook or on a blog); inbound specific content (i.e. content personalised according the user's preferences); or multimedia content with little or no textual information; and content that is evolving over time (e.g. due to harmful comments added to the originally non-harmful content).

2.2.8. Assessment of the tools: Usability tests

Analysis of users' needs with regard to usability

As a first step, the users' needs with regard to usability were identified based on previous experiences and work with children's welfare organisations and other experts in the field, especially at the 'Youth Protection Roundtable'. This led to a list of **general requirements regarding usability**, covering the following aspects: ease of installation and uninstallation; ease of configuration; transparency of documentation; ease of customisation; speed, look and feel; comprehensibility of the terminology used within the tool; impact on system performance; overall perception of the system; set-up of user profiles; maintenance; ease-of-use; comprehensibility of reporting; updating capabilities; degree of compatibility with client software likely to be found on a typical user's computer.

The description of user needs was then validated against **international standards**, both general and special usability standards. The usability standards were derived from scientific research, negotiated by standardisation bodies and published as consensual declarations. In the case of usability, they became part of the occupational health and safety regulations in the EU, e.g. in Council Directive 90/270/EEC, which enforces the application of existing "principles of software ergonomics". The relevant usability standards[12] were checked to determine which of them could be applied to the analysis and evaluation of the filter software under consideration.

Usability review in laboratory

For each filtering tool a usability review was performed in parallel by two SIP-BENCH III experts in a usability laboratory. Thus, it was ensured that the usability of the products was tested in a standardised manner to achieve comparable and consolidated results.

Usability testing covered the relevant usability aspects including installation, configuration/customisation, general user experience, documentation, and supported operating systems.

For the processes of **installation and uninstallation** the testing criteria were, e.g., speed, capabilities, maintenance, reporting, terminology, overall perception of the software, impact on system performance, and degree of compatibility with client software likely to be found on a typical user's computer.

For the process of **configurability** additional testing criteria were, e.g., parameter configuration, setting up classes of users (e.g. according to age, cultural background), customising filtering criteria, option to manage and / or limit the time spent online and online purchases (such as app downloads, etc.).

Among the **testing** criteria for usage were e.g. user experience, context-sensitive explanations, and pleasure of use.

The transfer of these review criteria into the design of the usability criteria catalogue, as well as the test settings, was firstly based on DIN ISO. Secondly, the testing methodology incorporated experiences from SIP Bench II, about what is important to parents in their decision-making about a tool. New technological

[12] ISO 9241: Ergonomics of Human System Interaction (2006), ISO 14915: Software ergonomics for multimedia user interfaces, Web Accessibility Initiative of the W3C (WAI), IEC TR 6199, ISO/IEC 18021, ISO/TR 22411, ISO/IEC 25000

developments, like combined tools for different devices with similar configuration settings and interfaces, also required adaptations in the testing methodology.

The criteria catalogue was arranged into the following seven sub-categories according to DIN ISO standards.

Table 9 - Criteria Catalogue sub-categories

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

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

2.2.9. Assessment of the tools: Security tests

The security of the tools could be compromised by configuration tampering, with the intention of bypassing the filtering, or by security vulnerabilities caused by the tools themselves. Within the security tests, the SIP-BENCH III experts checked whether it is possible to:

- use the IP address instead of the URL;
- use an alternative browser;
- disable the application without a password;
- disable the tool through the Task Manager;
- access the Control Panel applets;
- use a proxy instead of a direct connection to the Internet;
- rename a blocked application;
- change time and data settings (to overcome time limits);
- use anonymisers;
- use translation sites;
- start the computer in Safe Mode;
- change the port of Peer to Peer application;
- access content through the Google cache.

In addition, the tools were assessed with standard tests for detecting vulnerabilities and security holes.

ADDITIONAL METHODOLOGY FOR ALTERNATIVE TOOLS

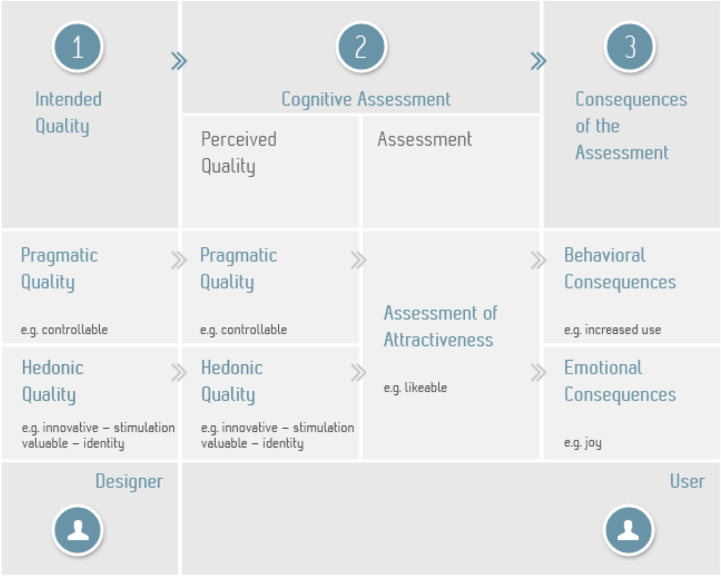
In SIP-BENCH III so-called 'Alternative tools' were included in the testing procedure. Most of these tools provide an area for safe use of the Internet by younger users, e.g. a walled garden or a sandbox mostly based on white list filtering. The usability of the process of usage of these tools needs to be addressed differently from the other types of parental control tools. The testing methodology, therefore, placed a special focus on the usability of the tools by the children.

This was done, in addition to the previously described testing methods, by applying the '**AttrakDiff**' methodology to the tools. AttrakDiff helps to understand how users personally rate the usability. It makes the evaluation of any product by users, customers possible. From the evaluation data, it is possible to measure how attractive the product is in terms of usability and appearance.

The theoretical work model was researched and tested in several studies by Hassenzahl and colleagues[13]. The studies showed that the hedonic and pragmatic qualities are perceived consistently and independently of one another. Both contribute equally to the rating of attractiveness. While testing and implementing AttrakDiff-1 it became clear that a separation of the two constituent aspects of hedonic quality, namely stimulation and identity would be preferable.

The AttrakDiff theoretical work model, illustrated in the diagram below, is able to evaluate how the pragmatic and hedonic qualities influence the subjective perception of attractiveness giving rise to consequent behaviour and emotions.

Figure 2 – AttrakDiff evaluation model



Source: © User Interface Design GmbH

[13] 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.

The model separates the four essential aspects:

- The product quality intended by the designer (1).
- The subjective perception of quality and subjective evaluation of quality (2).
- The independent pragmatic and hedonic qualities.
- Behavioural and emotional consequences (3).

To measure the attractiveness, an instrument of measurement is applied in the format of semantic differentials. It consists of 28 seven-step items whose poles are opposite adjectives (e.g. "confusing - clear", "unusual - ordinary", "good - bad"). Each set of adjective items is ordered into a scale of intensity.

Each of the middle values of an item group creates a scale value for pragmatic quality (PQ), hedonic Quality (HQ – including HQ-I and HQ-S) and attractiveness (ATT).

AttrakDiff[14] provides an online evaluation tool for rating the quality of interfaces and usability, providing graphic presentations. The tool is easy to use.

Through the application of the AttrakDiff, the perceived **pragmatic** quality, the **hedonic** quality and the **attractiveness** of the tools were measured by the SIP-BENCH III experts and displayed in a matrix of values, to gain an overall score.

The results of the usability tests and the AttrakDiff scores were synthesised in one score for the Alternative tools, to make the results comparable with those of the other analysed tools.

2.3. The validation process through the Steering Board

At the beginning of the Study a Steering Board (SB) was set up, incorporating independent experts with experience and knowledge in the specific field of investigation of the study. The role of the Steering Board was to validate each benchmarking cycle process by analysing results achieved and described in each cycle report. A SB meeting, at the end of each cycle, was arranged with the SIP-BENCH III consortium members to discuss the main findings and provide expert feedback and advice. In addition, the SB Members were consulted for the selection of the tools to be tested under each cycle and during the cycles on an ad hoc basis.

When setting up the Steering Board, the SIP-BENCH III consortium considered the specific competencies and experience of its members, the EU geographical coverage, and the independence with respect to the market under analysis. The final list of SB Members was approved by the European Commission at the initial meeting.

The Steering Board composition at the date of the 4th cycle was as follows:

Table 10 - Steering Board composition

Name	Organisation	Country
Georgi Apostolov	Bulgarian Safer Internet Centre	Bulgaria
Maija Katkovska	Latvian Internet Association, Latvian Safer Internet Centre	Latvia

[14] http://www.attrakdiff.de/index-en.html

Martin Schmalzried	Confederation of Family Organisations in the EU (COFACE)	Belgium
Jose Luis Zatarain	Fundación Promoción Social de la Cultura (FPSC)	Spain
Mark Bootz	Technical Youth Protection	Germany
Jutta Croll	German Centre for Child Protection on the Internet – I-KiZ	Germany
Alex Amneus	Swedish Media Council	Sweden

Activities of the Steering Board were coordinated by the project coordinator INNOVA, preparing working papers, drafting minutes of the SB meetings and collecting feedback from SB Members. In total, five SB meetings have been held while running the study as detailed in the table below:

Table 11 - Steering Board meetings

N°	Meeting	Date	Purpose	Venue
1	1st Steering Board meeting	18/03/2013	Introduction SB/ Methodology presentation	Berlin, Germany
2	2nd Steering Board meeting	29/08//2013	Analysis and validation 1st testing cycle results	Berlin, Germany
3	3rd Steering Board meeting	28/03/2014	Analysis and validation 2nd testing cycle results	Rome, Italy
4	4th Steering Board meeting	05/12/2014	Analysis and validation 3rd testing cycle results	GoToWebinar call
5	5th Steering Board meeting	28/02/2017	Analysis and validation 4th testing cycle results	Rome, Italy

3. Results of the 4 benchmarking cycles

3.1. Tools tested in the four testing cycles

The SIP-BENCH III Study has been implemented by conducting four consecutive testing cycles in the period 2013-2016. In each cycle, the selected tools have been tested and analysed with respect to results of the tests in the four areas of performance: Functionality, Effectiveness, Usability and Security.

At the end of each testing cycle a summary of main findings has been provided in the form of a benchmarking cycle report as follows:

- 1st cycle: Summer 2013 - 1st benchmarking cycle report published in November 2013
- 2nd cycle: Winter 2013/2014 - 2nd benchmarking cycle report published in May 2014
- 3rd cycle: Summer/Autumn 2014 3rd benchmarking cycle report published in October 2016
- 4th cycle: July - December 2016; 4th benchmarking cycle report published in April 2017.

Before publishing each benchmarking cycle report, validation of results from the Steering Board of independent experts and approval from the European Commission has been obtained.

In total, an average of 25 tools has been tested in each cycle. An overview of the number of tools tested in the four cycles is provided in the table below.

Table 12 - Overview of tools tested in the four cycles

Cycle	Access device				TOTAL
	PC	Mobile devices	Game consoles	Alternative tools	
Cycle 1	13	9	3	0	25
Cycle 2	13	10	0	3	26
Cycle 3	10	10	0	5	25
Cycle 4	10	10	0	5	25

From the second cycle, the study started testing ‘Alternative tools’ and ended tests on ‘Game consoles’ since no major updates have been identified in the market for parental control tools for such devices, by the SIP-BENCH III experts, with respect to tools for game consoles tested in the 1st benchmarking cycle. Results from that cycle showed limited functionalities of the tools for game consoles compared to other devices and limited ability for parents to monitor the online youngsters’ activity on such devices, while being able to switch off the access to the Internet.

In the synoptic table below an overview of the tools tested in the four cycles is provided. From one cycle to the other, the tools list has been reviewed since the methodology required a certain number of new tools in each cycle; new tools were available on the market at the launch of each new benchmarking cycle, while others were discontinued or available versions were deprecated.

Table 13 - Overview of tools tested in the four cycles

TOOLS	BENCHMARKING CYCLES			
	1st cycle	2nd cycle	3rd cycle	4th cycle
PC				
CONTENTBARRIER X9				✓
DANS GUARDIAN		✓		
F-SECURE INTERNET SECURITY	✓	✓	✓	✓
JUSPROG	✓	✓		
K9 WEB PROTECTION	✓	✓	✓	
KASPERSKY SAFE KIDS				✓
MAC OS X PARENTAL CONTROLS	✓	✓	✓	✓
MCAFEE FAMILY PROTECTION / ALL ACCESS	✓	✓	✓	✓ McAfee Total Protection
NET NANNY	✓	✓		
NET-INTELLIGENCE	✓			✓ Netintelligence Online Child Safety
NORTON ONLINE FAMILY	✓	✓	✓	✓ Norton Family Premier
OPTENET PC	✓	✓	✓	
PANDA	✓	✓	✓	✓ Panda Global Protection (2016)
PURESIGHT OWL	✓	✓	✓	
QUSTODIO		✓	✓	✓ Qustodio Premium
TREND MICRO ONLINE GUARDIAN FOR FAMILIES	✓	✓	✓	
WINDOWS 8 FAMILY SAFETY	✓			
WITIGO PARENTAL FILTER				✓
MOBILE				
AVG FAMILY SAFETY			✓	

BSECURE	✓			
CURBI (2.0.2)				✓
FAMILOOP (iOS 2.3 (updated May 2016)				✓
F-SECURE MOBILE SECURITY	✓	✓	✓	✓
IOS PARENTAL CONTROLS (MOBILE)	✓	✓		
KASPERSKY IOS SAFE BROWSER		✓		
K9 WEB PROTECTION BROWSER (MOBILE)	✓	✓	✓	
MOBICIP SAFE BROWSER	✓	✓	✓	✓ (Android - updated 06/2016)
MOBIFLOCK	✓	✓	✓	
MOBILE PARENTAL FILTER	✓	✓	✓	
NETNANNY FOR ANDROID	✓	✓	✓	
NORTON ONLINE FAMILY (MOBILE)	✓	✓	✓	✓
PARENTSAROUND (MOBILE)			✓	✓ (Android 2.604- updated 06/2016)
QUSTODIO				✓
SAFE BROWSING		✓		
SURFIE KIDS (1.05576)				✓
WEBPROTECTME SAFE BROWSER				✓
XOOLOO (MOBILE)			✓	✓ (Android 1.2.0- updated 02/2015)
GAME CONSOLE				
ASTARO - PARENTAL CONTROL FOR WII	✓			
MICROSOFT LIVE SAFETY	✓			
TREND MICRO KIDS SAFETY - PS3	✓			
ALTERNATIVE TOOLS				

CARE4TEEN			✓	
FAMIGO			✓	
JUMPTO SECURE KIDS				✓
KIDZUI			✓	
KINDERSERVER		✓		
MAGIC DESKTOP		✓	✓	✓
MAXTHON KID-SAFE BROWSER				✓
SURFGARTEN		✓		✓
XOOLOO (MOBILE) [YOUNGER AGE GROUP]			✓	
ZOODLES				✓

3.2. Overview of main findings of the four testing cycles

3.2.1. Rationale of the classification of tests results

The tests conducted in the four cycles produced **results** in the four areas of performance (Functionality, Effectiveness, Usability and Security) which **vary substantially** among the different tools, even within the same device category.

Within each cycle, it was not possible to present a ranking list for all results, since none of the tools scored better in all areas of performance against the other tools. The same also applies to comparing results of the four cycles. What has, however, been possible is to compare **performance within the same category** of tools (PC, Mobile, Game Consoles and Alternative tools) in one specific area and **how this performance evolved** along the four cycles.

The above comes also from a specific direction by the Steering Board Members, at the beginning of the SIP-BENCH III study, who suggested focusing on qualitative recommendations on the tested tools instead of providing a mere global ranking list. This was justified, firstly, because from a methodological point of view, the overall score is questionable and far less reliable than single scores measured for effectiveness, usability and security. Secondly, the Steering Board Members were convinced that parents would get the wrong impression of the tools when provided with a list that prioritises the tools, based on an overall score, because the perception of parents of the areas of performance may vary according to the different needs they have (for example, for some parents the effectiveness of certain types of content is most important, while others may ask for the most secure or usable tool). With an overall score, a tool with high security but low effectiveness might range on the list alongside a tool with low security but high effectiveness, thus giving misleading advice to parents.

Finally, it must be pointed out that SIP-BENCH III is a **vendor/supplier-independent** comparative expert assessment of parental control tools, aimed at providing parents with an overview of the existing tools, benchmarked according to the identified needs, and supporting their choice of the most appropriate tool which best matches their specific needs. In this regard, parents' different needs and priorities cannot be addressed with the provision of a list of tools, ranked by an overall result, but they can be more appropriately reflected and fulfilled through searchable tool lists in a database.

3.2.2. Scoring methods

As regards the scoring methodology applied to tests results, a scale has been assigned to measure tests results in each performance area.

Below a brief explanation is provided. It is useful to read the tables and figures in the following pages and the description of each testing cycle.

FUNCTIONALITY

As for functionality, the study did not assign a score as an overall result. It was decided to check the availability of a set of functionalities for each analysed tool, but not to rate the availability of the functionalities with a score. Therefore, for this area of performance, given a set number of functionalities searched by the study, a percentage has been assigned to each tool to provide information on how many functionalities are covered by that specific tool (% of functionalities covered).

It is not possible for a tool to gain 100 % functionality coverage due to contradicting functionalities (either/or-decision).

EFFECTIVENESS

The scope of the tests is to assess how effective each tool is 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 to 4. The scores provide measurement as it follows:

Score	**Description**
0	Very weak: the tool is less effective than a random tool
1	Weak: the tool has a low effectiveness and answers parents’ needs incompletely
2	Fair: the tool has a fair level of filtering. However, a 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

Usability concentrates on tasks users want to perform with a product/tool. There is a new 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: pleasure of use, aesthetics, emotions, stimulation or attractiveness. These quality aspects are not related to tasks users perform with a tool and are thus called non-task related or 'hedonic' aspects. Thus, the hedonic quality results more reflect the "child usage", while the usability results more reflect the "parent usage".

Results for usability 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 detailed test results are available both in individual tool fiches and in an online database. The scores are scaled from 0 (lowest performance) to 4 points (best performance).

SECURITY

Security is measured in terms of capacity of the tool to prevent the user from bypassing or disabling the tool through a specific set of actions. The assessment has been carried out through a binary model:

- 'Yes' the tool prevents the user from bypassing;
- 'No' the tool does not prevent the user from bypassing.

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

Score	Description
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

3.2.3. Main results in the four testing cycles

The main results which emerged across the four testing cycles are briefly summarised below, while a general description of the four cycles is provided in subsequent paragraphs. For detailed results of the benchmarking cycles, the single cycles benchmarking reports can be consulted online at the link: http://sipbench.eu/.

FUNCTIONALITY

- None of the tested tools, either for PC tools or mobile tools, achieved complete **functionality coverage**. It is not possible for a tool to gain 100 % functionality coverage due to contradicting functionalities (either/or-decision). Through the Yes/No list for each tool included in the four benchmarking cycle reports, it is possible to check which functionalities it provides or how many tools offer a specific functionality.
- Most of the PC tools provide parents with a **complete set of customisation functionalities**.
- **Mobile tools** able to filter the web pages' content have **limited functionalities** when compared to the tools available for PCs.
- All PC tools enable parents to **block the access** specifically to the **Internet**.
- The majority of the PC tools offer the option of **blocking access to social networks** and the option of forcing the user to use the Safe Search functionality of the most common search engines.
- The majority of the PC tools can **block Web based streaming** provided by YouTube.
- Mac, iPhone and iPad are **equipped with an OS-embedded parental control tool**. The Android operating system does not provide an embedded tool for mobile phones or tablets. The only way to filter the Internet is to use an external tool.

- Most of the PC tools can provide parents with at least **basic reporting** on the youngsters' web activity (visited websites or violations).

- Some PC tools allow **remote access for monitoring**. Some tools grant parents the option of managing the tool online (from a PC or another mobile device). For some tools, it is possible to manage both the mobile tool and the PC tool (provided that user installed both tools on teenager's devices).

- **English** is the most frequent language whereas the tools' choice is limited for many other European languages.

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

- Many mobile tools can be **easily uninstalled**. Many mobile tools consist of a browser with Internet access; often it is easy to use another browser and, in this way, bypass the tool.

EFFECTIVENESS

- The overall effectiveness of tools, in general, is low for both PC and mobile tools. Those with a high rate of over-blocking consequently have a low under-blocking rate and vice versa. The lower the level of both under-blocking and over-blocking, the better the tool. The overall effectiveness score provides only an **overview** of the results. However, in order to make a suitable selection of tools addressing specific needs, it would be useful to check all the functionalities offered and the related results achieved with the tests.

- Many of the solutions tested for mobile devices are also offered on PCs with different interfaces and functionalities. The **effectiveness** of **mobile** solutions is **slightly lower** than the ones assessed for similar PC products.

- Some **functionalities** are **embedded in the operating system** (iOS for example) but this does not relieve the responsibility of the software producers.

- **Effectiveness** among the two **classes of age** is quite **similar** for both PC and mobile tools.

- Content-filtering tools are less effective when dealing with **user-generated content**, which is difficult to categorise. In fact, tools present lower effectiveness with user-generated and Web 2.0 content. In all qualitative tests conducted on web 2.0, all the tools failed.

- **Adult content** is **better filtered** than the "other" content categories.

- Tools work **better on English** language content than on other languages.

- Some of the **game consoles** tested in the first cycle have their own embedded parental control tool which can control chat, online gaming and content downloading/purchasing, but none of the game consoles' parental controls is able to filter web pages according to content.

USABILITY

- **Usability** scores are **higher** for **PC and mobile tools** than for Alternative tools.

- In general, the ability to **customise the tool** to one's own needs are **poor**.

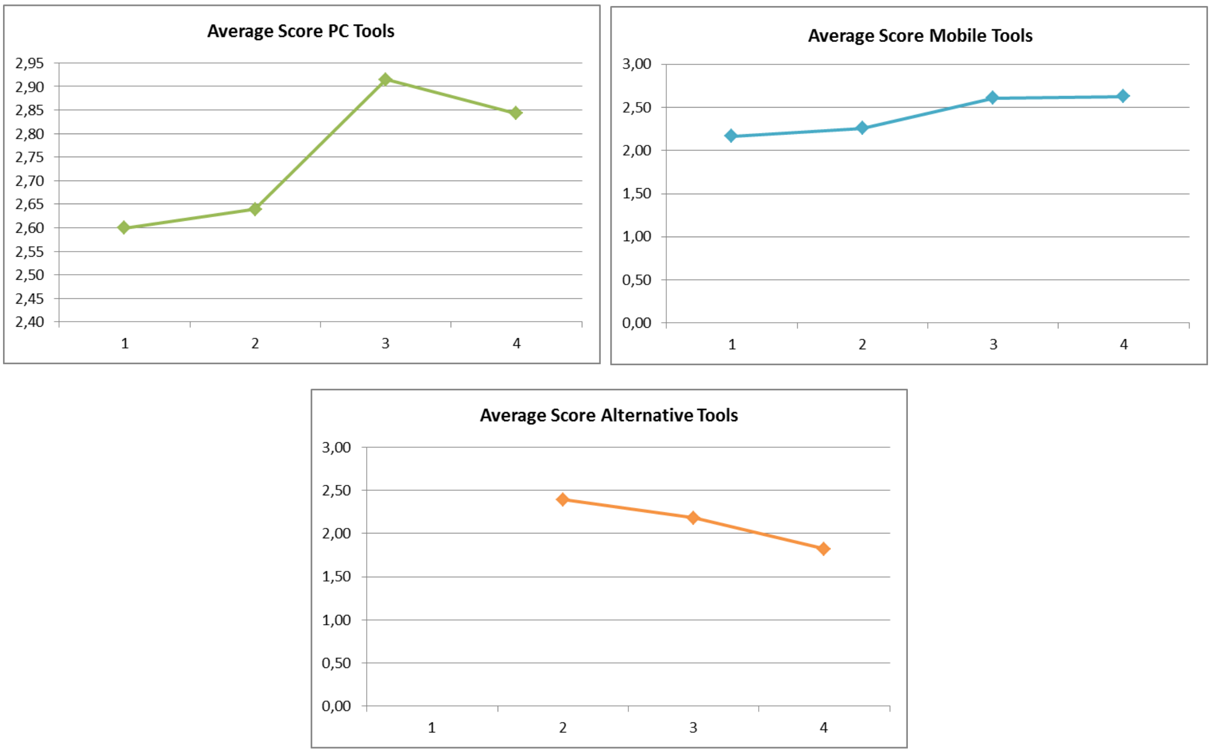
- **Better scores** are usually recorded in **PC tools** for installation and configuration than for usage.

- The **mobile tools** tested, as well as OS-based tools, come as an application that is installed automatically with the download. Therefore, there is no **installation** process to be handled by the user and installation could therefore not be tested.

- The complexity of the **configuration** process differs: most tools provide a web-based configuration; some tools provide a configuration within the tool and additionally a web-based configuration. Additionally, mobile tools sometimes offer the option of a seconding "parent" App for configuration and monitoring purposes.
- Over the four cycles, about one-third of **PC tools** provided a web- or server-based **configuration**.
- Only a few products provide additional information about **filtering,** in general, and about limitations and restrictions of the filtering procedures.
- Most tools do not allow appropriate reaction to an **alert message** for a blocked web site.
- As most parental control tools work 'in the background' of the mobile phones, there is **less usage** than with other computer software.
- The issue that most children consider their mobile phone as a very personal item is not sufficiently reflected in the mobile tools' functionalities, i.e. in most cases parents need to take the device from their children for **monitoring** their **usage** and to access the reporting.

The following Figure shows the results from the four testing cycles for **Usability**. The diagrams show the average score for each cycle and the trend emerging over the whole study period for each category of devices.

Figure 3 – Usability results over the four cycles



For **PC tools**, the best tool in each cycle has a **higher score** than the best tool had in the previous cycle, while the average score is slightly lower for the 4th cycle than for the 3rd. For **mobile tools**, the best tool in each cycle is **higher** than in previous cycles, except the 4th cycle. However, the average score for mobile tools has been **continually rising** over the four cycles.

The average score for **Alternative tools**, as well as the scores for the best tools for PC and mobile devices are **considerably lower** in the 4th cycle than in the previous cycles. A possible explanation is that user expectations have outgrown the performance of the tools currently on the market. Provided with a huge amount of well-designed applications for various purposes, users seem to be accustomed to certain standards and the development of tools seems to be lagging behind that development.

SECURITY

- **Security ranges** 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.
- Some of the PC and mobile tools present **security weaknesses**. The most common is allowing access to a prohibited page through translation site or Google Cache.
- The weakest point of some tools is that they can be **uninstalled** without a password, credentials or pin.

3.3. The first testing cycle

The main results of tests on the **25** selected **tools** in the first benchmarking cycle are shown in the table below per category of devices.

Table 14 - Overview of tests results in the 1st cycle

TOOLS	**Effectiveness ≤ 12**	**Effectiveness ≥ 13**	**Usability**	**Security**
PC TOOLS				
F-SECURE INTERNET SECURITY	1,5	1,5	2,36	1
JUSPROG	n/a	1,6	2,16	4
K9 WEB PROTECTION	1,1	1,2	2,76	3
MAC OS X PARENTAL CONTROLS	0,9	0,8	2,31	2
MCAFEE ALL ACCESS	1	1	2,87	0
NET NANNY	1,5	1,5	2,76	4
NETINTELLIGENCE	n/a	n/a	2,47	n/a
NORTON ONLINE FAMILY	1,8	1,6	3,12	1
OPTENET PC	0,8	1,1	2,54	1
PANDA	1,3	1,1	2,09	0
PURESIGHT OWL	1,7	1,6	2,89	4
TREND MICRO ONLINE GUARDIAN	1,1	1,2	2,76	0
WINDOWS FAMILY SAFETY	1,5	1,5	2,7	1
TOOLS FOR MOBILE DEVICES				
BSECURE	0,4	0,8	n/a	0

F-SECURE MOBILE SECURITY	1,5	1,5	2,24	1
IOS PARENTAL CONTROLS (MOBILE)	n/a	n/a	1,89	n/a
K9 WEB PROTECTION BROWSER (MOBILE)	1,1	1,2	1,42	1
MOBICIP SAFE BROWSER	1,1	1,2	1,92	0
MOBIFLOCK	0,3	0,6	2,27	1
MOBILE PARENTAL FILTER	1,1	1,2	2,17	1
NET NANNY FOR ANDROID	0,7	0,9	2,56	0
NORTON ONLINE FAMILY (MOBILE)	1,5	1,5	2,87	0
TOOLS FOR GAME CONSOLES				
ASTARO PARENTAL CONTROL - WII	n/a	n/a	1,05	n/a
MICROSOFT LIVE SAFETY - XBOX	n/a	n/a	1,76	n/a
TREND MICRO KIDS SAFETY - PS3	0,7	0,9	0,89	2

- For scoring methods please see under paragraph 3.2.
- **Effectiveness score:** from 0 (Very weak) to 4 (Excellent)
- **Usability score:** from 0 (low) to 4 (high)
- **Security score**: from 0 (Issues making the tool easily non-operative) to 4 (No issues identified)

For each performance area, highest scores recorded in each tool category are marked in bold.

Below a summary of main results in the three categories of devices are briefly reported.

RESULTS FOR PC PARENTAL CONTROL TOOLS

Functionality of PC tools

Topic	Results
Functionality coverage	None of the tested tools reached the complete functionality coverage. The three highest scoring products were in order: **PURESIGHT OWL, NET NANNY** and **TREND MICRO ONLINE GUARDIAN**.
Customisation functionalities	Most of the tools provide parents with a complete set of customisation functionalities.
Access to social networks	Eleven tools offer the option of blocking access to social networks and ten tools the option of forcing the user to use the Safe Search functionality of

	the most common search engines.
Access to the Internet	All tools enable parents to block the access specifically to the Internet.
Web-based streaming	The majority of the tools can block Web-based streaming provided by YouTube.
Report on users' activity	Most of the tools can provide parents with at least basic reports on the users' web activity (visited websites or violations).
Remote monitoring	Four tools allow remote access for monitoring.
Security	Some of the tools present security weaknesses. The most common is allowing access to a prohibited page through translation sites or Google Cache. Few tools can be uninstalled without a password.
Language	English is the most frequent language whereas the tools' choice is limited for many other European languages.

Usability of PC tools

Topic	Results
Installation	Eight out of the thirteen tools gain better scores for installation and configuration than for usage.
Customisation	In general, functionalities to customise the tool to one's own needs are poor.
Filtering	Only a few products provide additional information about filtering in general and about limitations and restrictions of the filtering procedures.
Configuration	About one-third of the tools provide a web- or server-based configuration.
Alert messages	Most tools do not allow appropriate reaction to the alert message for a blocked web site.

RESULTS FOR MOBILE DEVICES PARENTAL CONTROL TOOLS

Functionality of tools for MOBILE DEVICES

Topic	Results
Functionality range	Tools able to filter the web-pages content have limited functionalities compared to the tools available for PCs.
Embedded parental control tools	iPhone and iPad are equipped with an OS-embedded parental control tool. However, an external parental control tool is necessary to filter web-pages browsing according to the content. The Android operating system does not provide an embedded tool for mobile phones or tablets. The only way to filter the Internet is to use an external tool.

Remote management	As for usage restriction and monitoring, the tools offer very limited functionalities, in particular for Skype or streaming which are very popular among teenagers. Some tools give parents functionalities to manage the tool online (from a PC or another mobile device). With some tools, it is possible to manage both the mobile tool and the PC tool (provided the user installed both tools on teenager's devices).
Uninstallation	Many tools can be easily uninstalled. Many tools consist of a browser with Internet access; often it is easy to use another browser and in this way, bypass the tool. In many cases, mobile devices tools are useless.

Effectiveness of tools for MOBILE DEVICES

Topic	Results
Effectiveness compared to PC tools	Many of the solutions tested are also offered on PC with different interface and functionalities. The effectiveness of the mobile solutions is slightly lower than the one assessed for the similar PC products.
Low effectiveness	In general, tools have low effectiveness. The over-blocking rate is low for some tools but in these cases the under-blocking rate is very high.
Performance against classes of ages	The tools perform fairly similarly with a configuration for the two age classes (≤12 and ≥ 13).
Performance with Web 2.0 content	Tools present lower effectiveness with user-generated and Web 2.0 content. In all qualitative tests conducted on web 2.0, all the tools failed.
Performance by category of content	The adult content is better filtered than the "other" content categories.
Language	Tools work better with English languages than with other languages.

Usability of tools for MOBILE DEVICES

Topic	Results
Monitoring	The fact that most children consider their mobile phone as a very personal item is not sufficiently reflected in the tools' functionalities, i.e. parents need to take the device from their children for monitoring their usage and to access the reporting.
Installation	The tools tested come as an application that is installed automatically with the download. Therefore, there is no installation process to be handled by the user.
Configuration	The complexity of the configuration process differs: most tools provide a web-based configuration; some tools provide a configuration on the tool and additionally a web-based configuration.

Usage	As most parental control tools work 'in the background' of the mobile phones, there is less usage than with other computer software.

RESULTS FOR GAME CONSOLES PARENTAL CONTROL TOOLS

Functionality

Topic	Results
Functionality coverage	The functionalities of the tools for consoles are very limited compared to other devices. There are only basic ‘enable’ or ‘disable’ functions or irregular working filtering functionalities for websites. The OS-embedded tools control other online activities: online gaming and content downloading/purchasing (apart from a series of offline activities filtering).
Access to the Internet	All the consoles enable parents to switch off the access to the Internet.
Monitoring	None of the tools are able to monitor the online child/teenager activity.

Usability

Topic	Results
Configuration	Compared to parental control tools for PCs, those for game consoles seem to be less well-known by parents. Nonetheless, they can be useful but the configuration of game consoles can be difficult for parents.
Installation	It is a challenge for parents to learn about and to decide on the need to install an additional parental control tool on game console. Tools available for game consoles serve as applications installed automatically with the download. Therefore, there is no installation process to be handled by the user.
Alert messages	As most parental control tools work in the background of the consoles, there is less usage than with other computer software. Nonetheless, it is important that parents can easily handle the alert messages to keep them involved with the products. The tools do not address the alert message for a blocked web site to children and youth but to adults only. Also, no appropriate option for reaction to the alert message is provided.

3.4. The second testing cycle

The second benchmarking cycle on the **26** selected **tools** generated test results as shown in the table below per category of devices.

Table 15 - Overview of tests results in the second cycle

TOOLS	**Effectiveness ≤ 12**	**Effectiveness ≥ 13**	**Usability**	**Security**
PC TOOLS				

DANS GUARDIAN	0,7	0,9	2,1	0
F-SECURE INTERNET SECURITY	1,5	1,5	2,2	1
JUSPROG	n/a	1,8	2,6	4
K9 WEB PROTECTION	1,1	1,2	2,7	3
MAC OS X PARENTAL CONTROLS	1,4	1,3	2,8	2
MCAFEE ALL ACCESS	1,0	1,0	3,0	0
NET NANNY	0,7	0,9	n/a	4
NORTON ONLINE FAMILY	1,8	1,6	3,1	1
OPTENET PC	1,1	1,2	2,4	3
PANDA	1,3	1,1	2,0	0
PURESIGHT OWL	1,1	1,2	3,2	4
QUSTODIO	1,1	1,2	2,9	4
TREND MICRO ONLINE GUARDIAN	1,1	1,2	2,7	0
TOOLS FOR MOBILE DEVICES				
F-SECURE MOBILE SECURITY	1,5	1,5	2,7	1
IOS PARENTAL CONTROLS	1,4	1,3	2,4	1
K9 WEB PROTECTION BROWSER	1,1	1,2	1,7	1
KASPERSKY IOS SAFE BROWSER	1,6	1,2	2,1	0
MOBICIP SAFE BROWSER	1,1	1,2	1,7	0
MOBIFLOCK	0,3	0,6	2,1	1
MOBILE PARENTAL FILTER	1,2	1,4	2,2	1
NET NANNY FOR ANDROID	0,7	0,9	2,7	0
NORTON ONLINE FAMILY	1,5	1,5	2,7	0
SAFEBROWSER	0,6	0,7	2,3	1
ALTERNATIVE TOOLS				
KINDERSERVER	n/a	n/a	2,2	n/a
MAGIC DESKTOP	n/a	n/a	2,5	n/a
SURFGARTEN	n/a	n/a	2,6	n/a

- For scoring methods please see under paragraph 3.2.
- **Effectiveness score:** from 0 (Very weak) to 4 (Excellent)
- **Usability score:** from 0 (low) to 4 (high)
- **Security score**: from 0 (Issues making the tool easily non-operative) to 4 (No issues identified)

For each performance area, highest scores recorded in each tool category are marked in bold.

RESULTS FOR PC PARENTAL CONTROL TOOLS

Functionality of PC tools

Also, in the second cycle, none of the tested tools[15] achieved complete functionality coverage. The two highest scoring products are **PURESIGHT OWL** and **TREND MICRO ONLINE GUARDIAN**, as in the first cycle. High scores have also been recorded for **OPTENET PC** and **QUSTODIO**.

Functionality tests on PC tools conducted during the second cycle led to analogous results of the previous cycle.

Effectiveness of PC tools

In general, tools have low effectiveness. The over-blocking rate is low for some tools but in these cases the under-blocking rate is very high. Results of effectiveness tests on PC tools were similar to the first cycle's results.

Usability of PC tools

Three products score in the top area and gain 3 points or more (PURESIGHT OWL, NORTON ONLINE FAMILY, MCAFEE ALL ACCESS). Eight out of thirteen tools gain better scores for installation and configuration than for usage.

About one-third of the tools provided a web- or server-based configuration, as in the first cycle.

RESULTS FOR MOBILE DEVICES PARENTAL CONTROL TOOLS

Results on Functionality, Effectiveness and Usability were the same of the first cycle.

Since this cycle, Apple also provided content filtering functions as an out-of-the-box feature base on the OS.

RESULTS FOR ALTERNATIVE TOOLS

The alternative tools were tested for Win7 (Kinderserver and Magic Desktop) and for iOS (Surfgarten). All tools allow browsing by white list only, but their white lists differ in terms of quality and quantity.

Alternative tools can restrict access to the Internet completely or they can block Internet access for a defined application.

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

One category of Alternative tools is the so-called 'Walled Gardens'; these tools filter websites based on a white list only. Therefore, there is no problem of under-blocking. In Walled Gardens, no harmful content can get through the filter accidentally and this method is recommended mainly for young children.

Another category is the 'Child Friendly Environment' whose aim is to educate children and its design is tailored for the youngsters.

As the tools offers only access to a white list or a full access to the Internet, there is no filtering and it was not possible to calculate **effectiveness**.

In the case of Alternative tools, the SIP-BENCH III experts tested **usability** only, as these tools work in a different manner and full functionality/effectiveness tests are not possible.

Alternative tools tested under the second cycle offered a good level of **security**.

3.5. The third testing cycle

The third benchmarking cycle on **25** selected **tools** provided with the test results shown in the table below.

Table 16 - Overview of tests results in the third cycle

TOOLS	**Effectiveness ≤ 12**	**Effectiveness ≥ 13**	**Usability**	**Security**
PC TOOLS				
F-SECURE INTERNET SECURITY	1.5	1.5	2.93	1
K9 WEB PROTECTION	1.1	1.2	2.90	3
MAC OS X PARENTAL CONTROLS	1.0	1.0	2.94	2
MCAFEE ALL ACCESS	1.0	1.0	3.00	0
NORTON ONLINE FAMILY	1.8	1.6	3.28	1
OPTENET PC	1.1	1.2	2.44	3
PANDA	1.3	1.1	2.24	0
PURESIGHT OWL	2.2	2.4	3.09	4
QUSTODIO	1.1	1.2	3.11	4
TREND MICRO ONLINE GUARDIAN	1.1	1.2	3.22	0
TOOLS FOR MOBILE DEVICES				
AVG Family Safety	1.5	1.5	2.13	0
F-SECURE MOBILE SECURITY	1.5	1.5	2.84	1
K9 WEB PROTECTION BROWSER	1.1	1.2	1.96	1
MOBICIP SAFE BROWSER	1.1	1.2	2.22	1

MOBIFLOCK	0.4	0.8	2.93	0
MOBILE PARENTAL FILTER	1.2	1.4	2.90	4
NET NANNY FOR ANDROID	0.7	0.9	3.19	4
NORTON ONLINE FAMILY	1.8	1.6	3.10	0
Parentsaround (Mobile)	0.7	0.9	2.80	4
Xooloo (Mobile)	1.4	1.3	2.06	4
ALTERNATIVE TOOLS				
Care4teen	n/a	n/a	2.5	n/a
Kidzui	n/a	n/a	2.1	n/a
MAGIC DESKTOP	n/a	n/a	2.2	n/a
Famigo	n/a	n/a	2.4	n/a
Xooloo (Mobile) [younger age group]	n/a	n/a	1.7	n/a

- For scoring methods please see under paragraph 3.2.
- **Effectiveness score:** from 0 (Very weak) to 4 (Excellent)
- **Usability score:** from 0 (low) to 4 (high)
- **Security score**: from 0 (Issues making the tool easily non-operative) to 4 (No issues identified)

For each performance area, highest scores recorded in each tool category are marked in bold.

RESULTS FOR PC PARENTAL CONTROL TOOLS

Functionality of PC tools

Also in the third cycle, none of the tested tools achieved complete functionality coverage. The two highest-scoring products are **PURESIGHT OWL** and **Norton Online Family**. High scores have been recorded also for OPTENET PC and QUSTODIO, as in the previous cycle.

Results of functionality tests on PC tools were similar to results of the two previous cycles.

Effectiveness of PC tools

In general, tools have low effectiveness. The over-blocking rate is low for some tools but, in these cases, the under-blocking rate is very high.

Results of effectiveness test on PC tools were similar to results of the first and second cycles.

Usability of PC tools

Almost all tools (9 in 10) gain better scores for installation and configuration than for usage. Four tools score in the top area **NORTON ONLINE FAMILY, TREND MICRO ONLINE GUARDIAN, QUSTODIO and PURESIGHT OWL**.

RESULTS FOR MOBILE DEVICES PARENTAL CONTROL TOOLS

Results in the third cycle on Functionality, Effectiveness and Usability were the same as in the first and second cycles.

RESULTS FOR ALTERNATIVE TOOLS

Functionality of ALTERNATIVE TOOLS

The alternative tools tested in the third cycle were for Win7 (Care4teen, KidZui and Magic Desktop) and for Android (Famigo and Xooloo_Mobile).

Care4teen, KidZui and Magic Desktop allow browsing by white list only, but their white lists differ as for their quality and quantity.

Famigo and Xooloo (Mobile) are similar. They are closed systems with their own entertainment choices available to purchase. It is not possible to search the internet as with a web browser.

Effectiveness of ALTERNATIVE TOOLS

It was not possible to calculate the effectiveness score on the Alternative tools tested in the third cycle as these tools work in a different manner and full functionality/effectiveness tests are not possible.

Usability of ALTERNATIVE TOOLS

In the overall usability, Care4teen reaches the highest score, followed by Magic Desktop and KidZui (2.2). Xooloo (Mobile) reached the worst rating.

Security of ALTERNATIVE TOOLS

In general, the tools offer a good level of security.

3.6. The forth testing cycle

The fourth and final benchmarking cycle conducted on **25** selected **tools** has produced test results as shown in the following table.

Table 17 - Overview of tests results in the fourth cycle

TOOLS	Effectiveness ≤ 12	Effectiveness ≥ 13	Usability	Security
PC TOOLS				
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	1.8	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
TOOLS FOR MOBILE DEVICES				
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

- For scoring methods please see under paragraph 3.2.
- **Effectiveness score:** from 0 (Very weak) to 4 (Excellent)
- **Usability score:** from 0 (low) to 4 (high)
- **Security score**: from 0 (Issues making the tool easily non-operative) to 4 (No issues identified)

For each performance area, highest scores recorded in each tool category are marked in bold.

RESULTS FOR PC PARENTAL CONTROL TOOLS

Functionality of PC tools

Also in the fourth cycle, none of the tested PC tools achieved complete functionality coverage. However, it emerged that they provide a broader range of functionalities than tools tested in previous cycles. The three highest-scoring products are **Content Barrier X9**, **Norton Family Premier**, **Kaspersky Safe Kids**.

Effectiveness of PC tools

In general, tools have low effectiveness. The over-blocking rate is low for some tools but, in these cases, the under-blocking rate is very high.

Results of effectiveness test on PC tools were in line with results of the other cycles.

Usability of PC tools

Almost all tools (9 in 10) tools achieve higher scores for installation and/or configuration than for usage. Three tools (Norton Family Premier, Kaspersky Safe Kids, Mac Os X Parental Controls) scored in the top area.

RESULTS FOR MOBILE DEVICES PARENTAL CONTROL TOOLS

Functionality of tools for MOBILE DEVICES

Topic	Results
Functionality range	None of the ten tested tools achieved complete functionality. However, the mobile tools tested in the fourth cycle provide a broader range of functionalities than previously tested tools. The highest scoring tools are: **Surfie Kids, Qustodio Mobile, Norton Family parental control**. Most tools have the option of forcing the user to use the safe search functionality of the most common search engines.
Usage	Seven tools enable parents to create and manage different profiles for users with different needs.
Blacklists	Most of the tools allow parents to create their own blacklist.
Customisation	Only three tools allow the customisation of filtering topics (F-Secure Mobile Security, Qustodio and Serfie Kids).
Filtering	Keywords filtering is very uncommon: only one tool offers this option (WebProtectMe Safe Browser). 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.
Access to the Internet	All tools enable parents to block the access specifically to the Internet (whether using a specific functionality or using the "time restrictions").
Access to social networks	Six tools have the option of blocking access to social networks; only three tools allow the parents to monitor social network usage (Norton Family, Qustodio and Serfie Kids).

Blocking	The tools rarely provide the option of blocking an entire protocol whereas blocking applications is more common. None of the 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 or streaming apps can be blocked. Five tools can block Skype chat and only three tools block video chat.
Remote management	Remote management is possible with 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.
Reporting	Most of the tools can 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	As in the other cycles, English is the most frequent language, whereas the choice of tools is limited for many other European languages.

Effectiveness and Usability of tools for MOBILE DEVICES

Results on Effectiveness and Usability in the fourth cycle were in line with results of the previous three cycles.

RESULTS FOR ALTERNATIVE TOOLS

The alternative tools were tested for Win7 (Magic Desktop and JumpTo Secure Kids) and for Android (Surfgarten and Maxthon Kid-Safe Browser) or both (Zoodles).

Three of the tested tools were PC tools (JumpTo, Zoodles, Magic Desktop) while two were for mobile devices (Maxthon, Surfgarten).

Functionality of ALTERNATIVE tools

Topic	Results
Functionality coverage	None of the five tested tools achieved complete functionality. However, the alternative tools tested in the fourth cycle provide a broader range of functionalities than previously-tested tools. The highest scoring products in terms of functionality were: **Surfgarten, Zoodles Premium** and **Magic Desktop**. Almost all tools enable the parent to create and manage different profiles for users with different needs.
Access to the Internet	All tools are white-list based and only allow a limited access to the Internet. Therefore, specific restriction functionalities are usually not necessary.
Blacklists	In addition, three tools allow parents to create their own blacklist.
Filtering	Only one tool allows the customisation of filtering topics.
Remote management & Monitoring	Remote Management and Monitoring is possible for two tools.

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

Effectiveness of ALTERNTIVE tools

Three tools out of the five Alternative tools (Magic Desktop, Maxthon Kid-Safe Browser, Zoodles Premium) are walled-garden or walled-garden-like tools. Effectiveness of these tools was not tested since, in this case, over-blocking may result in 100 % and under-blocking in 0 %.

Usability of ALTERNATIVE tools

Usability scores are higher for PC and mobile tools than for Alternative tools.

In the overall usability test, the highest score for Alternative tools is achieved by three tools (Surfgarten, Magic Desktop and Zoodles Premium), while scores for the other two tools are considerably lower.

Security of ALTERNATIVE tools

Higher scores are registered for Security for Alternative tools than for PC and mobile tools, and this is obvious, given the nature of these tools working as a ‘protected’ environment.

4. SIP-BENCH III towards the target community: overview of dissemination activities

The SIP-BENCH III Study is conceived as a benchmarking exercise to benefit potential end-users, primarily parents and child carers, but also the wider community interested in acquiring knowledge on parental control tools and their performance. Due to the nature of the study, the public delivery of results was a key objective.

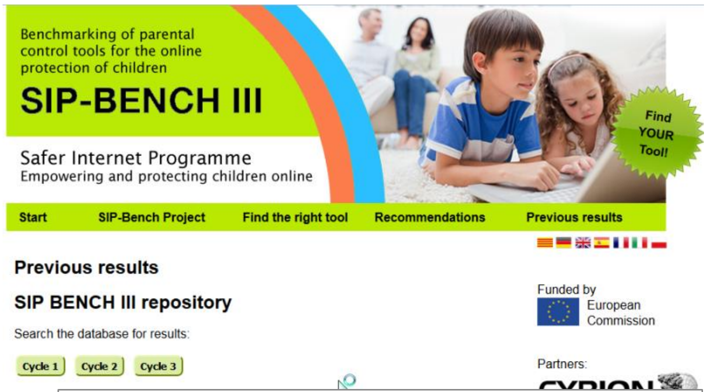
To this end, a number of dissemination tools have been set up and exploited by the SIP-BENCH III consortium to ensure prominence and wide circulation of the study cycles and recorded results.

A brief overview of the dissemination activity conducted over the study implementation period is provided in the following pages.

4.1. Dissemination tools

DEDICATED WEB-SITE

A dedicated website has been set up at the beginning of the first edition (SIP-BENCH II) of the study (http://www.sipbench.eu/) and managed through the whole period of the project execution. The interface is available in **six languages** (English, French, German, Italian, Spanish, and Polish). The site hosts information on the study and provides the target group (e.g. parents) with general and up-to-date information and advice on the use of parental control tools, a list of existing tools as well as information on market evolution.



Previous results

SIP BENCH III repository

Search the database for results:

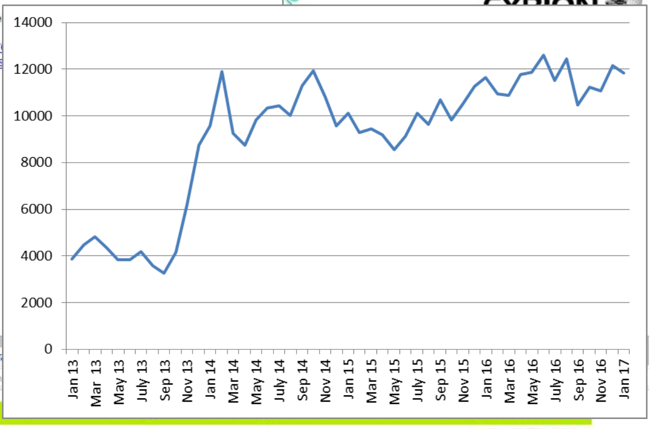
SIP_Be

- 3r
- As

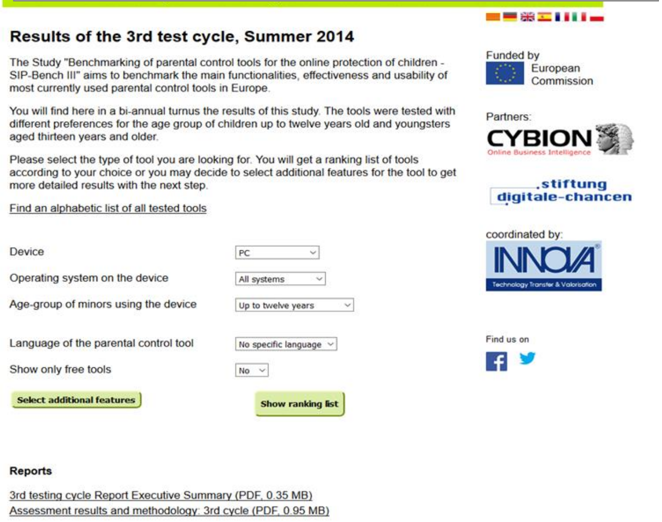
The website has been **progressively updated** with results of the four consecutive benchmarking cycles.

The site has been designed to be attractive, informative and easily interpreted by the target group, bearing in mind differing levels of technical understanding as well as different requirements, depending on the age of the youngster, cultural background and language(s) used by the users.

Visits to the web site by end-users has **gradually increased over the last four years** from 3,880 visits in January 2013 to 11,836 visits in January 2017, as it is shown in the diagram below.



The added-value of the site is a **search engine** for end-users who could easily check parental control tools analysed over the four cycles and results which emerged from the tests. Through a '***Search for a tool***' **function,** it is possible to search for the performance results of a specific tool. The search can be made by: device, operating system, age-group, language. The search can also be organised according to additional features required such as: price, content filtering,


Funded by European Commission
Partners:
CYBION Online Business Intelligence
.stiftung digitale-chancen
coordinated by:
INNOVA Technology Transfer & Valorisation
Find us on
Select additional features
Show ranking list

Results of the 3rd test cycle, Summer 2014

The Study "Benchmarking of parental control tools for the online protection of children - SIP-Bench III" aims to benchmark the main functionalities, effectiveness and usability of most currently used parental control tools in Europe.

You will find here in a bi-annual turnus the results of this study. The tools were tested with different preferences for the age group of children up to twelve years old and youngsters aged thirteen years and older.

Please select the type of tool you are looking for. You will get a ranking list of tools according to your choice or you may decide to select additional features for the tool to get more detailed results with the next step.

Find an alphabetic list of all tested tools

Device	PC
Operating system on the device	All systems
Age-group of minors using the device	Up to twelve years
Language of the parental control tool	No specific language
Show only free tools	No

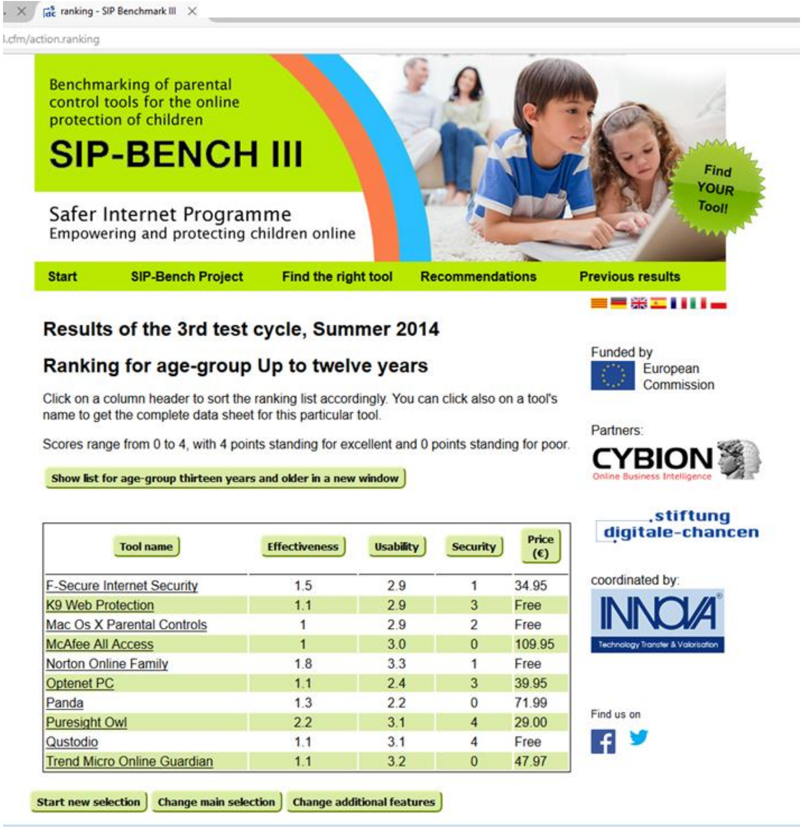
Reports

3rd testing cycle Report Executive Summary (PDF, 0.35 MB)
Assessment results and methodology: 3rd cycle (PDF, 0.95 MB)

keywords, usage restriction, time and blocking message. By activating the search function according to search criteria, the site shows a list of tools that best match the selected criteria. The list shows scores obtained by the tool, in the specific cycle checked, in terms of effectiveness, usability and security. Information on the price of the tool is also provided. In addition, the site provides the list of tools analysed in previous cycles, which match the search criteria. The search functionality can be easily managed by end-users.

Below a specimen screenshot is provided, showing results of the third benchmarking cycle.

Figure 5 – Tool search screenshot


ranking - SIP Benchmark III
l.cfm/action.ranking
Benchmarking of parental control tools for the online protection of children
SIP-BENCH III
Safer Internet Programme
Empowering and protecting children online
Find YOUR Tool!
Start
SIP-Bench Project
Find the right tool
Recommendations
Previous results
Funded by European Commission
Partners:
CYBION Online Business Intelligence
.stiftung digitale-chancen
coordinated by:
INNOVA Technology Transfer & Valorisation
Find us on

Results of the 3rd test cycle, Summer 2014

Ranking for age-group Up to twelve years

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

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

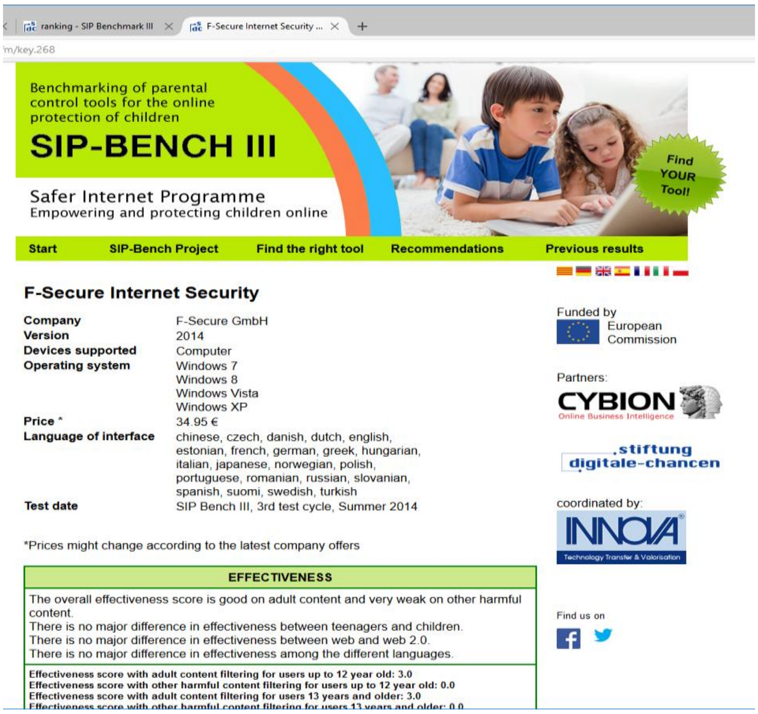
Show list for age-group thirteen years and older in a new window

Tool name	Effectiveness	Usability	Security	Price (€)
F-Secure Internet Security	1.5	2.9	1	34.95
K9 Web Protection	1.1	2.9	3	Free
Mac Os X Parental Controls	1	2.9	2	Free
McAfee All Access	1	3.0	0	109.95
Norton Online Family	1.8	3.3	1	Free
Optenet PC	1.1	2.4	3	39.95
Panda	1.3	2.2	0	71.99
Puresight Owl	2.2	3.1	4	29.00
Qustodio	1.1	3.1	4	Free
Trend Micro Online Guardian	1.1	3.2	0	47.97

Start new selection | Change main selection | Change additional features

The site also provides **individual tool fiches** with more detailed information for target users who are interested in a specific product. Information is provided in a clear and comprehensive way, including practical information such as price, language availability, licence options, etc.

Figure 6 – Tool fiche example


ranking - SIP Benchmark III
F-Secure Internet Security ...
m/key.268
Benchmarking of parental control tools for the online protection of children
SIP-BENCH III
Safer Internet Programme
Empowering and protecting children online
Find YOUR Tool!
Start
SIP-Bench Project
Find the right tool
Recommendations
Previous results
Funded by
European Commission
Partners:
CYBION
Online Business Intelligence
.stiftung digitale-chancen
coordinated by:
INNOVA
Technology Transfer & Valorisation
Find us on

F-Secure Internet Security

Company	F-Secure GmbH
Version	2014
Devices supported	Computer
Operating system	Windows 7 Windows 8 Windows Vista Windows XP
Price *	34.95 €
Language of interface	chinese, czech, danish, dutch, english, estonian, french, german, greek, hungarian, italian, japanese, norwegian, polish, portuguese, romanian, russian, slovanian, spanish, suomi, swedish, turkish
Test date	SIP Bench III, 3rd test cycle, Summer 2014

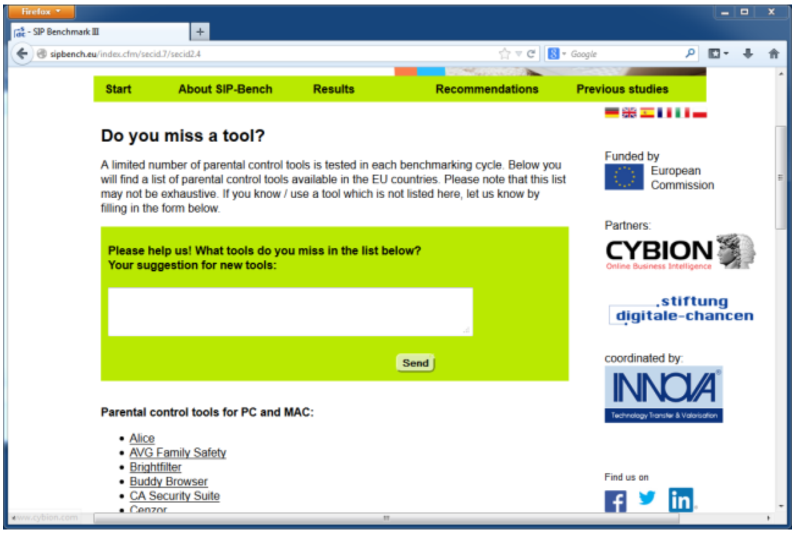
*Prices might change according to the latest company offers

EFFECTIVENESS

The overall effectiveness score is good on adult content and very weak on other harmful content.
There is no major difference in effectiveness between teenagers and children.
There is no major difference in effectiveness between web and web 2.0.
There is no major difference in effectiveness among the different languages.

Effectiveness score with adult content filtering for users up to 12 year old: 3.0
Effectiveness score with other harmful content filtering for users up to 12 year old: 0.0
Effectiveness score with adult content filtering for users 13 years and older: 3.0
Effectiveness score with other harmful content filtering for users 13 years and older: 0.0

The site includes also a Feedback Form that can be used by web site users and visitors to send information on new tools which are not listed in the web site and which could be considered for testing. Information received through the Form has been used by the SIP-BENCH III consortium to update the list of tools.



Do you miss a tool?

A limited number of parental control tools is tested in each benchmarking cycle. Below you will find a list of parental control tools available in the EU countries. Please note that this list may not be exhaustive. If you know / use a tool which is not listed here, let us know by filling in the form below.

Please help us! What tools do you miss in the list below?
Your suggestion for new tools:

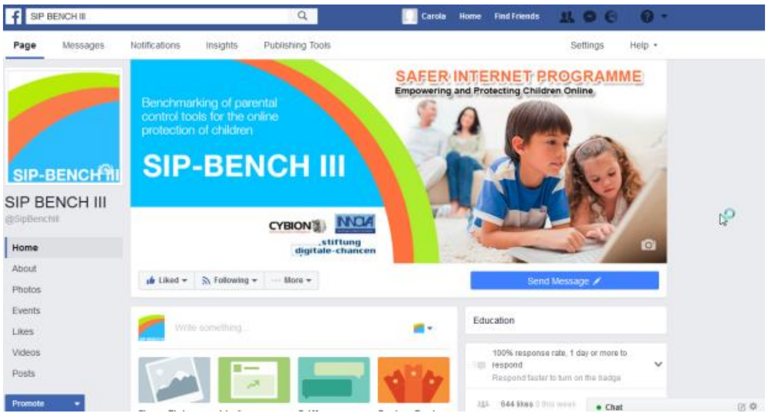
Parental control tools for PC and MAC:

- Alice
- AVG Family Safety
- Brightfilter
- Buddy Browser
- CA Security Suite
- Cenzor

SOCIAL MEDIA

Dissemination through social media has also been effected throughout the study implementation.

A **Facebook account** (https://www.facebook.com/SipBenchIII) has been set up to promote the study via other Facebook accounts linked to children safety online (e.g. Safer Internet Day, Insafe, etc.) and to disseminate tests results after each benchmarking cycle.



Benchmarking of parental control tools for the online protection of children

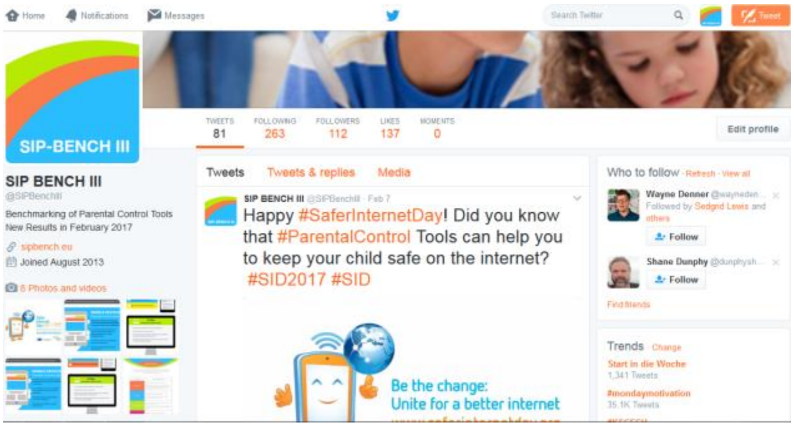
100% response rate, 1 day or more to respond
Respond faster to turn on the badge

The account has been updated 2-3 times a month with information related to children safety online initiatives and blog updates.

Currently the **Facebook** account has over **640 fans**.

A **Twitter** account (https://twitter.com/SIPBenchIII) has also been set up; at the end of the project, the account has **115 followers**. The Twitter account was mainly set up as an additional tool to inform a wider public interested in children-safety-online-related topics, results achieved with the study, upcoming events of interest and workshops related to the project as well as to related topics. Since its set-up, the Twitter account has been used to further support the dissemination of the benchmarking cycles results, to increase visibility of the SIP-BENCH III project website, to send out information on the latest benchmarking results and to invite interested parties in opening discussions related to youngsters' online safety and protection.

Moreover, the Twitter account enables persons to follow a number of active groups and discussion on these topics and to keep abreast of the latest developments.



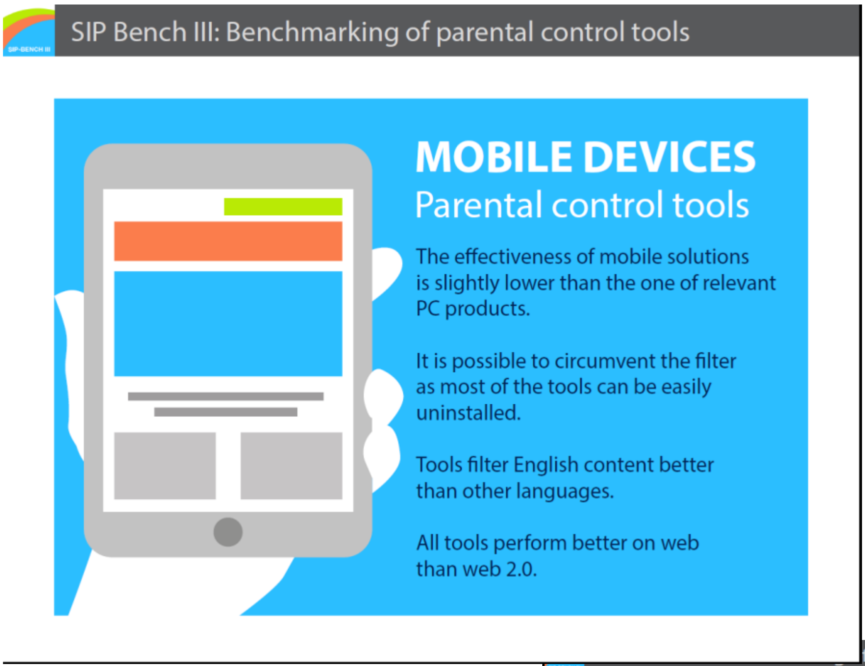
SIP BENCH III
@SIPBenchIII
Benchmarking of Parental Control Tools
New Results in February 2017
sipbench.eu
Joined August 2013
6 Photos and videos

SIP BENCH III @SIPBenchIII · Feb 7
Happy #SaferInternetDay! Did you know that #ParentalControl Tools can help you to keep your child safe on the internet? #SID2017 #SID

Wayne Denner @waynеden... Followed by Sedgnd Lewis and others
Shane Dunphy @dunphysh...

INFOGRAPHICS

For dissemination purposes, infographics have been developed after the first cycle and published through media. Below are some examples.



SIP Bench III: Benchmarking of parental control tools

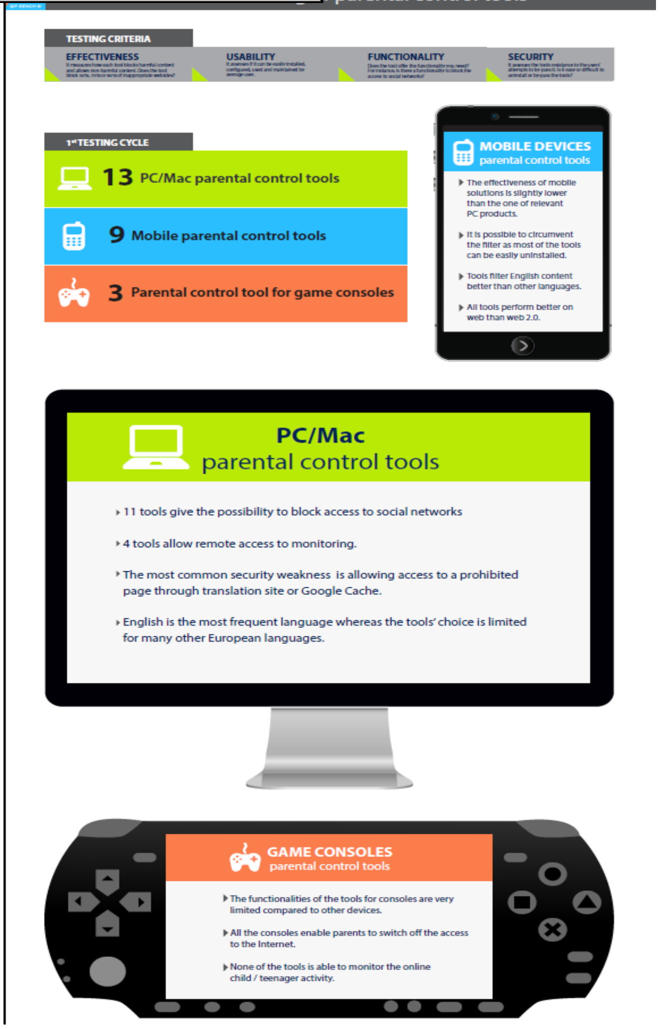
MOBILE DEVICES
Parental control tools

The effectiveness of mobile solutions is slightly lower than the one of relevant PC products.

It is possible to circumvent the filter as most of the tools can be easily uninstalled.

Tools filter English content better than other languages.

All tools perform better on web than web 2.0.



f parental control tools

TESTING CRITERIA

EFFECTIVENESS It measures how each tool blocks harmful content and allows non-harmful content. Does the tool block some, more or most of inappropriate websites?

USABILITY It assesses if it can be easily installed, configured, used and maintained by average user.

FUNCTIONALITY Does the tool offer the functionality you need? For instance, is there a functionality to block the access to social networks?

SECURITY It assesses the tools resistance to the users' attempts to by-pass it. Is it easy or difficult to uninstall or by-pass the tools?

1st TESTING CYCLE

13 PC/Mac parental control tools

9 Mobile parental control tools

3 Parental control tool for game consoles

MOBILE DEVICES
parental control tools

- The effectiveness of mobile solutions is slightly lower than the one of relevant PC products.
- It is possible to circumvent the filter as most of the tools can be easily uninstalled.
- Tools filter English content better than other languages.
- All tools perform better on web than web 2.0.

PC/Mac
parental control tools

- 11 tools give the possibility to block access to social networks
- 4 tools allow remote access to monitoring.
- The most common security weakness is allowing access to a prohibited page through translation site or Google Cache.
- English is the most frequent language whereas the tools' choice is limited for many other European languages.

GAME CONSOLES
parental control tools

- The functionalities of the tools for consoles are very limited compared to other devices.
- All the consoles enable parents to switch off the access to the Internet.
- None of the tools is able to monitor the online child / teenager activity.

WIDER DISSEMINATION

The cycles' test results were disseminated to a broader public through web sites of other initiatives or dissemination tools related to the Safer Internet Programme and online children protection initiatives:

- Safer Internet Centres

- Other EU funded projects under the Safer Internet Programme

- German Federal Family Ministry's initiative "Dialog Internet"

- Internet and children NGOs

- Save the Children mailing list

- Specialised media.

ATTENDANCE TO DEDICATED EVENTS

Finally, attendance at public events has been ensured by the SIP-BENCH III consortium, in particular, the Safer Internet Day which usually takes place in February each year.

Furthermore, three main events were attended by members of the SIP-BENCH III consortium which was an opportunity to disseminate results of the benchmarking study, share views with market stakeholders and policy makers:

- A vendors' workshop held in Brussels in 2014 with the participation of industries, media and EC representatives to assess quality of tools and discuss future developments;

- A workshop with industry and NGOs at the Internet Governance Forum on intelligent risk management in a mobile online environment. The discussion focused on the challenge of building a trusted online environment and how parental control tools can contribute to making the digital environment safe for children.

- The FORUM OF ICT COALITION to be held in Brussels in mid-May 2017. The SIP-BENCH III consortium is expected to present the overall results and main findings of the benchmarking study to representatives from information and communication industry and digital media companies. It will be an opportunity to discuss findings in regard to what technical resources for child protection can achieve.

Table 18 – Events attended

	Conference	Date and venue
1	Safer Internet Day	Editions 2013-2014-2016
2	Vendors Workshop by invitation from the EC	May 6th, 2014, Brussels
3	Internet Governance Forum: WS 154: Intelligent Risk management in a mobile online environment	September 3rd, 2014, Istanbul
4	ICT Coalition meeting	May 16th, 2017, Brussels

4.2. Dissemination of the benchmarking cycles results

Dissemination has been an ongoing task and it was crucial for fulfilling the main objectives of the benchmarking study. The dissemination strategy mainly addressed Safer Internet Centres and other stakeholder potential multipliers towards parents and carers and ensured a European coverage. The Benchmarking Cycle Report has been produced after each cycle, together with an Executive Summary. Both documents have been uploaded to the project website for public access at (http://sipbench.eu/index.cfm/secid.6).

The Benchmarking Cycle Report was accompanied by ranking lists (per age group) and detailed test results by product ('tools fiches'). These were provided in a searchable database via the project website to ensure that parents and other care-givers have an appropriate route to search for a tool most suited to their needs.

The Benchmarking Cycle Reports also include recommendations for parents and software companies.

Cycle results were also published on the consortium members' websites.

In addition, Steering Board Members actively participated in the dissemination activities, publishing press releases on their organisations website and forwarding them to their members.

After each cycle, a short press release in English, French and Polish was prepared and sent to Safer Internet Centres, schools, media, ministries of education, etc. (e.g. for Germany it was done via the Federal Family Ministry).

5. An overview of the tools prices

Prices of parental control tools vary widely. There are **different pricing strategies** followed by vendors. Accordingly, users can search for the tools that best suit their budget and needs.

Some parental control tools are available **free of charge** (e.g. Mac Os X Parental Controls or Norton Family parental control).

There are also many tools that come with a price or a **subscription fee** (e.g. Witigo Parental Filter).

The subscription fee varies from the very cheap tools (e.g. Maxthon Kid-Safe Browser with a fee of 1.40 Euro) to the more expensive tools (WebProtectMe Safe Browser with a fee of 9.9$/month for the premium version). Subscription fees may be required on a monthly or yearly basis and are subject to change. Providers also have special offers on a regular basis.

Tools are **individually priced**. The market pricing changes according to the tool, the number of devices or users in the same family, etc. The price for PC tools, for example, can differ, according to how many devices the tools are installed on

One of the cheapest PC tools is Kaspersky Safe Kids with an annual fee of 14.99 $/year.

Some tools provide **different editions** which are available in the market (for example basic, gold, premium, etc.) and offered at different prices. This offering of edition types expanded further during the benchmarking cycles and made it more difficult to compare the results the tools achieved in the tests.

In some cases, tools offer a **free trial version** for varying periods of time (for example three days, a week, two weeks, a month, etc.) and then a subscription fee (paid-for version) is required for subsequent use (e.g. McAfee Total Protection or Norton Family Premier). When a free version is offered, functionality may be limited. Usually, in such cases, tool providers inform the user that some functions are only available in the full version.

Some tools provide a free version plus a **premium version** offering additional functionalities (e.g. Mobicip Safe Browser). The free version covers the basics, enabling to set rules and time schedules, block pornography and other unsuitable content. If a paid-for version is chosen, it usually adds SMS monitoring, social media features and per-app controls.

There are some tools offering free versions which have quite comprehensive parental control apps (e.g. Qustodio basic).

Most paid-for tools provide various **subscription models** to suit different users' needs. Models include subscriptions for one or more years and also for usage on one or more devices.

Parental control tools can be **stand-alone** tools **or** be part of a **package** of software tools – so called security suites – that often also include virus protection, popup blockers, and other security features. In this latter case, the price may be higher.

6. Overall view of parental control tools' potential to protect children/teenagers

Previous research on the use of parental controls **has not** yet **reached a definite answer** on the **effectiveness** of the tools in reducing online risks to children. Some research supports the effectiveness of preventive software and, in particular, filtering, blocking and monitoring software in reducing unwanted exposure to harmful material. However, the evidence could not be generalised across all ages[16].

Other studies have reported on the **failure** of parental controls to reduce online risks[17].

Knowledge gained within the SIP-BENCH III initiative led to the conclusion that parental control tools can be useful in ensuring protection for children going online especially for the younger age groups. However, parental control tools **cannot** entirely **replace** direct monitoring by parents through both open dialogue and educational paths. Technology cannot be a substitute for direct interaction and mutual trust between the parties.

Parental mediation is essential in ensuring the efficacy of parental control tools. Conversely, well-designed parental controls tools can support parental mediation, for example, coherently-phrased blocking messages referring the child to their parents for advice in case of blocked content. Parental mediation practices may differ according to specific context conditions which may evolve over time (see, for example, the rapidly changing popularity of a particular content or device) and vary between locations (for example, rules can be different for the use of devices at home or in external contexts, e.g. use in the car or at school).

To be effective, parental control tools need to be familiar to and well-managed by parent users. Tools should be family-friendly and safety-enabled.

Nowadays, kids use all types of devices connected to the Internet, for example, toys speaking to the child via an app (Kayla doll). Modern parental control tools must be able to keep up. Therefore, before settling on a particular parental control tool, it is worth checking that it **supports all types of devices** used by the child. Whilst almost all products support Windows, support for Mac OS, Linux, Android, and iOS varies.

As for mobile devices, while iOS on Apple devices offers parental control capabilities, Android does not offer this, so third-party apps are a must. There are many apps in the Android marketplace, so selecting the right app for parents' needs can be a critical activity.

The selection of the most suitable tool should be made based on the functionalities required and the specific purpose of the parental control.

When assessing a parental control tool, different **features** may be **essential** for parents and may guide the tool selection:

- lock access to inappropriate websites in parent-selected categories and work no matter what browser the child uses;
- time-scheduling that lets parents define a weekly schedule for when the child is allowed on the Internet, the computer, or both;
- produce reports that lets parents easily check on the child's online behaviour;

[16] EU Kids Online III, KU Leuven, Belgium, February 2016

[17] Dürager and Livingstone (2012) could not find evidence that parental technical mediation, such as using a filter, could significantly reduce online risks

– allow defining different configurations for different children.

Having viewed the technical characteristics of the analysed parental control tools, the following can be stated in terms of tools' potential.

Different types of devices

In the past, a single parental control tool on the family PC was sufficient. Modern youths, however, use different types of Internet-connected devices, and modern parental control tools must keep up.

Parental control tools categories and specific functions

There are some tools which are ideal for younger kids who would likely not need the device functions and, instead, would use the device for educational apps or digital entertainment. In these cases, some tools let the user create a "sandbox" environment of specific apps and restrict access to the store. The app may also include a browser designed for kids with integrated content filtering.

Other tools may be more ideal for young teenagers who already have their own device and parents can set restrictions on app usage, time use, calls/texts.

Some tools allow for browser restrictions as well as app management, via remote access, meaning that the app's restrictions can be managed either on the device itself or configured remotely through a web browser, either on a computer or on another device. Some apps also include the option of a monitoring app which can be installed on a second device. Such apps are ideal for controlling the content accessed by a mobile device, particularly one in the hands of a teen. Monitoring capability may be allowed for texts, calls and usage time.

Filtering

The principal way in which parental control tools clean up the Internet for kids is by **filtering** out websites with explicit material and other inappropriate content.

The default **Web filtering** blocks harmful material. Parents are also allowed to customise the filtering based on what they think is appropriate for their child. The filtering degree differs from tool to tool. Many tools have a range of filtering pre-sets based on how old the child is. Some tools (like Net-Nanny) have an option for masking curse words instead of blocking the whole page, or even allowing the blocking of specific content. In addition to seeing what sites the children are visiting, parental control tools also allow exceptions for blocked websites.

Time setting

Time-setting to schedule access is another very common feature. Some applications let parents set a weekly schedule for Internet access, some control computer use in general, and some offer both as choices. A daily or weekly cap on Internet usage can also be useful.

Remote Notification and Management

With most parental control tools, parents can opt to receive notification via text or email when children try to visit blocked sites, make a post using iffy language, or otherwise bend the rules. Some tools record websites a child has visited. Others display a warning message when a child visits a certain website. Curbi, Mobicip, Parentsaround (Mobile), Surfie are all tools tested in fourth SIP-BENCH III cycle that offer a second App, in which an earning message could be displayed.

Some of these tools let children remotely request parental override to unblock a particular site, or get extra time online to finish homework.

In most cases, parents manage parental control tools by logging in to an online console. From the console, parents can tweak settings, review activity reports, or respond to a child's override request.

BLOCKING APPS

Most parental control tools allow parents to **block** usage of **certain apps** on devices used by their children. Some block new apps from even being installed before a parent consents, while others can only blacklist apps after they have been downloaded. An easy solution is to simply block the Google Play store (or any other Android app store) and only allow kids to install new apps once they have obtained the parents' permission. Along with stopping kids from downloading inappropriate apps, this method also protects them against malware.

SOCIAL MEDIA TRACKING AND FILTERING

As the children get older, content filtering may start to seem worthless and parents may be much more worried about interaction with the wide world (e.g. friends on social media). Social media filtering is also an important feature of parental control tools. Social networks like Facebook and Twitter can open kids up to a lot of potential emotional or even physical abuse. For most mobile and some PC tools, parents can choose to entirely block those apps, but many control tools, such as Norton and Qustodio, allow for more nuanced social media monitoring. These features include viewing logged conversations or blocking specific questionable contacts. For more advanced social media protection, there are also dedicated tools such as Net Nanny Social.

In most cases, the installation of social media tracking requires parents to know their children's login credentials, or the children would have to log in and install the tracker's app.

ADVANCED FEATURES

When parents get beyond the basics, parental control tools may incorporate many advanced features. Some limit access to games, TV shows, and movies based on ratings. Some let parents control just who the kids can chat with via various instant messaging systems. Blocking specific applications is another advanced feature, as is forcing Safe Search on popular search portals. Advanced versions of standard features are also available.

Availability of features may depend on which version of the tool is chosen.

At a general level, the basic criteria parents may apply in selecting the parental control tool are the following:

- **Feature Set:** Variety of features available as well as their usefulness. The top tools not only monitor access and time, but also support restrictions on additional items such as programmes, games, chat and downloads and provide reporting (this can be checked under tests of Functionalities).

- **Ease of Use:** This evaluates how easy a programme is to use (reference can be made to usability scores and usage).

- **Ease of Installation/Setup:** The best programmes are quick to download and do not create problems during the download or setup process (reference can be made to the scores obtained for Usability-Installation and Configuration).

- **Technical Support/Help:** Tool support is important, that is if the product provides a user guide as well as customer support contact methods such as email forms, telephone numbers or online documentation such as FAQs, forums and tutorials.

- **Time Control Effectiveness:** Parental time control tools should control time limits and access to the computer, internet or other applications precisely as the administrator (parents) set them.

WHERE/WHEN DO TOOLS WORK WELL?

Parents as users of the tools bring varied needs to the table:

- Some might simply want to ensure that their children do not overuse their devices and spend too much time online. In this case, any tool providing a time limit functionality might suffice for their needs.

- In other cases, parents require a simple solution for the filtering of content if they are not very computer-literate and do not want to deal with complex configuration procedures. Here, a simple tool with few options may be best for them.

- For parents who are technically-skilled and would like a choice of filtering by categories and/or black and white list in addition to some extended features such as social media monitoring, extended reporting functions and time limitations, a more elaborate tool would be best.

Tools always work best if the respective users make sure that the chosen tool is suited to their needs and also anticipates future needs, for example, more children in a household or the changing needs which arise when children grow older.

7. The identified emerging trends

Parental control tools have been developed to address specific needs and concerns related to protection of children and youngsters going online, a field that, in the last few years, has seen major progress and changes. In technological terms, this is due to progress made in developing new services and devices and shaping their features and in offering a variety of tool functionalities which are evolving over time. This is also due to changing trends in attitudes, user behaviour (both parents and children/youths) and use of parental control tools. Some trends can be identified as follows[18].

a. Technology developments and new devices to access the Internet

The ICT sector is evolving with very fast innovation cycles and new technologies can have a significant impact on the society and affect use patterns. **Smart devices**, the exploitation of **IoT models**, a broad range of innovative products, functionalities within platforms available for children and youths, and the rapidly increasing **interconnectivity** of devices and platforms, are all having a marked effect on people's everyday lives and the way in which users access the Internet and take advantage of its potential.

The new smart devices and the Internet of Things are meant to make life easier and more convenient, but implications for children's safety should be considered.

In many instances, these devices and platforms are designed to target a broad spectrum of potential users without appropriately considering the **'age' issue**. It is also true to say that, in many cases, children do not use devices and applications that are exclusively designed for their age group. Instead, they have **access** to those **developed for adults**. Addressing adults in addition to younger users in the same market may have unforeseen consequences since the use of these devices and platforms may be beneficial but also detrimental to children and youths. Not all internet use, in fact, results in benefits: the chance of children obtaining any benefit depends on their age, gender and socio-economic status, on how their parents support them, and on the positive content available to them. Not all risk, however, result in harm: the chance of a child being upset or harmed by online experiences depends partly on their resilience and resources to cope with what happens on the Internet.

b. Changing approach of children and youths accessing the Internet

Changes also occur in the way children and youths access the Internet and all the opportunities it offers.

Most young people and children live in a **digital home** where they grow up using a wide range of interconnected devices for various activities, i.e. learning and entertainment, communicating with family and friends, following hobbies and interests. **The Internet** is **deeply integrated** in youngsters' lives, with a majority of them using it daily while progressively increasing their digital skills. Ofcom's latest report[19], which contains statistics and an analysis of the UK communications sector, shows that children's internet use has reached record highs, with young people aged 5-15 spending around 15 hours each week online and for the first time exceeding time spent watching TV.

ICTs can transform children's learning opportunities and experiences and their access to knowledge and resources. Children are going online at an ever-younger age and using the Internet on a regular basis. **Learning**

[18] Larger parts of chapter 7 and 8 are based on findings of studies published in the framework of other EC funded projects or analysis carried out in the field by other authors. Please refer for more details to the bibliography at the end of this report. For the content of chapter 7, more specifically, reference is made to the report '*Let's play it safe*', elaborated by the SIP-BENCH III Steering Board member Jutta Croll for the ICT-Coalition for Children Online in 2016, see:

http://www.ictcoalition.eu/news/100/Let%25E2%2580%2599s_Play_it_Safe%253AEmerging_Trends_and_Evolutions_in_ICT_services.

[19] Communications Market Report 2016, August 2016

by observation in the domestic and social environment is a kind of informal learning for children which comes naturally, along with the use of digital devices.

Digital devices are more widespread among children than ever, including the very young. According to the Ofcom report, a third (34 %) of pre-schoolers (aged 3-4) own their own media device, such as a tablet or games console.

Furthermore, the usage of online services on **portable devices** with **touch screens** (smartphones, tablets) is increasing rapidly among the younger age group but also among children, who were accustomed to previously going online mainly with desktop PCs and laptops[20].

Cameras are now embedded in nearly all devices, therefore always at hand and always connected to the Internet, thus presenting the risk of children taking pictures and publishing them directly.

Live streaming has become very popular. Safety measures usually applied in chat rooms are less effective on live video-streaming services because there is no time delay and communication flows between the person streaming the video and the audience as if they were in the same room talking to each other, face-to-face.

c. From content-related to contact-related risks

Furthermore, it must be pointed out that children are increasingly becoming creators of online content (texts, images, animations, blogs, applications and videos). This trend should combine the need of youngsters to access opportunities to learn, to create, and share content with parents' need to avoid harmful, misleading and problematic access to the Internet.

Risks associated with the above changes call for a new focus which moves from content-related to **contact-related risks**. To address these potential risks, it is necessary to ensure a constant monitoring, easily-understood reporting mechanisms, prompt handling of reports and feedback to the users.

d. Parental mediation new model

In this context, a **new model** of **parental mediation** is emerging requiring increased digital literacy from parents who are often learners themselves.

Accordingly, what is considered a technological issue needs to be integrated with **social, cultural** and **psychological aspects;** these aspects should be combined to really address the issue of online activity related risks for youngsters.

In addition to digital literacy which should be expanded for both parents and young users, a safer and more skilled use should be encouraged.

e. A legal and normative changing framework

On the other hand, there is also an **evolution** in the regulatory framework for the protection of minors and in the **legal and normative aspect** which industry and producers should comply with. This framework recognises children as holders of human rights equal to adults (rights to provision for their development; rights to protection from threats to children's dignity, survival and development; rights of participation and being an active part of the society)[21]. The framework provides also for legal obligations and guidelines to be followed

[20] "Assessment of the Emerging Trends and Evolutions in ICT Services". *White Paper for the ICT Coalition for Children Online.* Annex B.1 - Analysis of User Behaviour in Regard to New Products and Services, Taking into Account Changes in Age Groups, Jutta Croll, January 2016

[21] "*One in Three: Internet Governance and Children's Rights*", Global Commission of Internet Governance, Sonia Livingstone, John Carr and Jasmina Byrne, PAPER SERIES: NO. 22 — November 2015

(e.g. guidelines for privacy). The UN-Convention on the Rights of the Child puts special emphasis on children's rights and demands that ratifying states implement the Convention's 54 articles. With the so-called Sofia Strategy adopted by the Council of Europe in April 2016, children's rights in the digital environment have been given special focus in the implementation process[22].

f. Increasing creation and distribution of user-generated content

One of the main trends seen in the last few years is the increase and rapid distribution of **user-generated content** which is of particular concern.

There are a variety of applications used for going online. The traditional browser is losing its relevance and most of the time is spent on social media/new apps (e.g. WhatsApp, Facebook, YouTube, etc.) which are becoming much more important.

YouTube, for example, is one of the most popular online destinations for children to watch content, with around three-quarters (73 %) of those aged 5-15 using the video site. It is also a hit with pre-schoolers with 37 % regularly watching YouTube videos, who typically pick 'TV content' such as cartoons and mini-movies[23].

The frequency of **usage of social media** is increasing aided by the ease of use of smartphones. Most often, kids are visiting web 2.0 sites, while the classical www is losing its relevance.

However, traditional filters are not able to filter inside such apps and these **filter tools** are not able to filter most of the content children and youngsters are visiting nowadays. No filtering system is able to filter deep links inside a platform (because the URL is encoded also). Therefore, it is possible to block YouTube completely, but not a specific video. Also, no filter can filter content which is received via an app, hence, effective filtering of the end-user is possible only to a certain extent.

Accordingly, **big platforms** should accept **responsibility** for the content they provide and develop measures to make accounts safe for children and youngsters ("Safety by design")[24].

Also, preventative approaches should adapt to the evolving opportunities offered by the technological improvements. The role played by parents, schools and peers, is essential as well as the function of the national requirements for regulation, content provision, cultural values and the education system.

Engaged parenting still appears to be the main solution for many parents. Even if efforts are made to promote more wide-spread usage of parental control tools, many parents continue to believe that education and parenting represent the first and best approach to deal with concerns about objectionable content or troubling communications.

g. Smart home and parental control tools

When going beyond the basics, parental control systems begin to diverge, with many advanced features. Some of them limit access to games, TV shows, and movies, based on ratings. Some let parents control just who the kids can chat with via various instant messaging systems. Blocking specific applications is another advanced feature, as is forcing Safe Search on popular search portals. More advanced versions of standard features may also be found. For example, the best content filters don't use only a database of categories. They analyse page content in real time so that, for example, they can allow access to a short story site but block harmful content.

[22] http://www.coe.int/en/web/children/children-s-strategy

[23] Communications Market Report 2016, August 2016

[24] "Let's Play it Safe. Children and Youths in the Digital World", Jutta Croll, January 2016

Modern kids use all kinds of Internet-connected devices and modern parental control systems must adapt. This applies especially in a smart home which is becoming a commonplace household model.

Before settling on a particular parental control utility, it would be useful to ensure that it supports all the device types found in the household and that there are no limits to the number of child profiles or devices to be monitored.

If getting parental control coverage installed on each device is seen as too difficult, the installation of a **whole-network solution** could be considered. These systems perform content filtering at the router level, so settings affect every device on the network. These systems do not ensure the same fine level of control and detailed monitoring that can be obtained with a local agent on each device, but in certain cases, it is functional.

In some cases, routers may also be used like invisible guardians watching over the kids ('Routerhino' or 'Starry Station'), including parental controls. They are usually able to block access to adult sites, social networks and chat applications. They also filter search engine results with Google or Bing, and videos on YouTube, thus ensuring safety. They are usually easy to set up, in some cases allowing monitoring through a touchscreen on the parent's device, as well as allowing additional devices to be added and monitored. They filter content, pause the internet (for one device or all) and limit access to specific apps.

Also, more recently, there are new tools being developed. For example, tools for specific needs children/youths might have. One example is tools for autistic children (e.g. ZAC Browser https://zacbrowser.com/ which reduces the number of user interface controls and removes access to much of the Web in order to simplify the experience for autistic children).

8. Recommendations

The proliferation of smart digital devices in families and households can potentially bring risks and harm along with interconnectivity. In this new social environment, awareness-raising among parents and other adults in charge of minors, including teachers, it is extremely important to have them appropriately-enabled to protect children and youngsters. At the same time, education for young Internet users is also necessary to prevent Internet misuse or harms and threats that may result from online activities.

Prevention, however, may come not only from users. Industry and tool providers should likewise be aware and be involved in a process that is aimed at creating a safe online environment for young users.

Similarly, action and initiative is required at policy level. The effects of fast innovation cycles can be properly tackled, creating a more harmless, overall framework and preventing potential dangers and threats related to the broad range of opportunities of the digital world.

Below, some recommendations have been drawn up aimed at the main target groups, namely parents, tool providers and policy makers.

Recommendations have been formulated based on:

- ✓ The major **lessons learnt** at the end of the SIP-BENCH III benchmarking study;
- ✓ The **inputs and advice** received from the Steering Board members;
- ✓ The analysis of the **main findings** of other studies conducted at EU level in the same field[25].

Recommendations for parents provide suggestions on how to integrate the use of parental control tools in parenting practices.

For tool providers and policy makers, proposals are made to have production strategies and policy making aligned to emerging needs and trends.

[25] In particular recommendations are based on findings of the report 'Let's play it safe', elaborated by the SIP-BENCH III Steering Board member Jutta Croll for the ICT-Coalition in 2016, see: http://www.ictcoalition.eu/news/100/Let%25E2%2580%2599s_Play_it_Safe%253AEmerging_Trends_and_Evolutions_in_ICT_services.

8.1. Parents

☞ Parental control tools can be used by parents in addition to open dialogue and direct communication with children and teenagers

Parental controls are useful tools to protect children and youngsters going online. However, they cannot be regarded as a substitute for open communication and dialogue between parents and children about:

- restrictions on what is allowed and for how long (what, when and how long they can play or go online);
- which games and apps they may enjoy/use;
- with whom they can play games or interact online;
- why it is important not to share personal information (such as address, school, family information, and weekly planning) and
- how to deal with inappropriate behaviour online by usual or new contacts.

To ensure this, it may be beneficial to communicate regularly with children about what problems they may encounter while surfing on the web or enjoying apps.

It is also useful to be clear about expectations and rules relating to youngsters' online behaviour.

Parental controls should be understood as facilitators for parent-child discussions as to what entails appropriate and inappropriate content and behaviours.

When using parental control tools, it is important to know that they work best when used openly and honestly in partnership with children. A monitoring or mediating approach may be more beneficial to children.

Where practical, it would be a good idea to keep the computer or game systems in a common area in the household so that any activity is plain to see. This may create a relaxed, interactive atmosphere and children may be stimulated to ask questions and have conversations there and then on topics related to their online activities.

☞ A transparent approach from parents would enhance the children's' understanding of the motives of why parental controls are used

Parents may start supporting children's exploration of the Internet from an early age and inform them of the benefits and the risks that the Internet offers. Discussing online safety from an early age may sustain the child's growth in a new digital environment, while building awareness of the opportunities and threats of going online and accessing the Web.

It is advisable for parents to spend time with kids on these issues.

A special focus may be placed on enhancing children's opportunities for improving digital skills and accessing information and entertainment apps through a well-balanced use of the Internet, as well as developing a reaction capacity and resilience to potential harm which may result from the online activity.

What is useful to address is not only the 'what' (what is risky, what should be avoided, what is inappropriate for a child, etc.) but also the 'why' (why avoid certain types of usage or behave in a certain way when online). In fact, children may well learn the lesson of what is risky or harmful but not why. Explanations may be conveyed with appropriate age-differentiated messages.

The educational path should find a balance between the parents' concerns of potential risks and harms and encouraging children to engage in fun activities and educational opportunities and to benefit from positive content.

☞ Ensure a balance between digital and non-digital activities

According to the recent '*JIM 2016*' study[26] digital homework time increases in line with the increasing age of young people. Parents may spend more time with growing children in order to explain to them the importance of an appropriate balance between digital and non-digital activities in their daily planning.

☞ A balance between parents' monitoring and the wish of youngsters to benefit from the opportunities offered by the access to the Internet would be beneficial

It is advisable that parents' monitoring is appropriately balanced with the potential benefits deriving from online activities. Digital media provides youngsters with opportunities for the acquisition of knowledge, assembly and association, participation and play.

Children easily adapt to new functionalities and respond with the acquisition of skills to handle potential threats. This adaptability can function as a self-protective shield embedded in a broader concept of protection, with supervision and education being balanced.

Children are also good at circumnavigating the tools' functions and are often able to quickly uninstall or deactivate filters. An open dialogue could be the best way to explain why filtering is necessary.

☞ Be aware of ethical challenges and act on a privacy-wise basis

It would be useful if parents discuss parental control settings with their child, as these settings will eventually affect children's future (online) activities and privacy. Parents should be aware of the far-reaching ethical consequences that the use of parental controls may present beyond the family unit. Monitoring children's online behaviour may disclose information about children's friends and other individuals.

☞ Filtering is only part of the solution

No filter of parental control tools is 100 % effective and many of the dangers that young people face online are because of their own behaviour and that of others. It is therefore important to talk to children about staying safe online and making sure they know that they can turn to parents if they get into any difficulty.

In addition to the more general advice above, some indications can be provided on technical aspects to guide parents in the selection and installation of tools.

☞ Ensure that the parental control tool supports the devices used

Before settling on a particular parental control tool, it would be helpful to ensure that it supports the types of device used in the household. While many products support Windows, support for Mac OS, Linux, Android, and iOS varies. It is also advisable to check if there is any limit on the number of child profiles or

[26] '*JIM 2016. Jugend, Information, (Multi-) Media*', Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland, February 2017

devices.

☞ Consider devices with their own parental controls

In addition to content filtering offered by ISP, many devices such as game consoles, smartphones and tablets have their own parental controls, for example to limit spending or to restrict access to apps, based on age rating. Likewise, many web browsers have built-in tools and features to help control the kinds of content users can view.

☞ Use the most updated version of the operating system with embedded tools

Microsoft's Windows and Apple's Mac OS, come with robust built-in parental controls. To obtain the most benefits, parents need to keep an existing Windows version up to date with the monthly security updates (e.g. most updated version of Win7 or Win10), and each user must log in under his or her profile.

☞ Learn how to set restrictions in the browsers

Browsers, for example, Mozilla Firefox, Google Chrome, and Apple Safari, are the software browsers more frequently used to surf the Internet. Each one offers different ways of filtering out websites. It is helpful to learn how to set restrictions in the browser. Browsers are free, but if there is more than one on the machine, it is necessary to enable filters on all of them. Some browsers are especially designed to foster a safe browsing experience, for example Mobicip, which is available for mobile devices as well as desktop computers.

☞ Protect the settings of parental control tools

The tools may require the creation of a password/pin to protect the settings, thus preventing children from making changes. It is crucial that parents make the password/pin something that children will not be able to guess, otherwise the tool will be of no use. Note that if the child or teen does a “factory reset” of the device, it will erase all the downloaded tools and the associated restrictions. Although it does seem like an extreme measure simply to remove parental restrictions, parents should be aware that the child can do this. It would be important to have an agreement with them and set family rules regarding the responsible and safe use of the devices.

☞ Prevent uninstallation of parental control tools

To prevent tools uninstallation, it would be necessary to:

- Disable the access to control panel (Windows)
- Disable the access to AppStore (in case of iOs devices)
- Install the tool with a proper user (i.e. root user on unix-like systems)
- Restrict the permissions (in case of Android devices)
- Follow and read carefully the vendor instructions.

☞ Selection of parental control tools according to the children age

Full-featured parental-control tools, such as ‘Qustodio’, allow parents to block websites, impose screen-time limits, and monitor online activity (for example, which sites your kid visits) on their devices. Several of these tools are part of a security suite and also offer added security against malware and viruses and send a summary of what the kid does online.
They are good for kids of all ages and especially kids who need a lot of support in following parents’ rules. Some mobile devices come with basic parental controls but the options vary a lot. Some apps can also be downloaded from the App Store or Play Store to track and control online activity, including text messaging and social media. To monitor kids’ social media accounts, parents need their passwords and user names. Parental control tools in this case are more suitable for younger kids. Once kids get older, they will either resist any attempt to limit their access or simply figure out a way to defeat what parents have restricted.

☞ Use "walled gardens" tools for very young kids

Kids' browsers or the sometimes so called "walled gardens" are protected environments that fill up the entire screen (so kids cannot click out of them). They typically offer games, preapproved websites, email, and various activities. Examples include: Zoodles and MagicDesktop (Windows), Maxthon (Android) and Surfgarten (iOS). They sometimes display ads or promotional content. They are good for younger kids but limiting for older kids who need (or are allowed) greater access to the wider Web.

☞ Use a combination of tools to enhance overall effectiveness

Parental control tools vary in terms of their capabilities and areas of performance. It could be useful to use a combination of apps and software for an effective and more comprehensive solution. Tools can be used which ensure complementary functionalities, for example, adopting apps that can filter content, but also monitor usage and online activity, would be more effective.

☞ Efficacy of the tools depends on parents’ ability to override the tools limitations

The efficacy of the tools, in some cases, also depends on the ability of parents to override the tools limitations, i.e. when a tool does not allow restricting access to the Internet completely. In some tools parents can achieve this by setting the time restriction for Internet access to zero minutes. Although some parents might discover this alternative route to their intended destination, this could not be called a good application of the tool.

Parents’ involvement in the tool configuration process is a crucial step for tool efficacy.

8.2. Tool providers

☞ Design the next generation of tools following a safety–by-design approach

A careful analysis may be useful for the design of the next generation of parental controls. This in turn, may inspire industry. Safety-by-design should be a guiding principle in the development process. This is true particularly when new features and functionalities are integrated in existing devices which have been designed as safe. In this case, the option of disabling specific features/functionalities that could cause problems in combination with other features/functionalities could be an alternative consideration.

☞ Children should be regarded as a special group of users, especially for new devices

The integration of innovative features in new devices should take into account safety requirements, especially when users are children who are to be regarded as a special group of users.

☞ Ease the handling of parental control tools

Handling of parental control tools should be made easier. They should work efficiently across operating systems and devices. Parental control tool interfaces, both for desktop and mobile devices, should be made user-friendly. Downloading, installation and configuration of settings should be simplified so as to be easily dealt with by parents and other adult caregivers with differing digital skills and capabilities.

☞ Focus on digital literacy development in families with children

Simple guidelines could be developed by tool providers to 'educate' parents on the importance of online safety for their children and take advantage of parental control tools functionalities.

☞ Ensure mutual learning and joint engagement

The next generation of parental control tools should provide more than setting limits. They should also support parents in the process of mutual learning and joint engagement.

☞ Building resilience

Protective measures should also entail solutions that help children build resilience to cope with the harm and risks they may encounter while undertaking their online activities.

☞ Ensure a broader range of tools functionalities

With innovation spreading and the diffusion of IoT applications and interoperability, a broader range of functionalities offered by parental control tools can be guaranteed by producers.

☞ Allow for content classification across devices and means of access to the Internet

Content classification based on clear and consistent standards needs to be applicable regardless of the platform and device that provide access to the Internet and its content, including mobile devices as well as PCs and smart TVs. Tools should be usable with different devices. They should not be conceived for a specific and single use.

☞ Define minimum functionalities and blocking requirements

Minimum criteria for the range of functionalities and blocking capacity of parental control tools may be established as the basic features to be integrated in new products.

☞ Combine different tools

An interesting option would be to combine different tools so as to take advantage of different features and functionalities. Xooloo is an interesting example in this case. The tool can create a child-shaped environment and be combined with other tools. Parental control tools can be used in combination with blocking software, for example. A combination could occur for example among Xooloo and Maxthon Kids-Safe.

☞ Configuration should be allowed on the basis of the user's environment

Configuration should be well-designed taking into account different users' environments i.e. more skilled users can easily deal with it whilst less skilled users may be not and could skip configuration thus potentially impairing the effectiveness of the filtering process.

☞ Focus on Web 2.0 and user-generated content

With growing Web 2.0 (blogs, forums, video streaming platforms, social networking), the risk of children and youngsters coming into contact with inappropriate material produced by “unchecked” sources is increasing. Furthermore, user-generated content is spreading on the Internet. At present, tools present lower effectiveness with user-generated and Web 2.0 content or even fail completely. Such content in fact is not easy to filter with traditional techniques (black lists and URL filtering). Content, in this case, evolves rapidly, is personalised by users, includes more multimedia with little textual information, is often outbound content. Tool providers should place particular focus on this area when developing new products. Greater capabilities of parental control tools both in handling and blocking user-generated content should be ensured.

☞ Dataset sharing can increase protection

Tool providers may share datasets, for example at EU level. This could create a common area of action and contribute to ensuring more effective protection potential.

☞ Introduce some standardisation

Some standardisation may be warranted in designing the tools. For example, standardisation in the notification processes, creation of a shared vocabulary among web page editors which allow for a better filtering through tags, standardise categories for topic filtering.

☞ Allow uninstallation prevention

Some tools can be uninstalled and closed without a password. This should not happen as it makes it easier for children and youths to find a way around parental controls.

☞ Facilitate access to instructions

For some tools, it is not easy to find instructions and guidance on how to deal with the tools. Simplification and support should be ensured for all products.

☞ Adapt tools to growing expectations from users

Expectations from users are growing and tools should be able to keep up with this challenge. A more integrated approach between production features and users’ requirements may be expected.

☞ Align production strategies to emerging needs and trends

In order to better adapt their products to users’ expectations and needs, industry should, in their production strategies, take cognisance of guidelines issued by organisations - both at EU and international levels - that not only monitor children safety issues but also produce studies on emerging needs and trends.

8.3. Policy Makers

☞ Education and awareness-building may help the uptake of parental control tools

Education and awareness-building efforts might help increase the uptake of parental control tools. Many parents may need support to fulfil their education and parenting role as a first ‘protection entity’ which should ensure child safety, especially for the youngest group (0 to 9 years).

☞ Promote a wider awareness building and communication strategy

Research shows that parents are often not aware of parental control tools’ potential benefits. Effective information and communication may be further pursued at EU level. Actions at EU Member States level may also be useful in targeting parents and professional educators. Information campaigns may be integrated with vocational programmes addressing such categories.

☞ Guidance should be provided to parents on a continuous basis

In order to increase parents' and caregivers' appreciation of online parental controls, it would be useful to continually provide means for better understanding the functionalities as well as the limitations of parental controls, which are continuously evolving, as well as guiding families on how to use these tools wisely. A continuous guide for parental control tools users may be useful.

☞ Promote studies to detect and monitor emerging needs of families and users

Studies which constantly monitor needs and requirements for online safety may be useful for promoting appropriately-backed policies in this field. Technological enhancements and innovations which change and affect the needs of families should be identified and monitored on an ongoing basis. In particular, exploring ways in which parents can foster more responsible internet use within their family could be studied.

☞ Boost discussion on online opportunities and threats

Promoting family discussion on online opportunities children and parents can benefit from, but also the risks they want to avoid and the strategies they would like to see put in place to achieve both, should be topics of discussion promoted at public level.

There are gaps in understanding the full range of online risks which children are exposed to and insufficient awareness of which children are particularly vulnerable to such harm.

It would be useful to focus on risks, but also on opportunities to promote a scenario where, in future, children can safely benefit from Internet opportunities.

Empowering children online, in a safe digital environment, should be a major objective to be pursued at public level.

☞ Pursue standardisation of content classification

It would be appropriate to standardise content classification across countries and across stakeholder groups and define what is appropriate and what is inappropriate for children, in order to define and align suitable protective measures. This could be beneficial in the market of parental control systems where many companies operate at international level.

☞ Promote research to target policy instruments in order to address uneven access for geographical and cultural reasons

Despite the rapid rise in access to online devices, there is uneven access across countries, specific areas within countries and within different cultural contexts. Opportunities to access innovative devices are not equally spread among countries and areas, even at EU level. A better understanding of this distribution would be useful to better target policy instruments and intervene where necessary.

Equal opportunities should also be ensured across countries and national factors. In this regard, specific research would be useful.

☞ Focus on emerging technologies and user-generated content-related issues

A particular focus for future policy-making may be the increased relevance of user-generated content in online activities for young people, especially with the growing access to social media and social platforms in everyday life. Despite parental control tools performance is improving slightly, filtering user-generated content remains a challenge. While most parental control tools enable parents to block access to harmful websites, they are less effective at filtering web 2.0 content (such as social networking sites or blogs). User-generated content (mainly Facebook and YouTube) represents a real challenge, both for parents and software producers, as traditional filtering techniques fail to achieve good results.

For future programmes, the Internet of Things and interoperability issues must be taken into account with regard to children’s safety when using these types of connected devices and toys.

Furthermore, it would be useful to look again at game consoles, since the new generation of these products will be more interactive.

Also, streaming services may be a target focus.

☞ Research how to improve supervision and resilience

Research on how to improve parents’ supervision, on one hand, and young users’ capacity to react and face online risks and harmful content autonomously, on the other hand, could be useful. Combining these two aspects could create more effective approaches to online safety issues. The main findings of the research could be addressed through specific measures and initiatives.

☞ Allow for continuous monitoring and benchmarking

The SIB-BENCH III benchmarking study has been an opportunity to test available parental control systems available in the market and provide an independent technical assessment on their performance and potential contribution to increasing safety online. Results have been publicly showed and target stakeholders have benefited from such findings. The attention generated after the publication of benchmarking results indicates the interest of the target public in the analysis and assessment of the testing cycles. It would be useful to have such benchmarking exercises as a continuous initiative to keep up with technical developments and innovations, allow for monitoring and comparison of performance of tools over time and follow improvements in the market.

9. Conclusions

Today, accessing the Internet has become an essential part of our daily lives to access all the opportunities it offers, stay updated and simplify many of our everyday tasks.

Our lives are also continuously shaped by technological innovation and evolution in tools and instruments which support us in our working and household contexts.

As we have seen throughout the whole report, all this affects the life of children and youngsters. From an early age, children live in a digital home and grow up using a wide range of interconnected devices for various activities, e.g. learning and entertainment, communicating with family and friends, hobbies and pastimes.

Their thoughts, creativity and fantasies are stimulated by interaction with such devices but their perception of life is also markedly affected by the experiences they have on the Web and through their online activities.

There is no doubt that access to such a wide range of opportunities may be beneficial and contribute to children's growth. However, the Internet has also a darker side and this is a potential threat, especially for young people and children who are not sufficiently aware of what is behind some undetected risks. Caution is necessary since threats and risks are emerging because of the all-embracing digital environment.

In this context, it is advisable for parents to pay particular attention to their children accessing and interacting on the Web. Protecting children who go online has become a **major challenge**. Parents should choose the right and most effective approach and strategy to protect their children and this is not an easy task without informed and proper support.

Firstly, **awareness-building** and **knowledge dissemination** are the most important initiatives to create an educated environment and enable informed decisions from parents.

Secondly, **rules** should be fixed in a **market** that offers a wide range of products supporting parental control tasks. **Content classification** would greatly support the improvement of tools, allowing for **standardised procedures** across countries and different target groups.

Thirdly, it would be helpful to **monitor** the evolution of users' **needs and requirements** by involving tool providers who can be inspired in the design of the next generation of parental controls. **Safety-by-design** should be a guiding principle in the development process. This should occur particularly when new features and functionalities are integrated in existing devices.

To assist parents in this objective, creating a **multi-stakeholder approach** by involving industry and policy-makers together with users as well as generating design-shared strategies, with potential impact on all parties concerned, would be helpful.

In this regard, a **family-centred approach** should be favoured. Family needs and objectives should be the foundation of both the design of new tools at industry level and the objective of policy strategies at policy level.

Tools should ensure safety according to users' needs. The market should not offer products which do not properly address the specific requirements of families.

Another important aspect to consider is **children** and **youngsters** as a category of people with their own **independent rights** that should be recognised and appropriately addressed. While innovation is a key priority for Internet, it must be considered that any technological enhancement implies effects on young users who need adequate protection and safety.

By testing a selected number of parental control tools, the **SIP-BENCH III** benchmarking study reached results that show some **major findings**.

- Performance **results** of the tested tools over the four cycles are quite **similar**. This suggests that no major improvements have been made over the three-year period and performance evolution demonstrates a steady trend.

- The **functionality coverage for the tools tested** is quite good, but it needs to be further developed to address new types of content and devices.

- Installation is usually quite simple, but **configuration** and customisation to parents' needs is sometimes **complex** and requires specific skills and ability.

- Parental tools are often **not easy to use** and **monitoring** is often not an easy task.

- The overall **effectiveness** is low for both PC and mobile tools.

- **Security** is still **problematic** for many tools. Some of them may be uninstalled even without a password.

- User-generated content is badly filtered.

- Filtering works well with **English** language content but it is less effective with other languages.

Based on these results, the capacity to address parents' concerns cannot be answered by a one-size-fits-all solution and an **assessment needs to be made on a case by case basis**.

The overall conclusion is that, among the tested tools, a **single perfect tool does not exist** and parents should look for the tool that best matches their needs, adequately balancing the areas of tools' performance.

The parents' **selection** of the tool/s may be guided, in principle, by the following **criteria**:

- The ease of the **installation** process;

- The range of **functionalities** offered by the tool;

- The type and number of **features** incorporated;

- The best **price** or a free subscription;

- The option of complete **monitoring** of Internet activity;

- The quality of reporting and feedback produced.

Not all the above criteria may be possible simultaneously; therefore, a good balance should be maintained among them. Furthermore, the beneficial effects of the application of a parental control tool should be considered against the **risk of over-restricting children's activity and Internet exploration**.

Using parental control tools is a **learning process**. Parents should be aware of this and should be ready to develop their skills along the usage and monitoring process.

A **guide** could be useful to 'educate' parents on how to integrate the use of parental control tools with parenting and how to inform and explain to children how to use these tools properly.

In terms of future tool development, a **balance** should be found between **vendors' perspectives** and **parents' needs**.

On the industry side, the development of **safety features** appropriate to (very) young users and the provision of **easy-to-use** safety functions, alert and blocking functions should be encouraged. Furthermore, development of tools which allow for more **transparency** and enable **productive parent/child interaction** should be supported.

Production of better-designed, age-appropriate and user-friendly tools and interfaces, shaped by the results of **user-friendliness** and **user experience** studies should be encouraged in the future.

On a policy level, a **renewed focus** on the issue of safety online, with an eye to what is really innovative in the market, should be set, concentrating efforts on emerging issues such as how to deal with the increasing mass of user-generated content, how to address the need for safety of very young children who are becoming frequent users of the Internet, how to address challenging innovations like the Internet of Things, how to ensure the protection of children's rights in this open and risky context, and how to guide producers in developing products in line with users' needs, safeguarding user-friendly features, effective monitoring, affordable prices and usability across countries and user groups.

Policy making may foster research and development on the emerging technologies and the **user-generated, content-related issues**, boost research on how to improve parents' supervision and youngsters' **resilience** and pursue **standardisation of content classification**.

Furthermore, additional actions may be taken to continue the **awareness-building** and **knowledge-dissemination** process towards target groups of users, together with initiatives that allow for constant **discussion** and **debate** among tool providers and users and boost a user-centred approach in the design and development of parental control systems.

Bibliography

- *AttrakDiff: Ein Fragebogen zur Messung wahrgenommener hedonischer und pragmatischer Qualität;* Ziegler, J. & Szwillus, G. (Hrsg.), Mensch & Computer 2003. Hassenzahl, M., Burmester, M., & Koller, F. (2003)

- *"Being young in Europe today - digital world",* EUROSTAT - Statistics Explained, February 2017

- "Children and parents: media use and attitudes report", Ofcom, October 2014

- "Children and technology in the United Kingdom (UK)" - Statista Dossier, 2016

- *"Children's use of mobile phones. An international comparison 2013"*. GSM Association and the Mobile Society Research Institute within NTT DOCOMO Inc, Japan, 2014

- "Communications Market Report 2016", August 2016

- EU Kids Online III, *"Findings, methods, recommendations"*, KU Leuven, Belgium, February 2016

- *"European Strategy for a Better Internet for Children"* - COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, COM (2012) 196 final, 2012

- *"Interaktion in Bewegung"*, S. 187-196, Stuttgart, Leipzig: B.G. Teubner

- *"ISO 9241: Ergonomics of Human System Interaction"* (2006), ISO 14915: Software ergonomics for multimedia user interfaces, Web Accessibility Initiative of the W3C (WAI), IEC TR 6199, ISO/IEC 18021, ISO/TR 22411, ISO/IEC 25000

- *"JIM 2016, Jugend, Information, (Multi-) Media"***,** Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland, Sabine Feierabend (SWR Medienforschung), Theresa Plankenhorn (LFK), Thomas Rathgeb (LFK), February 2017

- *"KIM-Studie 2016. Kindheit, Internet, Medien"*, Basisstudie zum Medienumgang 6- bis 13-Jähriger in Deutschlan, Sabine Feierabend (SWR Medienforschung), Theresa Plankenhorn (LFK), Thomas Rathgeb (LFK), February 2017 Basisstudie zum Medienumgang 6- bis 13-Jähriger in Deutschland

- "Let's Play it Safe. Children and Youths in the Digital World", Assessment of the Emerging Trends and Evolutions in ICT Services. White Paper for the ICT Coalition for Children Online, Jutta Croll, January 2016

- *"Mapping Safer Internet policies in the Member States. The Better Internet for Kids (BIK) Map"*, FINAL REPORT, Philip Baudouin, Bea Mahieu, Thierry Dor, Barbara Good, Judit Milayi, Soichi Nakajima, Study prepared for the European Commission DG Communications Networks, Content & Technology, 2014

- "*One in Three: Internet Governance and Children's Rights*", Global Commission of Internet Governance, Sonia Livingstone, John Carr and Jasmina Byrne, PAPER SERIES: NO. 22 — November 2015

- "Parental controls: advice for parents, researchers and industry", Bieke Zaman and Marije Nouwen, ISSN -045-256X, February 2016

- "*Parenting issues will not be solved because 'there is an app for that'*", EU Kids Online III, KU Leuven, Belgium, Press Release 11th May 2016

- "Perspektiven des technischen Jugend-schutzes. Aktuelle Herausforderungen und zukunftsfähige Konzepte", Andreas Marx, Mark Bootz, Friedemann Schindler, June 2016

- "*Seminario di Sicurezza Informatica Safer Internet*", Università degli Studi di Perugia, Facoltà di Scienze Matematiche, Fisiche e Naturali, Corso di Laurea Magistrale in Informatica, anno accademico 2010-2011, Stefano Bistarelli, Luca Caprini, Fabiana Zollo

- "*The Best Parental Control Software of 2017*", Neil J. Rubenking, January 5, 2017

- "*The protection of minors in a converged media environment*", Francisco Javier Cabrera Blázquez, Maja Cappello, Sophie Valais, European Audiovisual Observatory, Strasbourg 2015, IRIS plus 2015-1

WEB SITES:

http://ec.europa.eu/saferinternet

www.eukidsonline.net

http://www.attrakdiff.de/index-en.html

http://attrakdiff.de/files/mc2003_hassenzahl_review.pdf.

https://lsedesignunit.com/EUKidsOnline/index.html?r=64

https://www.consumer.ftc.gov/articles/0270-kids-parents-and-video-games

https://www.eset.com/int/about/newsroom/products/88-of-parents-concerned-about-what-children-can-access-online-reveals-survey/

https://www.commonsensemedia.org/blog/everything-you-need-to-know-about-parental-controls

http://www.coe.int/en/web/children/children-s-strategy

https://www.theguardian.com/technology/2014/aug/11/how-to-keep-kids-safe-online-children-advice

Annex

Categories of harmful content

ADULT CONTENT

- Non-nude but sexually stimulated women or men,
- Erotic nude pictures,
- Softcore porn,
- Sex accompanied by pain, injury or humiliation,
- Hardcore sex, ejaculation, erection, defecation, urination, bestiality, necrophilia,
- Pictures or stories about acts or results of stimulating erogenous areas,
- Games with hardcore sex or explicit sexual expressions,
- Sexual insinuations towards children,
- Requests to undress or display sexual behaviour in front of a camera or webcam,
- Promotion of prostitution.

VIOLENT CONTENT

- Pictures of raw violence,
- Blood scenes or scenes with seriously injured people,
- Details of infliction of pain and/or injuries,
- Pictures and stories about cruelty to animals,
- Scenes of domestic abuse,
- Scenes of violence of adults towards children,
- Scenes or praises of bullying,
- Games with explicit injuries or violence against children,
- Videos of real or faked murders or rape,
- Physical punishment,
- Scary sequences of scenes with threat and menace,
- Curse language,
- Indecent representations of children,
- Scary sequences of scenes with threat and menace,
- Separation and abandonment,
- Scenes that confuse facts and fiction with respect to violence,

- Misinterpretation of a specific theme leading to confusion,
- Actual humiliation of children,
- Violence on disabled people.

Racist and hate material

- Calls for hatred and racist humiliation or denigration,
- Stories that claim other races are inferior,
- Encouragement to judge people on their religion, birth, race, social background, etc.
- Stories that negate Holocaust.

Illegal drug taking and the promotion of illegal drug use

- Stories that claim medicines or drugs are harmless,
- Stories that position medicine or drug abuse as "cool",
- Condoning drug use and providing instructive detail,
- Stories that convince children to solve their problems by abusing drugs,
- Calls to join a religious cult,

Criminal skills/activity that could instigate damage to others

- Inspiring videos or content that show real or faked rape,
- Games that stimulate rape or harassment,
- Positioning rape, torture, sadistic violence or terrorization as "cool",
- Portrayal of violence as a normal solution to a problem,
- Promoting anti-social behaviour,
- Terrorism proselytising,
- Stories that convince children problems can be solved by murder or mass murder,
- Tips and tricks or do-it-yourself terrorism tools,
- Games that simulate murder or terrorism,
- Video of actual acts of terrorism,
- Glamorisation of weapons and knives,
- Tips and tricks for breaking into cars, buildings, etc.,
- Tips and tricks for sabotage,
- Calls for public indecency (urinating, vandalism, mooning, streaking),

- Stories that claim theft is harmless,
- Stories that claim theft from the rich or large companies is harmless to the rich or company,
- Calls to children to commit sabotage,

CONTENT THAT COULD INSTIGATE YOUNGSTERS TO HURT THEMSELVES

- Encouraging taking pleasure in pain,
- Attempts to persuade children to divulge information about their parents,
- Stories that convince children to solve their problems by suicide,
- Content promoting anorexia and bulimia.

GAMbLING

- Invitations to gamble or bet.

European Commission

SIP-BENCH III - Benchmarking of parental control tools for the online protection of children – FINAL REPORT

Luxembourg, Publications Office of the European Union

2017 – 83 pages

ISBN 978-92-79-70499-4
doi:10.2759/80227

KK-02-17-803-EN-E

doi:10.2759/80227 ISBN 978-92-79-70499-4