Marie Sklodowska Curie,
Research and Innovation Staff
Exchange (RISE)

Ref. Ares(2016)3135302 - 30/06/2016

European Commission

Horizon 2020
European Union funding
for Research & Innovation

ENhancing seCurity and privAcy in the Social wEb: a user-centered approach for the protection of minors

ENCASE
ENhancing seCurity and privAcy in the Social wEb

WP2 – Requirements and System Architecture

Deliverable D2.1 "System Requirements and Software Architecture"

Editor(s):	Andri Ioannou (CUT)
Author(s):	Andri Ioannou, Michael Sirivianos, Kwstantinos Papadamou, Antigoni Parmaxi (CUT)
Dissemination Level:	Public
Nature:	Report
Version:	1.8

ENCASE Project Profile

Contract Number	691025
Acronym	ENCASE
Title	ENhancing seCurity and privacy in the Social wEb: a user-centered approach for the protection of minors
Start Date	Jan 1st, 2016
Duration	48 Months

Partners

	Cyprus University of Technology	Cyprus
	Telefonica Investigacion Y Desarrollo SA	Spain
	University College London	United Kingdom
	Cyprus Research and Innovation Center, Ltd	Cyprus
	SignalGenerix Ltd	Cyprus
	Aristotle University	Greece
	Innovators, AE	Greece
	Universita Degli Studi, Roma Tre	Italy

Document History

AUTHORS

(CUT)	Andri Ioannou, Michael Sirivianos, Panagiotis Zaphiris, Kwstantinos Papadamou, Antigoni Parmaxi
(UCL)	Gianluca Stringhini
(INNO)	Makis Stamatelatos
(CYR)	Pantelis Nikolaou, Adamos Fiakas

VERSIONS

Version	Date	Author	Remarks
0.1	28.03.2016	CUT	Initial Table of Contents
0.2	01.05.2016	CUT, INNO, CYRIC	Added the review of the related web-tools
0.3	15.05.2016	CUT	Added the literature review
0.4	18.05.2016	CUT, INNO, CYRIC, UCL, ROMA3, AUTH, SGX, TID	Initial Use Case definition
0.5	19.05.2016	CUT, INNO	Added review of cyber security risks for minors
0.6	20.05.2016	CUT	Added the Software architecture overview
0.7	23.05.2016	CUT	Added Scenarios for Use case A
0.8	31.05.2016	CUT	Added Scenarios for Use case B
0.9	06.06.2016	CUT	Added Scenarios for Use case C
1.0	09.06.2016	CUT, INNO, CYRIC, UCL, ROMA3, AUTH, SGX, TID	Initial User Stories definition
1.1	13.06.2016	CUT	Added User stories and their acceptance criteria
1.2	17.06.2016	CUT	Added the Operation Requirements
1.3	20.06.2016	CUT	Added the Security & Privacy Requirements
1.4	22.06.2016	CUT, INNO	Comments and corrections
1.5	23.06.2016	INNO	Added the SOTA analysis table
1.6	26.06.2016	CUT, INNO, CYRIC	Comments and corrections
1.7	28.06.2016	CUT	Document layout and format check
1.8	30.06.2016	CUT, INNO, CYRIC	Proof reading – Final version

Executive Summary

The overall aim of ENCASE is to leverage the latest advances in usable security and privacy for minors (age 10-18) in order to design and implement a browser-based user-centric architecture for the protection of minors from malicious actors in online social networks. This architecture will consist of three distinct browser-add-ons.

This deliverable, D2.1 “System Requirements and Software architecture”, is an initial specification of the system’s requirements and the software architecture that combines the three browser add-ons that will be implemented. The requirements’ extraction process that we followed is also described in this deliverable. The content of this deliverable may change during the implementation. A second version of D2.1 will be delivered in Month 12 where more detailed system requirements and software architecture will be specified.

The requirements extraction is a two-phase process: The first step involves eliciting requirements via an analysis of complementary use cases in order to demonstrate the core functionalities of the ENCASE toolset. Each use case consists of scenarios outlining different aspects of the envisaged system. Then, the scenarios of each use case evolve into user stories that are considered as the functional requirements of the system. Additionally, the various components of the ENCASE software architecture are outlined in this document.

Table of Contents

List of Figures

List of Tables

No table of figures entries found.

1. Introduction

1.1. Purpose of the document

The main purpose of this document is to define the requirements of the system to be implemented. At first, a survey of all the existing security and privacy enhancing web-based tools along with a survey of the research state-of-the-art are provided. Following the requirements engineering methodology, this deliverable defines all the use cases and user stories of the ENCASE ecosystem.

1.2. Structure of the document

The document is structured as follows. Section 1 describes the purpose of the document, the requirements engineering methodology that we adopted. The templates for the use cases and user stories are also included in this section. Section 2 provides a survey of the state-of-the-art of web-based tools and the research state-of-the-art. Section 3 defines the use cases that our system is going to handle and Section 4 provides the identified system requirements. Finally, Section 5 provides an initial description of the software architecture. We conclude in Section 6.

1.3. Requirements engineering background

According to Sommerville and Sawyer in their 1997 book [1], Requirements engineering is the process of discovering, documenting and managing the requirements for a computer-based system. The goal of requirements engineering is to produce a set of system requirements which, as far as possible, is complete, consistent, and relevant and reflects what the customer actually wants.”

Requirements in ENCASE are going to be extracted from (i) the review of existing security and privacy enhancing web-based tools, (ii) a survey of the research state-of-the-art, and (iii) the usage scenarios documented and specified in this deliverable. A second iteration of this document is going to be provided in month 12. It is necessary for a complete set of requirements to be in place prior to the design of the final system, where the architecture, components, modules, interfaces, and data are going to be specified.

In order to have a common understanding of the terms “use case” and “scenario” used in this document and in requirements engineering in general , we present basic definitions as provided in the book “Managing Software Requirements: A Unified Approach” by Leffingwell and Widrig.

Use Case: A description of a set of actions, including variants (alternatives), that a system performs that yields an observable result of value in a particular environment and related to a particular goal.

Scenario: An instance of a use case, expressed as a sequence of events.

1.4. Methodology

Requirements in broad terms need to be discovered, documented and maintained (i.e. change if necessary, keeping track of change and potential impact to the design, and validate the requirements once the process is over). These activities are referred to as Requirements Elicitation, Requirements Analysis and Requirements Specification according to Robertson & Robertson [2].

Requirements Elicitation is where the requirements process starts. It ensures a common understanding of the problem that the system aims to solve. The requirements elicitation involves collecting information about all involved stakeholders, including end-users. The information that is sought is about what users are currently working with, why it is inadequate, what their vision of an improved system is, and why. To elicit requirements, there are many different techniques that can be used (e.g., interviews, surveys, brainstorming, etc.), sometimes in combination. For the purposes of ENCASE we are primarily going to use use cases, which are developed after thorough review of the literature and informal discussions with involved stakeholders (i.e., parents and children).

Requirements Analysis The main objectives of Requirements Analysis are: (i) to detect and resolve conflicts between contradicting requirements, and, more importantly, (ii) to provide detailed requirements: an initial set of high-level requirements describing the functional characteristics of the overall system is followed by a step-by-step approach of decomposing the system into more detailed functional and nonfunctional requirements.

Functional requirements capture the intended behavior of the system. This behavior may be expressed as services, tasks or functions the system is required to perform [REF]. This should be contrasted with non-functional requirements, which specify overall system characteristics. Non-functional requirements are also often called qualities of a system. Other terms for non-functional requirements are "constraints", "quality attributes", and "quality of service requirements". Non-functional requirements, can be divided into two main categories:

- Execution qualities, such as security and usability, which are observable at run time,
- Evolution qualities, such as testability, maintainability, extensibility and scalability, which are embodied in the structure of the system [REF].

In this sense, functional requirements are supported by non-functional requirements, which impose constraints on the design or implementation (such as performance, QoS, or reliability).

Several levels of requirements are developed, providing sufficient granularity so that they can be allocated to individual subsystems and components in the next step of system design. Similarly, in the case of ENCASE a prioritisation is going to take place prior to embarking on system design. Consulting with the stakeholders and end-users, more important technical requirements are coming to surface in order to provide a very relevant system design.

Requirements Specification is the formal documentation of the requirements extracted from requirements analysis. Requirements must be specific, so that they leave no room for ambiguity or misinterpretation. The specification document in ENCASE is D2.1 which has to be maintained over the life of the project.

1.5.Data Collection

The goal of the data collection is to identify the magnitude of the problem and to extract requirements for our solution. We have been collecting a 1% sample of all public Tweets from the Twitter API for a period of nine (9) months. Each tweet is stored in JSON format and contains information such as the text that was posted, profile information about the user who posted it, and

the client application it was posted from. From this dataset, we extracted tweets that were likely to contain controversial content (e.g., politics, gender issues, racism), with the hope of observing bullying messages and hate speech in them. To get this set of tweets, we first extracted tweets containing the GamerGate hashtag, which was target of bullying and harassment in late 2015. We then enumerated all the additional hashtags appearing in the same tweets, which accounted for 1301 hashtags. These hashtags are not all associated with controversial content. We therefore manually filtered this list, coming up with 272 hashtags. We then extracted all tweets containing those hashtags from the dataset. The total number of extracted tweets is 507,259.

To further filter the tweets and extract those that contain hate speech and other bullying content we will apply topic extraction with Latent Dirichlet Allocation (LDA), combined with the use of HateBase, an API for detecting hate speech words.

1.6.Use Case Scenario template

To provide a structured scenario description, a scenario template is defined:

Field Name	Field Description
Code number	A number identifying the scenario in a unique manner
Name	A short self-explanatory title of the scenario
Author/Partner	The original author(s) of the scenario
Stakeholders	The involved personas
High-level Description	A short story describing when, why and what happens when a Persona uses one or more of the browser add-ons that ENCASE offers. A comprehensive and self-explanatory narrative, focusing in describing a basic use of the system
Variant	An optional field, identifying alternative ways to use the system by the same personas
Issues	Specifying the key issues in the story for the different personas. It can include technical limitations, regulatory constraints, performance challenges
Benefits	Specifying how the different personas benefit from ENCASE in order to clarify the added value for the system users in particular when compared to current limitations
Notes	Any general remark related to the Scenario that should be kept in mind while carrying in the later development stages
Services	The browser add-on(s) that will be used to materialize the scenario

1.7.User Story template

To provide a structured User Story description, a template is defined as follows:

Code number	Coded identification of every user story
Title	User story title
Description	User story text in the following format: As a ... I want to … so that ...
Acceptance	Criteria based upon which the successful implementation of the user story will

criteria	be established. • Criterion 1 • Criterion 2 . . • Criterion n

2. State-of-the-art

This section summarizes all the research state-of-the-art and existing web-tools for mitigating threads that renders minors and other vulnerable population groups susceptible to abusive behavior in OSNs.

2.1.Benefits and risks of Web 2.0 tools

The advancement of Web 2.0 tools offers a rewarding source of knowledge sharing, interaction and socialization. Amongst the benefits reported in the use of these tools include the development of 21st century skills such as creativity, innovation, team building, critical thinking, confidence, information sharing, higher academic achievement and improvement of ICT skills and competences [24], [25]. Yet, being present in OSNs such as Facebook, Twitter, Snapchat and MySpace presents particular risks such as exposure to cyberbullying, child abuse, inappropriate material and contact with dangerous strangers. Social Web can facilitate abuse of children by adults - being in place to assume fake identities online, a possible “danger” can intrude a child’s private zone leading to violence or even sex crimes [26]. Online bullying, or cyberbullying, can also be a traumatic experience.

2.2.Security and privacy enhancing web-based tools review

This section provides a review of the existing web-based tools and mobile applications that are trying to address the security and privacy issues in the OSNs. We list below the most relevant ones to the concepts of ENCASE.

Qustodio:

Qustodio is parental control software available in most of the platforms [3]. It enables parents to monitor and manage their kids’ web and offline activity on its devices. It also allows them to track with whom their children are communicating with in OSNs and manage their whole OSN activity. In addition, Qustodio can be used as a sensitive content detection and protection tool.

Avira SocialShield:

SocialShield is a Social Network Protection application developed by Avira [4]. It is a monitoring tool that informs parents of their children’s online activities. It monitors and checks their child’s social network accounts for any comments, photos etc. that may influence the child’s reputation in a negative way or may indicate that the child is in danger. Furthermore, SocialShield is able to protect the children from cyberbullying, to prevent them from participating in online discussions with inappropriate content and it is also able to verify the identities of the child’s online friends.

Web of Trust (WoT)

Web of Trust is a safe browser add-on for website reputation rating that helps users to make informed decisions about whether to trust a website or not when browsing online [5]. In order to provide its users with an extra layer of security against malicious links posted by malicious users, Facebook uses WOT’s reputation data to inform users about low reputation links.

WebWatcher

WebWatcher is a parental control, cross-platform compatible, monitoring software [6]. It is able to capture the content of emails and instant messages in OSNs, as well as actual keystrokes and screenshots. It assists parents in keeping their children safe online by viewing what is captured in their child’s screen from everywhere.

Cloudalc WebFilter Pro

Cloudalc WebFilter is cloud-based content filtering application [7]. Cloudalc monitors billion of web pages to protect families and especially kids from malicious attacks and threads and to have a safer Internet surfing experience. It blocks web pages, spam servers and adult material.

Abuse User Analytics (AuA)

Abuse User Analytics is an analytical framework aiming to provide information about the behavior of OSN users [8]. This framework processes data from users’ activities in the online social networks with the goal to identify deviant or abusive activities through visualization.

FoxFilter - THE Parental control for Firefox

A free browser add-on produced by Mozilla and is known as the parental control for Firefox browser [9]. It is a personal content filter that helps blocking pornographic and other inappropriate content. A user can block content for an entire site or enter custom keywords that will be used to block content for any site that contains those keywords.

Parental Control and Web Filter from MetaCert

It is a parental control browser add-on that blocks pornography, malware and spyware [10]. It protects kids and adults across multiple categories. It allows you to choose among two main categories (extra strong for kids and Strong for adults) while also allows you to define the specific categories that you prefer to be protected (such as Bullying, Drugs, Aggressive behavior, Gambling, Sex etc.).

MetaCert Security API

MetaCert is a Security REST API [11]. It provides a layer of security on top of web applications so that the application can protect users from Phishing attacks, Malware and Pornography.

eSafely

eSafely is a parental control browser add-on that provides kid-safe access to popular web resources, free of adult content [12]. Generally, it offers the following: a) Kid Safe Facebook that protects children against cyberbullying by replacing harassing messages with friendly icons in Facebook chat; b) Kid Safe Images that when a site is identified as hosting adult content it replaces the images with images more suitable for children; c) Kid Safe YouTube; and d) Kid Safe Search.

Nude.js: Nudity Detection with JavaScript and HTMLCanvas

Nude.js is a JavaScript implementation intended for client side nudity detection based on approaches from research papers [13]. It analyzes image and video data and returns whether it contains nude content or not.

ReThink

ReThink is a non-intrusive, patented software product that stops cyberbullying before the damage is done [14]. When an adolescent tries to post an offensive message on social media, ReTHink uses patented context sensitive filtering to determine whether or not it is offensive and gives the adolescent a second chance to reconsider their decision.

PureSight Multi

PureSight Multi is a monitoring and filtering cross-platform software that allows children to use the internet without fearing bullies or harassment and keeps parents in the know [15]. It features cyberbullying protection on Facebook, Web filtering, Reports and alerts, file sharing control and parent portal.

MM Guardian Parental Control app

MM Guardian is a mobile application that allows you to block incoming calls and texts, monitor alarming texts and control which apps on the device can be used and when on a children's' smartphone [16]. It also allows the parent to locate and lock his children’s mobiles with a text message, as well as to set time restrictions to limit their use.

Funamo Parental Control app

Funamo Parental control is a mobile application that allows parents to monitor their children's mobile devices [17]. Contacts, calls, SMS, browser history, applications and locations are automatically logged and history data is uploaded to the Funamo server each day. It also allows parents to enable safe search engines in the web.

Screen Time Parental Control app

Screen Time is a parental control mobile application that empowers parents with the ability to monitor and manage the time that their children spent on their devices and set time usage limits on selected apps, as well as a bedtime curfew, lights out and school time curfews [20]. The app runs in the background of the mobile device and it can be controlled via any web browser.

The following table summarizes the web-based tools analysis. Such analysis is aiming at overviewing the features provided by existing web-tools for user protection. Moreover, such capabilities can be considered as benchmark capabilities which could be supported by ENCASE solution at web add-on level and/or be carried out in an integrated and more efficient way. Of course it is the ENCASE actual scope and priorities to determine whether these features should be incorporated in the ENCASE add-ons.

Key Capabilities	Tools	SW	App	Browser add-on	API

Monitoring (Monitor web online/offline activity, track OSN communication activity, etc.)	Qustodio	■			
	Avira SocialShield		■		
	PureSight Multi	■			
	Screen Time		■		
	WebWatcher	■			
Website reputation rating	Web of Trust			■	
Content Detection	Qustodio	■			
	WebWatcher	■			
Cyberbullying protection	Avira SocialShield		■		
Content Filtering (OSN content filtering and flagging, offensive message determination, identify deviant or abusive activities etc.)	CloudAlc WebFilter Pro		■		
	FoxFilter			■	
	Meta Cert			■	
	eSafety			■	
	ReThink	■			
	PureSight Multi	■			
Content Blocking (Content replacement, webpage blocking, etc.)	CloudAlc WebFilter Pro		■		
	FoxFilter			■	
	MetaCert			■	
User protection (e.g., OSN identity verification, etc.)	MetaCert API				■
	Abuse User Analytics	■			
Nudity Detection	Nude.js	■			
User Device App control (e.g., app locking, time usage limitation, etc.)	MM Guardian		■		
	Funamo		■		

	KidsPlace				
	AppLock				

Despite the aforementioned web-based tools, there are others like NetNanny, Safe Eyes, Elite Keylogger etc. that are trying to solve some of the problems that ENCASE does [21], [22], [23]. Most of them are parental control tools that are monitoring children's online activity using the following methods:

1. **Keystroke logging:** It is the action of recording the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored. In ENCASE we will
2. **Screen capturing and monitoring via screenshots:** The action of monitoring a user's activity on his device by capturing screenshots periodically. ENCASE will not adopt such type of monitoring.
3. **Android monitoring:** It is the action of monitoring, recording and reporting the activity of a user in his android mobile device. In ENCASE we will adopt this method but only for monitoring the user's OSN activity.
4. **SMS and instant messaging in OSNs capturing:** It is the action of monitoring a user's OSN activity and reporting, via SMS or instant messaging, any abnormal incident based on keywords. In ENCASE we will use more intelligent techniques, like machine learning techniques, to capture and analyze a user's OSN activity.
5. **Content blocking and filtering:** It is the action where the administration declares a set of websites or keywords (e.g., pornography) that he wants to be blocked and cannot be accessed from a user's device.
6. **Time usage limits:** A parent is allowed to set limits regarding the time that his child is able to use his device. We will not adopt this method in ENCASE.

Overall, most of the existing tools rely on monitoring and parent review to detect any abnormal activity. Some of them search for keywords to create alerts, while some others block the usual list of websites.

Cyber-bullying, cyber-grooming and exchange of sensitive content is not *intelligently* detected by existing web-based tools and this has a negative social effect on the children i.e. they are monitored to an excessive degree and this will probably lead them to find alternative ways to go online. ENCASE, with the malicious behavior detection browser add-on will be a good compensator for protecting the children from communicating with a person that is willing to bully or exploit them.

2.3. Research state-of-the-art on cyber security risks for minors

This section provides a review concerning the Internet activity and motivation of use by minors and presents in a coherent manner the identified risks and threats that children using the web and OSNs are exposed to.

2.3.1. Minors' access to the Internet and use of OSN

Nowadays, children are very familiar with technology. Research has shown that they have the ability to familiarize themselves with any electronic gadget very fast and they are able to do sophisticated tasks using these devices. Research has also proven that as soon as children come in touch with electronic device such as PC's, tablets, smartphones and so on, they can use them instantly, in contrast with adults who may need to study the instructor manual of the gadget.

More and more children, these days, have access to the internet through handheld electronic devices such as smartphones, tablets and portable game consoles [43]. According to Ofcom reports on Internet safety measures and strategies of parental protection for children online in the UK tablets became the favorite device for online access for children aged 8-11 who mostly used them for playing games [44], [45]. Smartphones are the most popular device for social networking and, according to the same reports, the children aged 12-15 have their own smartphone. Most parents believe that children are more at risk when they are online at home than outdoors. However, statistics have proven the opposite. This is because smartphones, tablets and other handheld devices, offer instant access to the Internet everywhere and children prefer that as they are not supervised by their parents. According to the 2016 ITU report on child online protection in USA the number of children who have access to the internet is constantly increasing since 2011 [43]. Children below five years of age use the internet on a weekly basis and as age increases the frequency of access to the internet also increases. The 40% of children aged 8-11 years old make use of the internet daily while the 36% of them use it multiple times per day. The same report reveals that 70% of teenagers are online daily while 25% of them reported that they are permanently connected online. A survey conducted by South Korean government has shown that one out of ten children aged 10-19 years are addicted to the Internet [46]. According to that study, when children are connected online they enjoy using a variety of activities whose number increase by age. For instance, children under 9 years old search for information about school, play games or watch videos [47]. Children aged 10 to 19 also listen to music as well as the above mentioned activities, however their basic everyday use of the internet is for social networking reasons.

The intrusion of online social networks in people's everyday life the last decade, has met with huge success. There are many social networks services available, so as to meet different needs according to age, language, profession and culture. According to the 'Net Children Go Mobile' network report [48], approximately 70% of children in Europe have at least one social network profile while most of them have a profile in media sharing services such as YouTube or Instagram. In UK one out of four children use Twitter to share photos and other content [49] rather than tweeting. A study conducted by Pew Research Center for USA [47] concluded at similar findings. Facebook is the most popular social media site among American teenagers aged 13 to 17 since 71% of them are using the corresponding website. Half of teens use Instagram, while the popularity of Snapchat increases rapidly reaching a 41% of teen's population. Snapchat allows people to send and receive pictures and videos directly to their phone and created new security concerns for parents [50]. The study of Pew Research Center showed also that about 71% of teens are using more than one online social network site [47].

2.3.2. A taxonomy of online risks for minors

It has being shown in the previous section that the popularity of Internet in general and OSN in particular is high and with increasing tendency among children and teenagers. Thus, the online risks for these sensitive age categories received increased awareness. Several different international organizations and research groups have been trying to study and categorized the dangers which have emerged in the past years including EU Kids Online, ITUs-Child Online Protection (COP), Youth Protection Roundtable (YPRT), Net Children Go Mobile and many others. These organizations conduct surveys in regular time intervals and, based on the findings, recommend safety measures for every identified potential danger that the Internet might pose to children. However, the security and privacy risks themselves are rarely mentioned making it difficult to define energetic actions and to design tools that proactively try to minimize the aforementioned risks and dangers. For instance, in contrary to a few studies such as those of Australian Communications and Media Authority where dangers, of Internet and OSN use, such as electronic fraud, malware and other e-safety threats, are explicitly mentioned, research in Europe usually describes generic categories of risks such as sexual and commercial [51], [52].

Categorization of online risk for children is not easy. In most cases risks are caused or affected by a variety of reasons emanating not only from children's online lives but their real lives as well. In addition many risks and threats are crossing several categories. In the corresponding literature the following distinctive situations have been defined [43], [49], [53]:

- Online risks which are the expansion of problems in real life, for example pornography.
- Risks which arise from the interaction of two under-agers such as cyberbullying.
- Risks which arise from the interaction between a child and an adult, such as cyber grooming.
- Risks which arise by the collection of data, against the protection of privacy, such as viruses and other malware.

In addition of potential dangers, children on the internet might be exposed to, can be assessed based on the legal importance and by discriminating the cases where the child is the victim or the predator.

Another popular, in the related bibliography, categorization of online risks is based on the way the Internet is 'used' and/or perceived by the children. The first clearly concerns the risks of the Internet as product of technology or simply stated the risks that arise due to minors' access to Internet content. The second category, concerns incidences where the Internet provides the means through which the children are exposed to dangers, i.e. contact risks, and finally, the third category refers to cases where children are aimed at as online consumers [54], [55].

2.3.2.1. Content risks

As already stated, children are able to familiarized themselves with Internet and generally with technology as they grow up parallel to it. This fact combined with the fact that in 2015 there were more than one trillion websites, turns children into a vulnerable group or exposed to many dangers related to the content of the Web. Content risks are divided, according to bibliography, in three categories: (a) illegal content; (b) harmful content or age inappropriate content and; (c) harmful advice.

Illegal content refers to content which is illegal to be published online. For example, it might be content about sexual exploitation of children which is illegal in most countries. Inappropriate content usually depends on the age of children that have access to and may contain, for instance, adult pornography. Hatred or violence related content, although not illegal, may harm children in case they gain access to it. Age inappropriate content may be mentioned, as term in national or local cultures and social values, however, in literature and official documents this term focuses more widely on pornography and other sexual content [55]. The meaning of pornography may vary between countries and between groups within a country. Pornographic content is fairly easy to be found by anyone online, however, younger children are more exposed to offline pornography than online ones [56]. Nevertheless, a lot of studies agree that exposure of children to online pornography content increases by age. In addition it was found that random exposure of children to pornographic content, on the Internet, is more common than intentional access and it increases when the names of the websites or URLs are misleading for children. According to ITU the rates at which children of young ages are exposed to websites of pornographic content appears an increasing tendency [43]. This happens even to children whose parents have locked access to sites of inappropriate content. The high percentage of children that randomly access to pornographic content continues with intentional access. According to Dooley et al. only children of very early age reported being upset by being exposed to pornographic content [57]. As for the exposure of children to violate content researchers did not arrive yet at concrete findings and it seems that additional research is required.

Harmful advice refers to content which may lead a child to consume alcohol and drugs or to commit suicide or different psychological and nutritional disorders. In combination with the fact that anyone can provide such advice online through social networks and other platforms, it is very easy to children to have access to and be influenced by it. Researchers state that many of these advices maybe well intended; thus, it is difficult to be categorized to harmful or useful [55].

2.3.2.2. Contact risks

Contact risks refer to instances or events that children have direct interaction online, either with other children or with adults. This can be achieved through child’s participation in online chat or social networks chats. A frequent phenomenon is when adults try to develop relationships of trust with children with the aim of having sexual intercourse with them. This constitutes a criminal act in almost all countries and is known as cyber grooming [55], [43]. Cyber grooming is often when an adult sexual predator seeks a communication with its victims in a direct online conversation with the aim of coming in offline sexual relation with them without mentioning his/her real age and identity to the children taking advantage of their naivety [58].

Cyberbullying is another contact risks for the children. The term cyberbullying refers to bullying that children undergo through the Internet. Bullying may come in different types such as threats, humiliation or harassment. Cyberbullying differs from cyber stalking and cyber harassment. While in cyberbullying there is participation of peers of both sides, in the event of an adult participant it constitutes cyber harassment [59]. Experiencing tense emotions such as anger, desperation or vengeance are frequent reasons causing children to be exposed to cyberbullying. Emotions which

stem from problematic situation in the family background and problematic relationships in general are also common reasons. Researchers indicated that cyberbullying constitutes in many cases some form of entertainment, satisfying in this way power struggle needs.

In comparison with traditional bullying, cyberbullying offers some advantages to predators. The most important of which is the ability to remain anonymous which they achieve by using aliases, fake profiles, fake accounts, face social media profiles, text messages, instant messaging and other services that internet provides so they do not reveal their identity. Cyberbullying is one of the biggest threats that social networks pose. In recent years more than 3 million children have undergone cyberbullying in any form whether this constitutes harassment or threats. A high percentage (95%) of them reported that they have been victims of cyberbullying on Facebook.

Eight out of 10 adolescents who use social networks share personal information about themselves such as photos or videos, location information and contact information to a much greater extent compared to previous years. According to several studies sharing personal information such as age, phone number, school and location are the main reasons for young people to undergo cyberbullying through social networks [56], [60]. In recent years electronic games have shown an enormous increase. These games either through PCs or game consoles support features for online games and games with multiple players. Most of these games have special chat rooms so that communication among players may be easily achieved. Robinson’s research indicates that approximately 20% of the children who reported having undergone some kind of cyberbullying where cited cyberbullying to have being taken place during in an online game [46]. The most usual way of cyberbullying in an online game refers to schools, online game communities and direct communication between online players. OECD reports that the risks that minors run for sexual harassment by adults is limited; 25% young children share information and interact with strangers on the Internet, however, only 5% of them had spoken to a stranger discussing sexual matters [55]. In addition it is mentioned by OECD that most children tend to ignore the conversation and take proper steps. It is noteworthy that potential sexual predators are adolescences and adults younger than 21 years old. In general, the possibility of physical sexual contact with an adult through an online approach is very rare. Ybarra reports that only eight out of a sample of 1500 hundreds reported physical sexual contact, all of whom where aged 17 and above [61]. Furthermore, it was found cyber-grooming for children aged of 12 or less is extremely rare [60]. These results indicate that cyber grooming contains minimum danger; however it is difficult to measure precisely. Research agrees that online harassment constitutes the most widespread Risks that children face. Various individuals use the means of technology offers (social media, chartrooms etc.), with a view to harming others through bullying, humiliation and embarrassment and treats. Those who cause cyberbullying are underagers as are their victims. Despite this there have been instances where cyberbullying is caused by adults. Cyber talking refers to the event where an individual is exposed to an online extreme behavior of another individual whose purpose is malevolent treats and/or psychological or physical predicament of the victim. Overall, cyberbullying and cyber harassment constitute an ever increasing field the prevalence of which is extremely worrying [59].

2.3.2.3. Children targeted as consumers

Children on the internet face the risks of consumers, mostly for products and services especially designed only for adults. Such cases relate mostly to products such as alcohol, tobacco and prescription medicines. Children may come in contact with advertisements about these products. Furthermore, children may come in contact with the promotional illegal products such as drugs or doping substances. A study in US showed that 75% of teenagers that tried to buy cigarettes online managed to do so, while in 2002 only a percentage smaller that 3% had succeed in doing so [62].

Minors and more specifically young children are not able to realize that content on the internet is produced a financed and that is why they have difficulty critically assessing advertisements and advert messages. There have also been instances where online marketing exclusively targets websites for children for example online games. This fact has caused many countries to question integrated ads on websites aimed to children. Online marketing and advertisements may harm children. This happens mainly with products or services aimed for adult such as gambling, pornographic content and dating services. A study by Netchildren show that about 10% of the ads were about games and 5% about dating services [48]. Advertisement of pornographic content from banners and popups constitute the main reason while children accidentally came in contact with improper content.

2.3.2.4. Economic risks

It is a frequent phenomenon for children to spend exorbitantly if they have access to payment methods either through a mobile phone or other online services, thus creating huge cost for parents [64]. The most usual instances are by registering and transferring money in gambling and other online games. Many games require some form of subscription for some particular reason or to support multiplayers. Players may spend a lot to buy virtual characters or other features. There are, however, cases where children may spend huge amount of money through fraudulent transactions [56]. This occurs when services do not clarify that after the purchase of a product or service there would be extra charges. A common example of this is ringtone download services for mobile phones who charge extra for registration. According to OECD in 2008 24% of Belgian adolescents reported having paid more for ringtone downloaded and 9% registered in such kind of service without realizing it [55]. All the above risks are exacerbated with children of younger ages because of their inexperience. Nevertheless, minors who do not own a bank account or have access to their payment methods are less likely to suffer economic fraud.

2.3.2.5. Online privacy risks

Safety risks for private life information relate to all users. Children however, constitute an especially vulnerable group as they do not possess the necessary critical thinking to understand and predict the consequences. Personal information privacy in the case of children is at risk where the personal data is collected on the internet automatically following their request to search engines or other services. This may happen in various ways; the most usual is which collecting cookies, electronic registration in surveys and filling information data in electronic forms. In addition children as well as most adults, skip user term in order to have access to services they are interested in. According to OECD, 40 websites especially offered for children will analyzed and almost 75 of them ask for personal data

[55]. In most websites it was not compulsory however they did ask for personal data such as email age, birthday etc. so that they could gain access to subpages of the site [63]. There are also different websites who target children and the collection of their personal information offering quiz, competitions, research, using marketing techniques, such as a discount or free service or an award managed to gain the personal data as well as their families or friends. The research shows that minors give out personal information easier than adults in order to receive an award [62]. Children may share and reveal personal data because they cannot realize how widespread online viewers are, neither all the possible consequences. Underagers have also addicted social networks and other apps to great extent, publishing information photos videos, thus revealing important information about their life family, friends and of course themselves [58].

2.3.3. Summary

In conclusion, the huge spread of the World Wide Web and the opportunities that it offers, besides the enormous advantages, poses many risks especially for children. Research shows vast adoption of the internet by children. However, the rates where children are exposed to risks vary by country, age and gender. Pornography and cyberbullying constitute perhaps the greatest risks which children are exposed to, as is an extension of the problem of real life. Online social networks and other Web 2.0 applications are at the greatest risk because they constitute the ‘vehicle through which children may be exposed to many dangers and threats. Summarizing, the Internet contains many risks for children as they are a vulnerable group. It is an issue that needs further study and protective measures to be taken to reduce the risks that threatened children physically and psychologically.

2.4. Research state-of-the-art on security/e-safety in online environments

This section explores the research development pertaining to safety and security in online environments.

2.4.1. Introduction

The rapid evolution of social technologies, or the so-called Web 2.0 technologies, has occurred in many aspects of business, communication and education. Crook and Harrison define Web 2.0 as “a catch-all term to describe a variety of developments on the web and a perceived shift in the way the web is used [27]. This has been characterized as the evolution of web use from passive consumption of content to more active participation, creation and sharing – to what is sometimes called the ‘read/write’ web”. This term encompasses technologies that emphasize social networking, collaboration and media sharing such as Facebook, Twitter, YouTube and Flickr.

A fundamental dilemma that parents, educators and everyone need to address when considering the use of social technologies with children relates to e-safety. Increase use of social technologies, and their ubiquity in children’s lives, demand that actions are taken for ensuring children's safety and security. The question of how to allow such tools in children's life (e.g., their education to allow productivity, engagement and learning) without violating their safety and personal rights has been a key issue in a number of research papers in journals and conferences (cf. Special Issues in Journal of Computer Assisted Learning: Social Software, Web 2.0 and Learning). Some studies have been

guided by the wish to understand students’ and teachers’ concerns in incorporating social technologies in the classroom and some by the wish to identify methods for handling e-safety in a cost-effective way [29], [31]. Despite the popularity of social technologies in our daily lives, they are surrounded by concerns (from students, educators, parents, social workers, researchers and other stakeholders) with regard to their vulnerability linked to safety and security issues. For example, concerns about the use of Web 2.0 technologies in the school environment relate to exposure to online bullying, inappropriate material and risk of contact with dangerous strangers. This section provides the research state-of-the-art on e-safety in online environments.

2.4.2. Methodology

In order to synthesize the findings of research regarding e-safety in online collaborative environments, we followed a three-step approach (see Figure 1), which included: (a) compilation of the e-safety corpus which included research manuscripts related to e-safety from manually search in scientific databases; (b) refinement of the e-safety corpus and (c) synthesis of the research manuscripts.

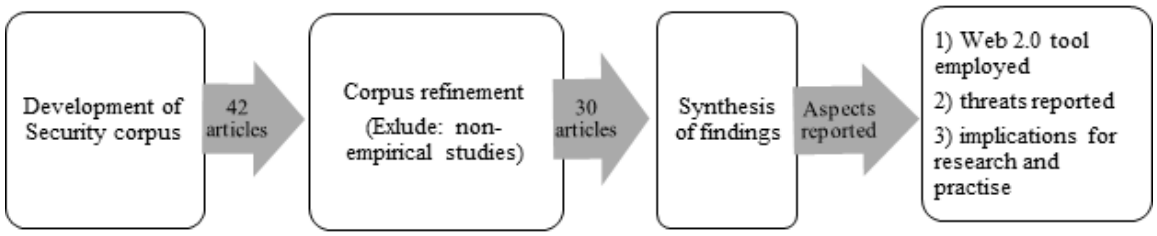

Figure 1. Flow diagram of the methodology adopted for exploring scholarly activity in e-safety in online collaborative environments.

2.4.3. Development of Security corpus

In order to understand scholarly activity on children's e-safety and security in online environments, we started by selecting appropriate resources which compiled the e-safety corpus. Appropriate articles for inclusion were selected via manual keyword (e.g., “security”, "safety", "social media", "e-safety", “threat”, Web 2.0 etc.) search in manuscripts’ title, abstract and given keywords. in the following databases: ERIC, Education Research Complete, Academic Search Complete, Computers & Applied Sciences Complete, Springer Link, Research Starters, Psychology and Behavioral Sciences Collection, Food Science Source, Taylor & Francis Group. The keyword search returned 45 manuscripts which comprised the preliminary e-safety corpus of this review.

2.4.4. Corpus refinement

Each manuscript from the corpus was screened in order to elucidate the aim of each study which was given in the form of a quote in the authors’ own words. This stage facilitated the screening of articles to be included in the e-safety corpus, excluding seven articles as reporting on non-empirical studies. The final corpus included 30 manuscripts.

2.4.5. Synthesis

Each paper in the e-safety corpus was then examined in detail to extract information related to the following pre-defined dimensions: (a) tools and threats dominant in online environments; (b) methods and tools for handling threats in online environments and; (c) implications for stakeholders including researchers, parents and educators.

2.4.6. Findings

Recent debates about students' activities with social technologies strive between the perceived benefits and the potential threats. The social web is seen to have the capacity to foster the 21st century skills, yet students, teachers, IT administrators and parents demonstrate increased concern about the online risks and threats, often related to child sex abusers, pornographic content, and bullying. Concerns about online safety fit within a broader agenda related to students' e-safety, recognizing the need to develop the skills and competences needed for taking advantage of the benefits that ICTs can provide. In the following sections, some themes are presented from the safety corpus of manuscripts.

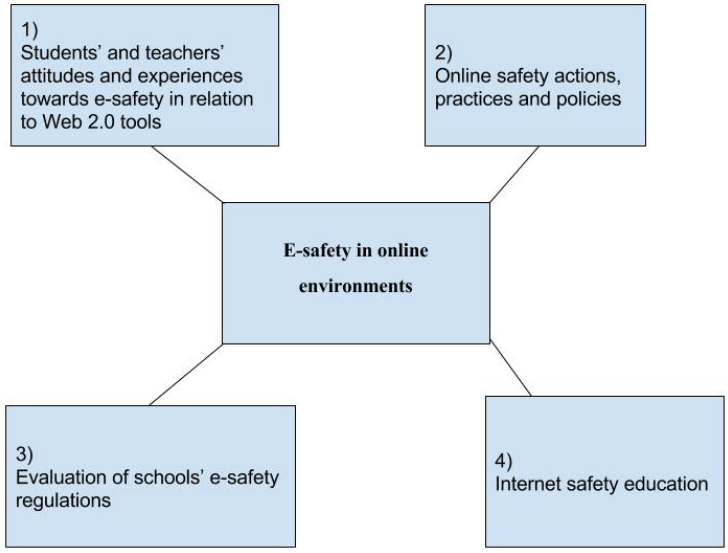

Figure 2. Overview of e-safety in online environments

2.4.6.1. Students' and teachers' attributes and experiences towards e-safety in relation to Web 2.0 tools

In this line, Sharples et al. report results of a survey of children, teachers and parents of teenage children across England [29]. The survey data were complemented with focus group interviews with students and individual interviews with teachers, managers and technical staff (IT administrators) to gain a thorough understanding of Web 2.0 activities and concerns. Findings demonstrated that a high percentage of the children surveyed (74%) have used social networking sites (SNS), whilst a substantial minority interacted regularly online with people they have not met face-to-face. Although teachers demonstrated the desire to take advantage of the benefits of Web 2.0 for creative and social learning, they reported being limited by a need to show a duty of care that

prevents worst-case risk to children, to restrict access to SN sites. The respondents also report concerns about Internet bullying and exam cheating. Finally, a Policy Delphi process voiced the need for schools to allow access to Web 2.0 sites, with children being educated in responsible and creative learning.

2.4.6.2. Online safety actions, practices and policies

Within this theme researchers engage in online safety actions, practices and policies. For example, Searson et al. describe the need for developing informed policies and practices that would involve a wide range of sectors of the society [30]. Such practices would inform technology integration in educational settings addressing the following factors: national and local policies, bandwidth and technology infrastructure, educational contexts, cyber-safety and cyber-wellness practices and privacy accountability. Two organizations offer examples and set guidelines for digital citizenship in educational settings that is ISTE and iKeepSafe. On the same line, Waters highlights the multifarious security challenges that school districts encounter, using as a stepping stone the example of a high school's page that has been hijacked by a former student [31]. The manuscript concludes by suggesting two web browser add-ons -Firesheep and BlackSheep- for users on unsecured Wi-Fi networks to identify the social networking sessions of others on that Network. Similarly, the Parent Teacher Association demonstrates its action in educating children and parents about Internet Safety (A SAFER DIGITAL WORLD). On the same line, Ramnath discuss how school administrators can protect students' safety while integrating technological advancements in teaching and learning [33]. The study engages in topics such as cyberbullying and cyber-stalking, the use of social networking sites for collaboration and the use of Mobile Device Management for the safety of mobile devices within and outside the school network. Similarly, Campbell-Wright examined e-safety in e-learning, the benefits and dangers of online interaction and guidelines for preparing organizations to handle e-safety [34]. Similarly, Wespieser, upon a survey distributed in 14,309 young people in London, demonstrated the high percentage of internet usage and social network sites, as well as issues of bullying and exposure to inappropriate material [36]. The British Educational Communications and Technology Agency (BECTA) investigated the use and impact of Web 2.0 technologies in and out of school [42]. Findings demonstrated that at Key Stages 3 and 4, learners' use of Web 2.0 is extensive and is currently done outside school, and for social purposes. The major challenge for schools in considering the adoption of Web 2.0 technologies is how to support children to engage in productive and creative social learning while protecting them from potential risk. Most learners demonstrated awareness of internet dangers, though many performed poorly in e-safety (e.g., in practice around password security). Whilst parents are generally positive in the use of technology for learning, yet concerns about e-safety exist. It is schools' responsibility in raising children's awareness on safe engagement with Web 2.0 and internet safety in general.

2.4.6.3. Evaluation of schools' regulations

Being in place to understand and evaluate schools' e-safety regulations is an issue that attracts high interest from researchers. Lorenz et al. explored 201 e-safety related stories presented by students aged from 12 to 16, parents, teachers, school IT managers and police [37]. Through the stories, typical behavioral patterns were mapped, beliefs, regulations and limitations regarding the use of social networks in schools in Estonia. The results demonstrated that few schools hold explicit policies

which target e-safety issues. Yet, even these few school-level policy documents fail to address the topics which were most frequently mentioned in the stories written by students. Safety incidents related to cyberbullying or exposure to illegal material remain unsolved or even undetected. Schools delegate any safety incidents to parents who in turn look to schools for assistance. As a principle, e-safety policies should focus on topics with which all stakeholder groups agree being important: gaming, fraud, password, harassment, pornography and meeting strangers. Emphasis should be placed in assessing e-safety risks and how they can influence online learning activities. Similarly, Cranmer reports on excluded young people's experiences of e-safety and risk demonstrating that the strategies they employ to manage their online safety are primitive and insufficient, thus pointing the need for developing further their online strategies and ultimately their digital literacy [40].

Following a somewhat similar path, Lorenz et al. moved further in analyzing the types and sources of safety incidents, the solutions offered, the students' reactions from these incidents and the solutions suggested by students and whether these solutions actually apply in real-life situations [38]. Findings demonstrated that many students do not understand what e-safety is, assuming that they are not involved in any way in an e-safety episode, even if they have been bullied or "attacked" on the internet. The awareness training about "stop-block-tell" does not work as it is something radically different from how students are thinking and acting. Blocking unwanted material is the least successful solution for the students, even if current typical awareness training is focusing on it. As findings demonstrated, students seem to be passive reactors to any malicious behavior, thus training focusing on "stop-block-tell" or "don't click everywhere" seems unsuccessful. The solution provided by the authors "is to include more technical and other practical aspects in the awareness training and distribute step-by-step, common-language how-to-s like how to set one's privacy settings, how to report a page, picture, video or how to behave when someone is being bullied, or what to do when one becomes a victim of fraud or slander. The awareness in those areas is also important for the adults who are setting the standard how their students or children behave and deal with the problems in the future" [38]. Ultimately, it is of major importance for schools to develop policies, strategies and solutions that address the core issues of children.

2.4.6.4. Internet safety education

Internet safety education is a topic that attracts researchers' interest as advancement of technological systems calls for schools to teach children to protect themselves on the web. Whilst internet safety was introduced with some "special occasion" events or a dedicated "Internet Safety Day", yet these actions seem to serve no purpose and have no real learning impact [32]. On this line, Naidoo et al. present a cyber –safety awareness framework that introduces cyber safety awareness education to primary school children in the South African community [28]. The cyber safety awareness framework offers multifarious benefits for bridging the lack of cyber safety awareness both in schools and in communities. The framework proposes that schools are grouped into clusters, with a cluster coordinator as its head. Cyber safety awareness information is expected to be disseminated through workshops attended by teacher representatives of these school clusters, and distributed back to parents, children, other teachers and ultimately to their communities. On the same line, Orech elaborates on the Digital Citizenship Project that aimed at integrating Internet Safety in the educational curriculum [32]. Through the program, students learned about

cyberbullying and prevention as well as strategies for protecting themselves in case of a cyber-insult. The project had successfully employed social media for engaging middle school teachers and students to discuss about netiquette, digital citizenship, cyber-crime prevention and managing digital footprint. Ultimately, sophomore students and teachers become cybermentors engaging in conversations about cyberbullying prevention and protection. Following a somewhat similar path, Moreno et al. consider internet safety education of vital importance for youth in US, thus they surveyed at what age should such education begin and what group is held responsible for teaching it [39]. Having distributed their survey to 356 teachers, clinicians, parents and adolescents they demonstrated that the optimal age for internet safety education is 7.2 years (SD = 2.5), whilst parents were identified as the stakeholder with the primary responsibility in teaching this topic. Clinician's role was also recognized as vital in providing resources, guidance and support.

2.4.7. Implications for researchers and practitioners

As the usage of social technologies advances, the more children and adolescents engage with these technologies on a daily basis. Internet usage has changed the way literacy is perceived and taught, raising the crucial need not only for information literacy, but also for digital literacy and specifically e-safety education. In this endeavor, the question of how parents and educators can accommodate children's behavior on the net still needs to be further investigated. As noted by Lorenz et al. there is a need for more technical training as well as, more automated solutions that would set one's privacy settings, instructing on how to report a page, picture, video or how to react when someone is being bullied [38]. Within this spirit, the overall aim of ENCASE is to leverage the latest advances in usable security and privacy to design and implement a browser-based user-centric architecture for the protection of minors from malicious actors in online social networks. With an intelligent, malicious behavior detection browser add-on, ENCASE promises to provide a solution for protecting the children from online harassment, cyber bullying victimization and other malicious activity.

3. Use Cases

In the context of ENCASE there will be three browser add-ons that will be implemented:

1. Malicious behavior detection
2. Fake identity and activity detection
3. Sensitive content detection and protection

Below, we present indicative use cases for each add-on.

3.1. Use Case A – Protection of minors

3.1.1. Use Case purpose

The goal of the protection of minors is to detect and protect minors and especially children from cyberbullying and sexual predators. Additionally, another goal is to detect and inform children when they are experiencing or are about to experience distress or aggressive behavior. Moreover, minors should be protected and informed about false information dissemination, when they are communicating with someone that has fake identity and/or activity and/or bad reputation for malicious behavior and when they are about to share sensitive content (of any type) with an inappropriate audience.

3.1.2. Scenario 1: Malicious behavior – Cyberbullying detection

Code number	A.1
Name	Malicious behaviour - Cyberbullying detection
Author/Partner	CUT
Stakeholders	Marios is a student (age: 13) at a primary school in Limassol. He enjoys surfing the web. He has several social network accounts since he enjoys chatting with his friends and family. Melanie is Mario's mother. She is familiarised with social media and is a friend with her son. Fanos and Tim are also Mario's fellow students (age 13). They have created a Facebook group chat with Marios for discussing topics relevant to their school subjects.
High-level Description	Marios is a primary school student in Limassol, Cyprus. He enjoys surfing the web. He has several social network accounts since he enjoys chatting with his friends and family. The last two days he opened a new Facebook group chat with two classmates, Fanos and Tim, discussing school subjects. Yet, Fanos and Tim started making fun of Mario's excessive weight. It all started as a joke but Marios couldn't afford being insulted in such a way. He was already trying to lose weight but has not been successful. Marios was depressed and his mother started worrying about her son being exposed to malicious behavior. Melanie found out about **ENCASE malicious behavior detection add-on** after searching the web. She decided to download the browser add-on on her son's laptop and on her own. Fanos and Tim continued insulting Marios and ENCASE malicious behavior add-on immediately detected and informed Marios that this conversation includes bullying. Melanie also received a similar notification, informing her about her son being a victim of malicious behavior. Melanie now is able to take action and discuss with her son how they should handle this type of attack.
Issues	Account creation: account on ENCASE malicious behavior add-on will be done by using basic personal information by the parent (i.e., email and password). Having

	created account on ENCASE, the parent will be able to detect and to get notified (via email or sms) on potential malicious behaviour online for any device the add-on has been installed.
Benefits	The ENCASE add on enables the parent and child to be notified on possible malicious behavior and take immediate action for protecting its child.
Notes	-
Services	Malicious behavior detection browser add-on

3.1.3. Scenario 2: Malicious behavior – Sexual assault

Code number	A.2
Name	Malicious behavior - Sexual assault
Author/Partner	CUT
Stakeholders	Serena is a 14 year old primary school student in Barcelona. She enjoys social media activity and has accounts on Facebook and Twitter. She is very outgoing, she enjoys meeting new people especially through social networks. Daniel is 22 year old, working as a DJ in a well-known club in Barcelona. He is very active in posting photos and videos from his work on Facebook and meeting new girls.
High-level Description	Serena is a 14 year old primary school student living in Barcelona. She enjoys social media activity and has accounts on Facebook and Twitter. She is very outgoing, she enjoys meeting new people especially through social networks. Being so active in social networks, Serena recently attended a seminar at her school related to "Cyber grooming in online social networks". She found out about **ENCASE malicious behaviour detection add-on** and she decided to give it a try. She downloaded it on her mobile and laptop browser few days ago. Serena is now browsing through her Facebook account, and amongst the suggested friends is a handsome young guy known as Daniel Stringini. She decides to send him a friend request and as soon as he accepts she drops him a friendly message in his inbox. They found each other living near-by and having similar interests and activities. Serena was happy as she found someone so mature and friendly to talk with, yet Daniel had other plans. He started approaching her using sexual hints about her body. The ENCASE malicious behaviour add-on gave its first yellow notification warning her that there is a danger for malicious behaviour. Serena ignored the notification as she enjoyed being admired. After a few days Daniel started asking her to meet and fully enjoy each other. Then ENCASE add-on gave a second red alert requesting her to stop communicating with this person as he is probably trying to sexually abuse her. Serena deleted Daniel from her friends and informed her friends and family about the incident.
Issues	Language: the ENCASE add-on will be in place to detect (using machine learning techniques) malicious behaviour in English.
Benefits	ENCASE add-on protected Serena from being exposed to sexual assault by a stranger.
Notes	Levels of alert: 1. Yellow alert: the victim should receive this type of alert when the probability for sexual assault is below a threshold. 2. Red alert: the victim should receive this type of alert when the probability for sexual assault is above a threshold.

Services	Malicious behavior detection browser add-on

3.1.4. Scenario 3: Fake identity and activity detection

Code number	A.3
Name	Fake identity and activity detection
Author/Partner	CUT
Stakeholders	Serena is a 15 year old primary school student in Barcelona. She enjoys social media activity and has accounts on various Social Networks. She enjoys meeting new people especially through social networks. Daniel is 35 year old, working as a taxi driver in Barcelona.
High-level Description	Serena is a 15 year old primary school student living in Barcelona. She enjoys social media activity and has accounts on Facebook and Twitter. She is very outgoing, she enjoys meeting new people especially through social networks. Being so active in social networks, Serena's mother encouraged her to install the **ENCASE Fake identity and activity detection browse**r add-on on her browser. Serena is now browsing through her Facebook account, and receives a friendship request from a guy called "Jonathan Stringini". Daniel has created a fake profile using this nickname on Facebook with a fake profile picture pretending an 19 years old guy working as a barman in a well-known club in Barcelona. She likes his profile and decides to accept his request. As soon as she accepts, Daniel drops a private message in her inbox. Immediately, Serena receives a notification for fake identity and activity detection for the specific account. The ENCASE add-on advised her to ignore the message. Serena deleted Jonathan from her friends and informed her friends and family about the incident.
Issues	-
Benefits	Serena was timely informed on the fake identity of Jonathan and protected herself from undesired activity.
Notes	-
Services	Fake identity and activity detection browser add-on

3.1.5. Scenario 4: Bad reputation for cyberbullying

Code number	A.4
Name	Bad reputation for cyberbullying
Author/Partner	CUT
Stakeholders	Serena is a 15 year old primary school student in Barcelona. She enjoys social media activity and has accounts on various Social Networks. She enjoys meeting new people especially through social networks. Daniel is 20 year old, currently unemployed. He is very active in social networks and has been recently voted by a lot of ENCASE users as a possible cyber buller due to demonstrating malicious behaviour towards other users.
High-level Description	Serena is a 15 year old primary school student living in Barcelona. She enjoys social media activity and has accounts on Facebook and Twitter. She enjoys meeting new people especially through social networks. Being so active in social networks, Serena's mother encouraged her to install the **ENCASE Fake identity and activity detection add-on** on her browser. Serena is now browsing through her Facebook account, and receives a friendship request from Daniel Stringini. She likes his profile and decides to accept his request. As soon as she accepts, Serena receives a notification that the specific

	profile has bad reputation within the ENCASE ecosystem as a cyber bully or predator. Serena decided to delete Daniel from her Facebook friends and informed her friends and family about the incident.
Issues	-
Benefits	Serena was timely informed on Daniel's previous malicious behaviour before he got the opportunity to attack her.
Notes	We will employ sophisticated reputation mechanisms to assess the veracity and the weight of each voter and their tags.
Services	Fake identity and activity detection browser add-on

3.1.6. Scenario 5: False information dissemination

Code number	A.5
Name	False information dissemination
Author/Partner	CUT
Stakeholders	Andreas is a 17 year old guy from Cyprus. He is a secondary school student in Limassol. He enjoys social media activity and he has accounts in various social networks. Peter is 28 years old, he is also from Cyprus and he has studied Computer Engineering at University of Piraeus.
High-level Description	Andreas is a 17 years old secondary school student in Limassol. Andreas enjoys social media activity and has accounts on various Social Networks. Being so active, he has recently installed the **ENCASE fake activity and identity detection browser add-on** in order to be able to identify users with malicious activity. Peter has studied Computer Engineering and he was working the last three years as a Programmer for a company in Greece. The last month Peter decided to quit his job and find a new one in his home country. A few days ago, Andreas and Peter applied for a job position at an R&D company in Cyprus. Peter, having heard that he is not the only one interested in this job position, he sent a Facebook friend request to the manager of the company in order to undermine Andreas and get the job. When the manager accepts the friend request, Peter sends him a message telling him that Peter is not a good programmer and that they should reject his job application. At the same time, Andreas receives a notification from the ENCASE add-on informing him that the user "Peter Solomou" is spreading false information about him on Facebook. Andreas decided to communicate with the company in order to report this incident and recover his reputation.
Issues	-
Benefits	Andreas was timely informed from the ENCASE add-on about the false information spread about him on social networks and he was able to take measures in order to recover his reputation
Notes	-
Services	Fake identity and activity detection browser add-on

3.1.7. Scenario 6: User receives false information

Code number	A.6
Name	User receives false information
Author/Partner	CUT
Stakeholders	Andreas is an 18 year old guy who is currently unemployed. He enjoys social

	media activity and has accounts on various Social Networks.
High-level Description	Andreas is an 18 years old guy who has just completed high school studies. He is currently unemployed and he is looking for a job the last one year. He also enjoys social media activity and has accounts on various Social Networks. Being so active, Andreas has recently installed the **ENCASE fake activity and identity detection browser add-on** in order to be able to identify and avoid malicious users with fake identities and/or activity. Andreas is a member in a Facebook page where news about job positions are posted. Yesterday, the administrator posted a few details about a company that is looking forward to hire a driver and Andreas commented on the post requesting for more information about the job position. Immediately, another member of the group who was also interest about the job and has been informed about from LinkedIn dropped him a message in his inbox. With this message this user was trying to fool Andreas providing him with false information about the job in order prevent Andreas from applying for this position. At the same time Andreas receives a notification from the ENCASE add-on informing him that the information he has received is false. Then Andreas ignored the false information and reported the malicious user.
Issues	-
Benefits	The ENCASE add-on enables the user to be notified when he receives false information of any kind and be sure that he always receives valid information from other users on social networks.
Notes	-
Services	Fake identity and activity detection browser add-on

3.1.8. Scenario 7: Sensitive photo detection and protection

Code number	A.7
Name	Sensitive photo detection and protection
Author/Partner	CUT
Stakeholders	Serena is a 16 year old high school student in Barcelona. She enjoys social media activity and has accounts on various Social Networks.
High-level Description	Serena enjoys using Facebook for sharing her holiday photos with her friends. Being so active in photo-sharing, her mother, Fedra, installs **ENCASE sensitive content detection and protection add-on** on her personal devices. This year Serena visited Mallorca and took a lot of pictures with her family in various occasions. She tried to upload one of her photos as her profile picture, but she received the following warning from the ENCASE add-on: Photo cannot be uploaded on your profile as it contains more than 80% nude content. Having seen the message, Serena decided to privately share the photo to her friends. The ENCASE add-on informed her of being able to share the photo and using steganography/watermarking or the following cryptographic techniques: group encryption and attribute-based encryption. Serena decided to use Group encryption to protect her photo and ensure that only her friends has access to this photo.
Issues	The browser add-on gives the user multiple ways to protect the sensitive photo that is going to be shared but it is up to the user to decide which technique is going to use.
Benefits	ENCASE sensitive content detection and protection browser add-on protected

	Serena from publicly sharing a photo that contains nudity on Facebook, providing her with alternatives in sharing the photo properly.
Notes	-
Services	Sensitive content detection and protection browser add-on

3.1.9. Scenario 8: Sensitive information detection and protection

Code number	A.8
Name	Sensitive information detection and protection
Author/Partner	CUT
Stakeholders	Serena is a 14 year old high school student in Barcelona. She enjoys social media activity and has accounts on various Social Networks. She used to share her personal information through chat messages or posts on Social Networks and she is unaware that her information is shared with inappropriate audience.
High-level Description	Serena enjoys using Facebook for discussing and meeting new friends. She used to share her personal information through chat messages or posts on Social Networks and she is unaware of the dangers behind sharing such type of information online. Serena recently participated in a seminar related to e-safety and was informed that sharing this type of data could end in being available to inappropriate audience. She was also informed about **ENCASE sensitive content detection and protection add-on**. Using Facebook to share her phone number to her new friend, Serena received a notification from the ENCASE add-on, reminding her that is not safe to share this type of information online. Serena deleted the message and felt secure after she received the ENCASE alert.
Issues	The browser add-on gives the user multiple ways to protect the sensitive information that is going to be shared but it is up to the user to decide which technique is going to use.
Benefits	ENCASE sensitive content detection and protection browser add-on protected Serena from publicly sharing personal information that should not be shared with inappropriate audience, providing her with alternatives in sharing the information properly and to her preferred persons.
Notes	-
Services	Sensitive content detection and protection browser add-on

3.1.10. Scenario 9: Secure sharing of sensitive content in OSNs

Code number	A.8
Name	Secure sharing of sensitive content in OSNs
Author/Partner	CUT
Stakeholders	Serena is a 18 year old high school student in Barcelona. She enjoys social media activity and has accounts on various Social Networks. She used to share her personal information through chat messages or posts on Social Networks. Fedra, is Serena's mother.
High-level Description	Serena is a 18 year old high school student in Barcelona. She is very active, especially on Facebook and she enjoys to share her personal information through chat messages or posts on Social Networks. Being so active in photo-sharing, her mother, Fedra, installs **ENCASE sensitive content detection and protection add-on** on her personal devices. Since Serena accepted to use the ENCASE add-on to securely share photos with her friends, they exchanged a common password that they all use to encrypt and decrypt the photos.

	Serena today is at the beach and she is capturing selfies that she wants to share through Facebook with her friends. She is trying to upload the photo and tag her friends on the photo, but she received the following warning from the ENCASE add-on: Photo cannot be shared as it contains more than 80% nude content. The ENCASE add-on also informed her of being able to share the photo and using steganography/watermarking or the following cryptographic techniques: group encryption and attribute-based encryption. Having seen the message, Serena decided to privately share the photo to her friends using Group Encryption. She encrypted the photo using the password exchanged from before with her friends before sharing the photo. Then, her friends were able to access and see that photo and no other that is unaware of the password is able to access the photo.
Issues	The browser add-on gives the user multiple ways to protect the sensitive information that is going to be shared but it is up to the user to decide which technique is going to use.
Benefits	ENCASE sensitive content detection and protection browser add-on provides Serena with multiple ways for sharing her sensitive photos properly with her preferred persons without sharing it with inappropriate audience.
Notes	-
Services	Sensitive content detection and protection browser add-on

3.2.Use Case B – Parental Awareness

3.2.1. Use case purpose

The goal of the parental awareness is to detect and inform parents when their children have become victims of cyberbullying and/or sexual predators. Also, parents should be informed when their children are experiencing or are about to experience distress behavior. Except these, parents should be informed when their children are communicating with someone that has fake identity and/or activity and/or bad reputation for malicious behavior and when they are about to share sensitive content (of any type) with inappropriate audience.

3.2.2. Scenario 1: Malicious behavior detection and report

Code number	B.1
Name	Malicious behavior detection and report
Author/Partner	CUT
Stakeholders	Stephanie is a student (age 16) at a high school in Limassol. Stephanie has several social network accounts since she enjoys chatting with her friends and family. Melanie is Stephanie's mother. She is familiarized with social media and she is a Facebook friend with her daughter. Peter is a 19 years old guy who is doing his army duty in the Cyprus Army. He has a lot of free time and he likes spending it surfing the web. He also has various Social Network accounts and he likes meeting and chatting with new girls.
High-level Description	Stephanie is a 16 year old high school student living in Limassol. She enjoys social media activity and she loves chatting with her friends and family. She also enjoys meeting new people especially through social networks. Stephanie's mother, Melanie, was a little worried about her daughter's online activity and the people that she used to meet online. On a discussion that

	Melanie has with some other parents she get informed about **ENCASE malicious behavior detection add-on** and she decided to give it a try. She downloaded the add-on on her daughter's mobile and laptop browser few days ago. Yesterday, Stephanie received a Facebook friend request from a handsome young guy known as Peter Michael. She found him interesting and she decided to accept the request and add him as a friend. After a few hours, Peter dropped her a friendly message in her inbox. After a few days of chatting with Peter, Stephanie was excited but day by day Peter's behavior was changing until he started approaching her using sexual hints about her body and asking her to meet and fully enjoy each other. Here, the ENCASE malicious behavior detection add-on took place and gave her a notification warning her that there is a danger for malicious behavior from Peter. At the same time the add-on also sends a notification to Stephanie's mother that there is a possibility her daughter is exposed to a danger related to malicious behavior. After being notified, Melanie talked to her daughter and advised her to stop communicating with Peter and delete him from her Facebook friends' list.
Issues	-
Benefits	The ENCASE add on enables the parent to be notified on possible occasions where its child might be a victim of malicious behavior and to be able to take immediate action for protecting its child.
Notes	-
Services	Malicious behavior detection browser add-on

3.2.3. Scenario 2: Distressed behavior detection and report

Code number	B.2
Name	Distressed behavior detection and report
Author/Partner	CUT
Stakeholders	Marios is a student (age 13) at a primary school in Limassol. He enjoys surfing the web. He has several social network accounts since he enjoys chatting with his friends and family. Melanie is Mario's mother. She is familiarized with social media and a friend with her son. Fanos is Mario's fellow student (age 13). He is also Mario's best friend. They both have a Facebook account and they use to chat from their discussing everything.
High-level Description	Marios is a primary school student in Limassol, Cyprus. He enjoys surfing the web. He has several social network accounts since he enjoys chatting with people and especially with his best friend Fanos. Recently Marios has been a victim of bullying by two other students at his school. They started making fun of Mario's excessive weight. It all started as a joke but Marios couldn't afford being insulted in such a way. Marios was depressed and his mother started worrying about her son's behavior. After searching the web, Melanie found out about the **ENCASE malicious behavior detection add-on** and that it was able to detect distressed behavior. After searching the web. Since she knew that her son used to share everything with his best friend through Facebook chat, the ENCASE add-on was her best chance to find out if her son's behavior was something more than just stress. She decided to download the browser add-on on her son's laptop and on her own. A day after, while chatting with Fanos through Facebook, Marios told him that he

	cannot afford bullying anymore and that he wanted to set an end to his life. Immediately, the ENCASE add-on detected a distressed behavior and Melanie received a notification, informing her about her son's distressed behavior. Melanie now is able to take action and discuss with her son how they should handle this situation.
Issues	Language: the ENCASE add-on needs to be in place to detect (using machine learning techniques) malicious behavior in multiple languages including English, Greek, Spanish, Italian and German
Benefits	The ENCASE add on enables the parent to be notified on possible situations where its child is expressing distressed behavior and take immediate action for protecting its child.
Notes	-
Services	Malicious and distressed behavior detection browser add-on

3.2.4. Scenario 3: Bad reputation for cyberbullying

Code number	B.3
Name	Bad reputation for cyberbullying
Author/Partner	CUT
Stakeholders	Stephanie is a 16 year old high school student in Barcelona. She enjoys social media activity and has accounts on various Social Networks. She enjoys meeting new people especially through social networks. Melanie is Stephanie's mother. She is familiarized with social media and she is a Facebook friend with her daughter. Daniel is 18 year old, currently unemployed. He is very active in social networks and has been recently tagged by ENCASE ecosystem as a possible cyber bully due to demonstrating malicious behavior towards other users.
High-level Description	Stephanie is a 16 year old high school student living in Barcelona. She enjoys social media activity and has accounts on Facebook and Twitter. She enjoys meeting new people especially through social networks. Being so active in social networks and having heard that a lot of people exists that have malicious behavior in Social Networks, Stephanie's mother encouraged her to install the **ENCASE Fake identity and activity detection add-on** on her browser. Stephanie is now browsing through her Facebook account, and receives a friendship request from Daniel Stringini. She likes his profile and decides to accept his request. As soon as she accepts, Daniel drops a private message in her inbox. Immediately, Stephanie receives a notification that the specific profile has bad reputation within the ENCASE ecosystem as a cyber-bully or predator and warns her for ignoring his message. Stephanie instead, ignores the notification and replies to Daniel's message. At the same time, Stephanie's mother receives a notification that her child is communicating with someone who has bad reputation within the ENCASE ecosystem as a cyber-bully or predator. After being notified, Melanie talked to her daughter and advised her to stop communicating with Daniel and delete him from her Facebook friends' list.
Issues	-
Benefits	Stephanie's mother was timely informed that her daughter was communicating with Daniel who has previous malicious behavior for cyberbullying before he got the opportunity to attack to Stephanie.

Notes	-
Services	Fake identity and activity detection browser add-on

3.2.5. Scenario 4: Fake identity and activity detection

Code number	B.4
Name	Fake identity and activity detection
Author/Partner	CUT
Stakeholders	Stephanie is a 15 year old primary school student in Barcelona. She enjoys social media activity and has accounts on various Social Networks. She enjoys meeting new people especially through social networks. Melanie is Stephanie's mother. She is familiarized with social media and she is a Facebook friend with her daughter. Daniel is 40 year old, working as a taxi driver in Barcelona.
High-level Description	Stephanie is a 15 year old primary school student living in Barcelona. She enjoys social media activity and has accounts on Facebook and Twitter. She is very outgoing and she enjoys meeting new people especially through social networks. Being so active in social networks, Stephanie's mother encouraged her to install the **ENCASE fake identity and activity detection add-on** on her browser. Stephanie is now browsing through her Facebook account, and receives a friendship request from a guy called "Jonathan Stringini". Daniel has created a fake profile using this nickname on Facebook with a fake profile picture pretending a 19 years old guy working as a barman in a well-known club in Barcelona. This profile was well-constructed by Daniel with a lot of photoshopped photos of a fake person and it was very difficult for someone to identify it is a fake profile. Stephanie likes his profile and decides to accept his request. As soon as she accepts, Daniel drops a private message in her inbox. Immediately, Serena receives a notification for fake identity and activity detection for the specific account. The ENCASE add-on advised her to ignore the message. Stephanie instead, ignored the notification since "Jonathan" looks to be a real person. She also replies to Daniel's message. At the same time, Stephanie's mother receives a notification by the ENCASE add-on, informing her that there is possibility her child is communicating with a user on Facebook that has fake identity and activity. Then, Melanie advised her daughter to stop communicating with this person and delete him from her friends.
Issues	-
Benefits	Stephanie's mother was timely informed on the fake identity of Jonathan and protected her daughter from undesired activity.
Notes	-
Services	Fake identity and activity detection browser add-on

3.2.6. Scenario 5: Share sensitive content with inappropriate audience

Code number	B.5
Name	Share sensitive content with inappropriate audience
Author/Partner	CUT
Stakeholders	Stephanie is a 15 year old primary school student in Barcelona. She enjoys social media activity and has accounts on various Social Networks. She used to share

	her personal photos through chat messages or posts on Social Networks and she is unaware that her photos are shared with inappropriate audience. Melanie is Stephanie's mother and she is not so familiar with social media.
High-level Description	Stephanie enjoys using Facebook for chatting and sharing her photos with her friends. Being so active in photo-sharing, her mother, Melanie, is worried about what type of photos her daughter is sharing to social networks. Recently, Melanie attended at a seminar, that a police department organized for parents, regarding ways to control what children are sharing through social network. She heard there about the **ENCASE sensitive content detection and protection add-on** and she decided to install it on her daughter's personal devices. Yesterday Stephanie visited a store near her home in order to see the new available swimsuits and find out which one likes more and buy it. Apparently, she found herself confused with the amount of choices she has and she decided to try them and took photos in order to share them with her friends and help her decide which one she should buy. She tried to upload one of those photos to Facebook, but she received the following warning from the ENCASE add-on: Photo cannot be uploaded as it contains more than 80% nude content. At the same time, Stephanie's mother received a notification informing her that her daughter is trying to upload a photo that contains more than 80% nude content. Immediately, Melanie called her and she urged her to not upload it but to use Group encryption, that ENCASE add-on offers, to protect her photo and ensure that only her friends has access to this photo.
Issues	The browser add-on gives the user multiple ways to protect the sensitive photo that is going to be shared but it is up to the user to decide which technique is going to use.
Benefits	ENCASE sensitive content detection and protection browser add-on helped Melanie to protect Serena from publicly sharing a photo that contains nudity on Facebook.
Notes	-
Services	Sensitive content detection and protection browser add-on

3.3.Use Case C – Educators' Awareness

3.3.1. Use case purpose

The goal of this category is to raise educators' awareness in understanding the risks undertaken in the use of social media for educational purposes.

3.3.2. Scenario 1: Malicious behavior detection

Code number	C.1
Name	Malicious behavior detection
Author/Partner	CUT
Stakeholders	Mary is a German language instructor in a secondary school in the UK. She has just completed her studies in German language and culture and her MA in Computer-Assisted Language Learning.
High-level	Mary is a 30 year old German language instructor. Having completed her studies

Description	in German language and culture and her MA in Computer-Assisted Language Learning she is appointed as a German language instructor in a secondary school in the UK. Being a social media savvy, Mary decides to incorporate social media in her teaching and creates a Facebook group where her students can use the target language in authentic environments. Yet, Mary accepts negative criticism from her school director for "exposing children in malicious behavior in social media". Mary is initially insulted by the critique but then decides to find out more about the risks of social media in schools. She came across **ENCASE malicious behavior detection add-on** and she decides to install it for protecting her class from malicious behavior.
Issues	-
Benefits	Mary is now in place to protect her class from malicious behavior and demonstrate to her school ways for using safely social media for educational purposes.
Notes	-
Services	Malicious behavior detection add-on

3.3.3. Scenario 2: Fake identity and activity detection

Code number	C.2
Name	Fake identity and activity detection
Author/Partner	CUT
Stakeholders	Mary is a German language instructor in a secondary school in the UK. She has just completed her studies in German language and culture and her MA in Computer-Assisted Language Learning. Kevin Kalen has just completed his high school degree and he is currently unemployed. He enjoys surfing in social media and meeting new people.
High-level Description	Mary is a 30 year old German language instructor. Having completed her studies in German language and culture and her MA in Computer-Assisted Language Learning she is appointed as a German language instructor in a secondary school in the UK. Being a social media savvy, Mary decides to incorporate social media in her teaching and creates a Facebook group where her students can use the target language in authentic environments. She creates the group and all of her students join with high level of excitement. All of a sudden, a new member appears in the group from someone called Kevin Kalen. Kevin posted that one of the students in the group had passed away and everyone in the group got very upset. Immediately upon posting, Mary received a notification from the ENCASE add on she had installed on her computer. The add-on informed her that the information given by Kevin Kalen is probably fake. Mary deleted Kevin from the group and informed her students about the incident. She also gave them a short information handout on how the ENCASE add-on can protect them from fake and malicious actions.
Issues	-
Benefits	Mary and her class were immediately protected from a fake account.
Notes	-
Services	Fake identity and activity detection add-on

3.3.4. Scenario 3: Sensitive content with inappropriate audience

Code number	C.3

Name	Share sensitive content with inappropriate content
Author/Partner	CUT
Stakeholders	Mary is a German language instructor in a secondary school in the UK. She has just completed her studies in German language and culture and her MA in Computer-Assisted Language Learning. Peter Smith is one of Mary's students. He is very keen in using social media and meeting new people.
High-level Description	Mary is a 30 year old German language instructor. Having completed her studies in German language and culture and her MA in Computer-Assisted Language Learning she is appointed as a German language instructor in a secondary school in the UK. Being a social media savvy, Mary decides to incorporate social media in her teaching and creates a Facebook group where her students can use the target language in authentic environments. She creates the group and all of her students join with high level of excitement. Peter, one of Mary's students, tries to post one of his photos from his holidays in Germany during the summer wearing a swimming suite. Immediately, Mary receives a notification from the ENCASE add-on that sensitive/inappropriate content is being rejected from the group. Peter is also notified and is informed that 80% nudity is unacceptable and photo will be deleted.
Issues	-
Benefits	Mary and her class is protected from sensitive and inappropriate content within social media.
Notes	-
Services	Sensitive content detection and protection

4. System Requirements

4.1. User Stories and Acceptance criteria

4.1.1. Malicious Behavior (Cyberbullying and sexual predators) detection

Code number	MBD1
Title	Link child's add-on with parent's malicious behavior add-on
Description	**As a parent** **I want to** get notified when my child may be a victim of malicious behavior in OSNs **so that** i can take measures and prevent any undesired incidents
Acceptance criteria	1. A parent should be able to create an account and link it with its child OSN account. 2. The system should require an email address for registration. 3. The ENCASE add-on should verify the declared, by the parent, email address. 4. A child must provide its consent in order for the parent to be notified in case of malicious behavior detection. 5. A parent should be able to receive notification on his browser or via email. 6. Both parent and child should be able to unlink his/her account from each

	other.

Code number	MBD2
Title	Minor may become a victim of cyberbullying
Description	**As a minor** **I want to** get timely notified when someone is trying to bully me through a social network **so that** i can avoid such malicious users
Acceptance criteria	1. The browser add-on should timely detect cyberbullying and notify the user. 2. The add-on should provide levels of alert when malicious behavior is detected: Levels of alert: a. Yellow alert: the victim should receive this type of alert when the probability for assault is below a threshold. b. Red alert: the victim should receive this type of alert when the probability for assault is above a threshold. 3. Anyone that is flagged as sexual predator is being noted in the system using a reputation score. The reputation score increases each time someone is flagged as sexual predator. 4. The minor should be able to permanently ignore the notification in cases where she/he is sure that there is no cyberbullying.

Code number	MBD3
Title	A child may become a victim of cyberbullying
Description	**As a parent** **I want to** get timely notified when someone is trying to bully my child through a social network **so that** i can take the appropriate measures
Acceptance criteria	1. The parent should be able to link the ENCASE add-on on her/his child's device with the add-on installed on her device. 2. The ENCASE add-on should request from the parent some basic information (email/phone number, password) in order to request to link her/his device with the add-on installed on her child's device. 3. The ENCASE add-on should timely detect cyberbullying and notify the parent and the child. 4. The add-on should provide levels of alert when malicious behavior is detected: a. Yellow alert: the victim should receive this type of alert when the probability for cyberbullying is below a threshold. b. Red alert: the victim should receive this type of alert when the probability for cyberbullying is above a threshold.

Code number	MBD4
Title	Minor may become a victim of a sexual predator
Description	**As a minor** **I want to** get timely notified when i am communicating with someone that may be a possible sexual predator **so that** i can avoid him

Acceptance criteria	1. The add-on should be able to timely detect sexual assault 2. Anyone that is flagged as sexual predator is being noted in the system using a reputation score. The reputation score increases each time someone is flagged as sexual predator. 3. The add-on should provide levels of alert when malicious behavior is detected: Levels of alert: a. Yellow alert: the victim should receive this type of alert when the probability for assault is below a threshold. b. Red alert: the victim should receive this type of alert when the probability for assault is above a threshold. 4. The minor should be able to get notified in case of sexual assault

Code number	MBD5
Title	A minor may become a victim of a sexual predator
Description	**As a parent** **I want to** get timely notified when my child is communicating with a possible sexual predator **so that** i can prevent any undesired incident
Acceptance criteria	1. The ENCASE add-on should timely detect sexual assault and notify the parent and the child. 2. When sexual assault is detected the add-on should provide visual and/or textual notification to the parent and child 3. The add-on should provide levels of alert when malicious behaviour is detected: a. Yellow alert: the victim should receive this type of alert when the probability for assault is below a threshold. b. Red alert: the victim should receive this type of alert when the probability for assault is above a threshold.

Code number	MBD6
Title	Minor is about to experience distress or aggressive behavior
Description	**As a parent** **I want to** get notified when my child is about to express distress or aggressive behavior **so that** i can take measures to prevent any undesired incidents
Acceptance criteria	1. The add-on should be able to capture and analyze the user's social network activity in order to detect if she/he is about to express distress or aggressive behavior. 2. The ENCASE add-on should be able to notify (in visual or in textual way) the parent when his child is about to experience distress or aggressive behavior. 3. The add-on should provide hierarchical notifications based on the percentage of distress or aggressive behavior extracted from the analysis.

4.1.2. Fake identity and activity detection

Code number	FID1
Title	User with fake identity detection

Description	**As a minor** **I want to** get notified when I have a friend in social networks with fake identity **so that** I can report and delete them from my social network friend's list
Acceptance criteria	1. The add-on should be able to access a minor's friend's list. 2. The add-on should be able to analyze profiles that the minor visits on social networks and notify him when a profile is fake one before he decides to befriend it. 3. The add-on should be able to detect fake identify from basic profile information 4. Upon detection, the minor should be notified that the account is flagged as fake 5. The add-on should create a list with all flagged fake accounts for future reference.

Code number	FID2
Title	User with bad reputation due to cyberbullying or predation
Description	**As a minor** **I want to** get notified when I am communicating with a user with bad reputation due to cyberbullying or predation **so that** I can report and delete him from my social network friend's list
Acceptance criteria	1. The ENCASE add-on should detect when a user is communicating on social networks with another user that has bad reputation on the ENCASE ecosystem for cyber bullying or sexual predation. 2. The add-on should notify the minor when he/she is communicating with a user with bad reputation.

Code number	FID3
Title	False information dissemination
Description	**As a user** **I want to** get notified when false information about me are spread over a social network **so that** I can take measures to stop that and to restore my reputation
Acceptance criteria	1. The ENCASE fake identity and activity add-on should scan the social network information of the user. 2. The add-on should associate the extracted info with the data being analyzed in the back-end in order to detect any false information about the user. 3. The add-on should be able to timely notify false information about me spread on the network.

Code number	FID4
Title	User receives false information
Description	**As a user** **I want to** get notified when I receive false information of any type **so that** I can report and ignore it
Acceptance criteria	1. The add-on should be able to collect and analyze any information that the user receives in social network.

	2. The add-on should be able to detect any false information that is included in the collected dataset. 3. The add-on should notify the user when false information is included in the information he/she receives.

4.1.3. Sensitive content detection and protection

Code number	SCD1
Title	A minor is about to share a sensitive photo with inappropriate audience
Description	**As a minor** **I want to** get notified when I am about to share a sensitive photo with inappropriate audience… **so that** I can take measures to prevent sharing it with inappropriate audience
Acceptance criteria	1. The add-on should be able to scan and accumulate percentage of nudity in a photo that the minor is about to share. 2. The add-on should notify the user of being in danger to share sensitive photo with inappropriate audience. 3. The add-on should prevent sharing photo if the nudity percentage exceeds 75%. 4. The add-on should be able to provide alternative ways (e.g., encryption) for securely sharing sensitive photos.

Code number	SCD2
Title	A child is about to share a sensitive photo with inappropriate audience
Description	**As a parent** **I want to** get notified when my child is about to share a sensitive photo with inappropriate audience **so that** i can prevent that.
Acceptance criteria	1. The add-on should be able to scan and accumulate percentage of nudity in a photo that a child is about to share. 2. The add-on should notify the parent of his/her child's activity -being in danger to share a sensitive photo with inappropriate audience.

Code number	SCD3
Title	A minor is about to share a sensitive information with inappropriate audience
Description	**As a minor** **I want to** get notified when I am about to share sensitive information with inappropriate audience **so that** I can take measures to prevent sharing it with inappropriate audience
Acceptance criteria	1. The add-on should scan and prevent sharing of sensitive information with inappropriate audience. 2. The add-on should notify the child of risking to share sensitive information with inappropriate audience.

Code number	SCD4
Title	A child is about to share a sensitive information with inappropriate audience
Description	**As a parent** **I want to** get notified when my child is about to share sensitive information with

	inappropriate audience **so that** I can take measures to prevent it.
Acceptance criteria	1. The add-on should scan and prevent sharing of sensitive information with inappropriate audience. 2. The add-on should notify the parent of his/her child's activity -being in danger to share sensitive information with inappropriate audience.

Code number	SCD5
Title	Securely share sensitive content
Description	**As a user** **I want to** be able to securely share sensitive content through social networks **so that** i can prevent it to be shared with inappropriate audience
Acceptance criteria	1. The ENCASE sensitive content detection and protection should allow the user to securely share sensitive content on Social networks using: a. Group encryption b. Attribute-based encryption c. Watermarking d. Steganography

4.2.Operational Requirements

#	Operational Requirements	Rational / Comments	Mandatory (YES/NO)
O1.1	The add-ons should be intuitive in its use by both advanced social media users and amateurs.	-	YES
O1.2	The add-on should allow for easy accomplishment of tasks (i.e. installment) by both advanced social media users and amateurs.	-	YES
O1.3	The add-on should avoid complicated calculation in its interface, to avoid any performance issues.	All the analysis of the collected information should be performed in the back-end of the ENCASE framework.	YES
O1.4	The user should be able to install each add-on separately.	-	YES
O1.5	The GUI of each add-on should be	As the add-on will be used by	YES

	pleasant and attractive to use	children the GUI of the add-on should be pleasant and attractive.	
O1.6	The user should be able to easily recover from errors	The user should be able to disconnect a device that by mistake requested link.	YES
O1.7	The user should be able to create account within the ENCASE ecosystem	-	YES
O1.8	User registration must be fast	-	YES
O1.9	Once registered the user can keep single sign-in for all three ENCASE add-ons.	-	NO
O1.10	The add-on should be able to notify users for sensitive content in spite of not being registered.	-	YES
O1.11	The add-ons should minimize the risk of product failing.	-	YES
O1.12	The add-ons should allow the users to provide feedback to administrators.	-	NO
O1.13	The add-ons should provide step-by-step guidance to users upon registration.	-	YES
O1.14	The add-ons should timely send notifications to users	Upon detection of a threat the add-ons should notify the user fast (e.g., less than 5 sec.)	YES
O1.15	The communication protocols between the add-ons and the back-end must be lightweight and simple.	-	YES
O1.16	The user should be able to set control of the add-ons by setting his/her preferences when receiving notifications.	-	YES

4.3.Security and Privacy Requirements

#	Security & Privacy Requirements	Rational / Comments	Mandatory (YES/NO)
S&P1.1	The system should not leak any user's personal information to other browser add-ons or to social networks.	-	YES
S&P1.2	All communication channels within ENCASE framework must use communication protocols that provide communication security (e.g., SSL or TLS).	-	YES
S&P1.3	All users personal information will not be linked to a physical person	-	YES
S&P1.4	Browser add-ons will not store any user's personal information locally.	-	YES
S&P1.5	The back-end service should be security-hardened so that it is very difficult to compromise.	-	YES
S&P1.6	The add-ons should securely collect user's social network information	-	YES

5. Software Architecture

The objectives of ENCASE stem from the need to safeguards the security and privacy of minors against malicious actors in OSNs like cyber bullies. The measurement-driven approach that ENCASE follows to assess the urgency and existence of threads like fake activity of online sexual abusers and cyber bullies in OSNs, will guide the design and the implementation of the mitigation mechanisms. Those mitigation mechanisms are browser add-ons where each one is responsible to mitigate one of the threads that ENCASE aims to tackle.

The first browser add-on that will be developed is responsible for malicious behavior detection. More specifically, this add-on will inform users of whether they have befriend or are communicating

with a person that is presently attempting to bully or exploit them, or has in the past exhibited aggressive behavior, or has caused other persons to exhibit emotional distress.

The second is responsible for fake identity and activity detection in OSNs. This browser add-on will enable users to be aware of whether they are communicating with a person that misrepresents its identity, and therefore its intentions, or are being the receivers of false information, or are themselves the subject of malicious false information that spreads through the network. Additionally, this browser add-on will be responsible to inform the user when he is communicating with a person that has bad reputation for cyber bullying or sexual assault.

The third browser add-on that will be implemented, scans an OSN user’s content that is about to be shared (e.g., a photo) in order to determine if it is sensitive. Subsequently, it provides informative alerts and enables the user to protect it from unwarranted leakage to unwanted recipients with easily learnable and usable interfaces.

Figure 3 depicts those mitigation mechanisms interacting with an OSN Data Analytics software stack under a unified architecture. The Data Analytics Software stack comprises libraries for aggressive or distressed online behavior detection, as well as fake user account, false information diffusion and audience boosting detection.

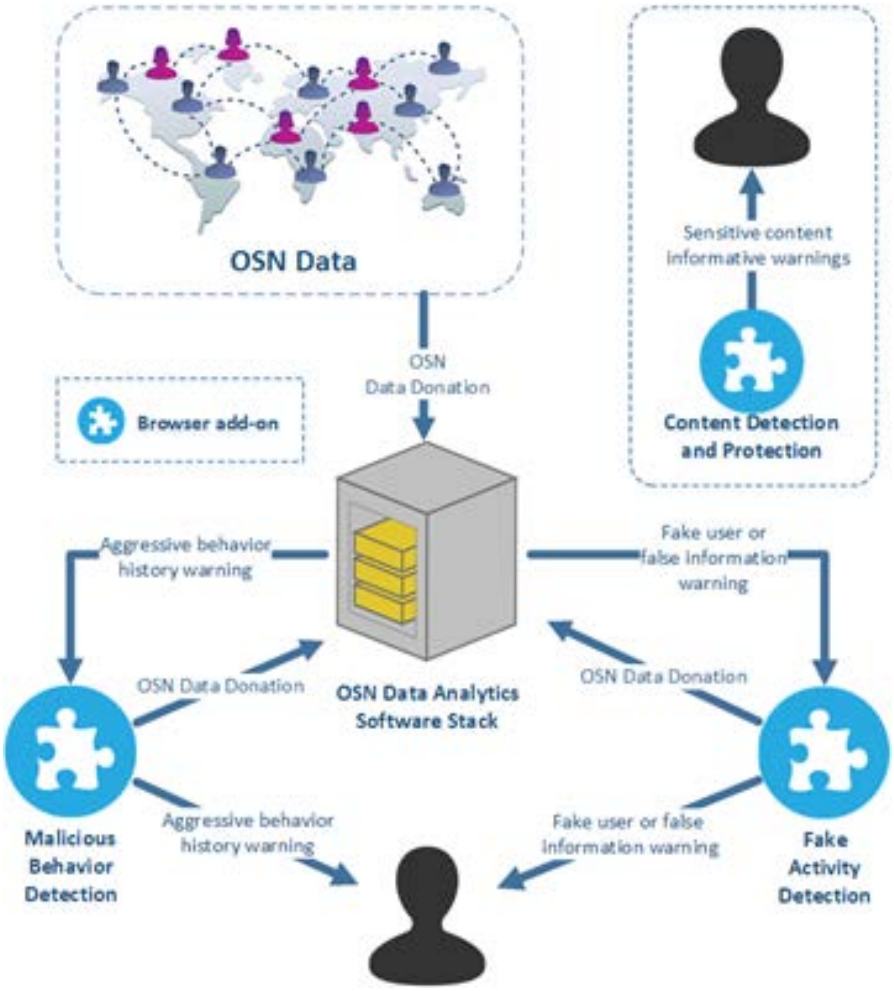

Figure 3. Software Architecture

6. Conclusion

This deliverable is fundamental to the subsequent stages of ENCASE for several reasons: (i) it provides a survey of existing security and privacy enhancing web-based tools related to ENCASE and also provides a survey of the research state-of-the-art where the initial system requirements have been extracted from; (ii) it defines the usage scenarios which are expressing the functionality of the three browser add-ons that will be implemented in the context of ENCASE; (iii) it defines the initial requirements for the three browser add-ons that will be implemented; and (iv) it provides an overview of the software architecture that will be the basis for the design of the final software architecture.

7. References

1. Requirements Engineering: A Good Practice Guide, 1st Edition, John Wiley & Sons, Inc. New York, NY, USA ©1997 ISBN:0471974447
2. S. Robertson, J. Robertson. Mastering the Requirements Process. AddisonWesley, 1999
3. Protect, understand and manage your kids internet activity with Qustodio. https://www.qustodio.com/en/
4. SocialShield: Avira Social Network Protection for your child. http://www.thewindowsclub.com/socialshield-review
5. Know which sites to trust. https://www.mywot.com/
6. Computer & Mobile monitoring software. http://www.webwatcher.com/?refID=lnkshr&siteID=Cty0dj6o3sg-GHtU.M9eT5Zlm7qQ5Ms1ig
7. Web Security Service. http://www.cloudacl.com/webfilter/
8. A. C. Squicciarini, J. Dupont, R. Chen, Online Abusive Analytics through Visualization
9. The Parental control for Firefox. https://addons.mozilla.org/en-US/firefox/addon/foxfilter/
10. Parental Controls & and Web Filter. https://chrome.google.com/webstore/detail/parental-controls-web-fil/dpfbddcgbimoafpgmbbjiliegkfcjkmn
11. MetaCert Security API. https://metacert.com/
12. eSafely protects you where your Web filter doesn't. http://www.esafely.com/
13. Nudity detection with JavaScript and HTMLCanvas. https://github.com/pa7/nude.js
14. ReThink. http://www.rethinkwords.com/
15. PureSight Online child safety. http://puresight.com/puresight-prevents-cyberbullying.html
16. MM Guardian Parental Control. https://play.google.com/store/apps/details?id=com.mmguardian.childapp
17. Funamo Parental Control. https://play.google.com/store/apps/details?id=funamo.funamo
18. Kids Place - Parental Control. https://play.google.com/store/apps/details?id=com.kiddoware.kidsplace
19. AppLock. https://play.google.com/store/apps/details?id=com.domobile.applock
20. Screen Time Parental Control. https://play.google.com/store/apps/details?id=com.screentime.rc&hl=en_GB
21. Net Nanny. http://purchmarketplace.com/pc-software-net-nanny-7-0-download-only-1/?&ICID=ttr-cid|544|pid|49840|pos|
22. Safe Eyes - Parental control software. http://www.internetsafety.com/safe-eyes-parental-control-software.php
23. Elite Keylogger. https://www.elitekeyloggers.com/elite-keystroke-recorder-info
24. Wright E.R. & Lawson A.H. (2004) Computer-Mediated Communication and Student Learning in Large Introductory Sociology Courses. Paper presented at the Annual Meeting of the American Sociological Association, Hilton San Francisco&Renaissance Parc 55 Hotel, San Francisco, CA. Available at: http://citation.allacademic.com/meta/p_mla_apa_research_citation/1/0/8/9/6/pages108968/p108968-1.php
25. Green H. & Hannon C. (2007) TheirSpace: Education for a Digital Generation. Demos, London. Available at: http://dera.ioe.ac.uk/23215/1/Their%20space%20-%20web.pdf
26. Wolak J., Finkelhor D., Mitchell K.J. & Ybarra M.L. (2008) Online 'predators' and their victims: myths, realities and implications for prevention and treatment. American Psychologist 63, 111–128.
27. Crook, C., & Harrison, C. (2008). Web 2.0 technologies for learning at key stages 3 and 4: summary report.

28. Naidoo, T., Kritzinger, E., & Loock, M. (2013, June). Cyber Safety Education: Towards a Cyber-Safety Awareness Framework for Primary Schools. In International Conference on e-Learning (p. 272). Academic Conferences International Limited.
29. Sharples, M., Graber, R., Harrison, C., & Logan, K. (2009). E-safety and Web 2.0 for children aged 11–16. Journal of Computer Assisted Learning, 25(1), 70-84.
30. Searson, M., Hancock, M., Soheil, N., & Shepherd, G. (2015). Digital citizenship within global contexts. Education and Information Technologies, 20(4), 729-741.
31. Waters, J. K. (2011). Social Networking: Keeping It Clean. The Journal, 38(1), 52.
32. Orech, J. (2012). How it's done: Incorporating digital citizenship into your everyday curriculum. Tech and Learning, 33(1), 16-18.
33. Ramnath, S. (2015). How schools can keep students safe, and on Facebook. eSchool News, 18(4), 16.
34. Campbell-Wright, K. (2013). E-safety. NIACE.
35. Sharples, M., Graber, R., Harrison, C., & Logan, K. (2009). E-safety and Web 2.0 for children aged 11–16. *Journal of Computer Assisted Learning*, *25*(1), 70-84.
36. Wespieser, K. (2015). Young People and E-Safety: The Results of the 2015 London Grid for Learning E-Safety Survey. National Foundation for Educational Research.
37. Lorenz, B., Kikkas, K., & Laanpere, M. (2011, November). Social Networks, E-learning and Internet Safety: Analysing the Stories of Students. In Proceedings of the 10th European Conference on e-Learning ECEL-2011: 10th European Conference on e-Learning ECEL-2011 Brighton, UK (pp. 10-11).
38. Lorenz, B., Kikkas, K., & Laanpere, M. (2012). Comparing Children's E-Safety Strategies with Guidelines Offered by Adults. Electronic Journal of e-Learning, 10(3), 326-338.
39. Moreno, M. A., Egan, K. G., Bare, K., Young, H. N., & Cox, E. D. (2013). Internet safety education for youth: stakeholder perspectives. BMC public health, 13(1), 543.
40. Cranmer, S. (2013). Listening to excluded young people's experiences of e-safety and risk. Learning, Media and Technology, 38(1), 72-85.
41. A SAFER DIGITAL WORLD.
42. Sharples, M., Graber, R., Harrison, C., & Logan, K. (2008). E-safety and Web 2.0: Web 2.0 technologies for learning at Key Stages 3 and 4.
43. Guidelines for children on child online protection. http://www.itu.int/en/cop/Pages/guidelines.aspx
44. Ofcom report on internet safety measures: Strategies of parental protection for children online. http://stakeholders.ofcom.org.uk/binaries/internet/internet-safetymeasures.pdf
45. Ofcom report on internet safety measures: Strategies of parental protection for children online. http://stakeholders.ofcom.org.uk/binaries/internet/fourth_internet_safety_report.pdf
46. M. Robinson. (2015, March) Koreas internet addiction crisis is getting worse, as teens spend up to 88 hours a week gaming. Business Insider. http://www.businessinsider.com/south-korea-online-gaming-addiction-rehab-centers-2015-3
47. A. Lenhart. (2015, April) Teens, social media & technology overview 2015. Pew Recearch Center: Internet, Science & Tech. http://www.businessinsider.com/south-korea-online-gaming-addiction-rehab-centers-2015-3
48. S. Livingstone, L. Haddon, J. Vincent, G. Mascheroni, and K. Olafsson. (2014) Net children go mobile: The uk report. London: London School of Economics and Political Science. https://www.lse.ac.uk/media@lse/research/EUKidsOnline/EUn%20Kidsn%20III/Reports/NCGMUKReportfinal.pdf

49. S. Livingstone, K. Cagiltay, and K. Olafsson, "Eu kids online ii dataset: A cross-national study of children's use of the internet and its associated opportunities and risks," British Journal of Educational Technology, vol. 46, pp. 988–992, August 2015.
50. T. Woda. (2015) Digital parenting: Understanding the risk of snapchat. uknowkids.com. http://resources.uknowkids.com/blog/digital-parenting-understanding-the-risk-of-snapchat
51. ACMA. (2009, July) Click and connect: Young australians use of online social media. Australian Communications and Media Authority. http://www.acma.gov.au/webwr/aba/about/recruitment/click_and_connect-01_qualitativen_report.pdf
52. Developments in internet filtering technologies and other measures for promoting online safety. Australian Communications and Media Authority. http://www.acma.gov.au/webwr/nassets/main/lib310554/developments_in_internet_filters_2ndreport.pdf
53. P. Hindley, J. Hurn, and S. Stringer, "Ward: Child protection concerns," in Psychiatry: Breaking the ICE - Introductions, Common Tasks and Emergencies for Trainee. John Wiley & Sons, 2016
54. R. Thompson, "Social support and child protection: Lessons learned and learning," Child Abuse & Neglect, vol. 41, pp. 19–29, 2015
55. The Protection of Children Online: Report on risks faced by children online and policies to protect them. https://www.oecd.org/sti/ieconomy/childrenonline with cover.pdf
56. S. Livingstone, "A rationale for positive online content for children," Communication Research Trends, vol. 28, pp. 12–16, 2008.
57. J. Dooley, D. Cross, L. Hearn, and R. Treyvaud. (2009) Review of existing australian and international cyber-safety research. Child Health Promotion Research Centre, Edith Cowan University, Perth. http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan046312.pdf
58. A. Marwick, D. Murgia-Diaz, and J. Palfrey, "Youth, privacy and reputations," Berkman Center Research, Tech. Rep. 2010-5, 2010. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163
59. R. Slonje, P. Smith, and A. Frisn, "The nature of cyberbullying, and strategies for prevention," Computers in Human Behaviort, vol. 29, pp.26–32, 2013.
60. Child Online Protection - Statistical Framework and Indicators. https://www.itu.int/dms pub/itu-d/opb/ind/D-IND-COP.01-11-2010-PDF-E.pdf
61. M. Ybarra and K. J. Mitchel, "How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs," Pediatrics, vol. 121, no. 2, pp. e350–e357, Feb 2008.
62. Implementing the Childrens Online Privacy Protection Act: A Report to Congress. http://www.ftc.gov/reports/coppa/07COPPA Report to Congress.pdf
63. E. Bartoli, "Children's data protection vs. marketing companies," International Review of Law, Computers & Technology, vol. 23, no. 1–2, pp.35–45, July 2009.
64. Guidelines for Policy Makers of Child Online Protection, 2009. http://www.itu.int/en/cop/Documents/guidelines-policy%20makerse.