enisa
European Network and Information Security Agency

Cyber-Bullying and online Grooming: helping to protect against the risks

A scenario on data mining / profiling of data available on the Internet

31-10-2011

DOCUMENT HISTORY

Date	Version	Modification	Author
01.04.2010	V 1.0	Consolidation of Experts Input on scenario	Involved Experts
01.06.2010	V 2.0	First draft contribution on assessed risks (including experts contributions)	ENISA, Louis Marinos, Involved Experts
01.10.2010	V 2.1	Final draft of risks	ENISA, Louis Marinos
21.12.2010	V 3.0	First draft of recommendations	ENISA, Louis Marinos
08.02.2011	V 3.1	Final draft of report	ENISA, Louis Marinos
08.05.2011	V 3.2	Final QA	ENISA, QA team
01.08.2011	V 3.3	Final version	ENISA, Louis Marinos

Acknowledgements

This report was produced by ENISA using input and comments from a group selected for their expertise in the subject area and in the areas of assessment (security, privacy, social and legal), including industry and academic experts. Furthermore, experts have been selected according to their engagement in the area of the scenario (e.g. child online protection, data mining, social networking, investigative activities and technology skills). It should be noted that group members participate as individuals. This paper should therefore not be taken as representing the views of any company or other organisation, and does not in any way bind group members when dealing with the issues it covers in other contexts.

The contributors are listed below in alphabetical order:

- **Alessandro Acquisti** (observer), CMU, US
- **Philip Anderson**, Northumbria University, UK
- **Scott Cadzow**, Cadzow Communications Consulting Ltd., UK
- **John Carr**, UK
- **Peter Dickman**, Google, US
- **Colin Gray**, CLJ Solutions Ltd, UK
- **Christopher Laing**, Northumbria University, UK
- **Vangelis Papakonstantinou**, Athens, GR
- **Aljosa Pasic**, ATOS, ES
- **Sascha Schubert**, SAS, DE
- **Dimitrios Vogiatzis**, NCSR Demokritos, GR
- **Piotr Wiench**, Warsaw University, PL

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of expertise for the European Union (EU), its Member States (MS), the private sector and Europe's citizens. As an EU agency, ENISA's role is to work with these groups to develop advice and recommendations on good practice in information security. The agency assists MS in implementing relevant EU legislation, and works to improve the resilience of Europe's critical information infrastructure and networks. In carrying out its work programme, ENISA seeks to enhance existing expertise in MS by supporting the development of cross-border communities committed to improving network and information security throughout the EU.

Contact details

For contacting ENISA or for general enquiries on Cyber Bullying and Online Grooming, please use the following details:

Louis Marinos, Senior Expert Risk Analysis & Management,
E-Mail: louis.marinos@enisa.europa.eu

Internet: http://www.enisa.europa.eu

Contents

1 Executive Summary

Children are the most valuable part of every society, regardless of culture, religion and national origin. Given the rapidly increasing digitalisation of their lives, it seemed important to assess risks related to internet usage and, in particular, the risk of become a victim of online grooming and cyber bullying activities.

A recent survey on the technology skills of children (2), (3) reveals that digital devices and the internet play a significant role in their lives. Today's kids are living in an environment that is radically different from that of their parents; virtual environments are increasingly prevalent in private and education environments. This development is detrimental to their physical activities, social skills and the behavioural model that prevailed in previous generations.

ENISA has formed a Working Group consisting of international experts in various disciplines related to the area of children's online protection. Interdisciplinary knowledge and relevant experience in the area were the criteria of their engagement. During the selection phase of the scenario to be assessed, the expert group has identified cyber bullying and online grooming as an area that requires further elaboration. With this assessment we aim to demonstrate how attacks based on misuse of data (i.e. data mining and profiling) can affect minors.

Although the issue of children's exposure to internet risks has been addressed in great depth by many organisations (also during the generation of this report), we have performed this risk assessment in order to point out **emerging risks** and issue **non-technical recommendations** for their mitigation. Thus, we believe that the findings of this assessment will help in triggering further activities at various levels of society, while contributing to the necessary awareness of the online protection of minors.

To this extent, this document should not be considered as overlapping with existing national and international initiatives in the area of child online protection. Rather, it complements them by pointing out additional elements that might be interesting to look at in the future. On the other hand, although non-technical, the assessed risks are based on very detailed analysis down to technological elements. Security experts might find this analysis interesting and even worth reusing in their own work/considerations.

1.1 Interesting developments

During the quality assurance process of this material some security related incidents have been through the media. These incidents are highly relevant for the assessed scenario and are indicative for the likelihood of materialization of security threats. It is interesting to mention that during the assessment, we have debated about the feasibility that location data could be collected (4), (5) and that mass loss of personal data of teenagers might happen (cases of (6) and (7)). Reality comes to show how feasible such attacks are and what impact they might bring to society.

1.2 Recommendations

We have grouped recommendations to categories according to the concerned target groups. These include Member States, law enforcement agencies, civil society and social partners, parents/guardians/educators and, last but not least, teenagers.

It is worth mentioning, that besides the formulated, rather non-technical recommendations, additional conclusions about possible improvements to protection of technical components can be derived by the performed analysis. The delivery of technical recommendations is not part of this report. However, this can be done by interested individuals at a later time and on demand.

It has to me mentioned that we have chosen almost identical groups for our recommendations and risks. With this we wanted to show the correspondence between our recommendation and the risks to be mitigated. These groups correspond to the 3 main owners of risks, namely the state in general (referred to as Member States / Law Enforcement and Civil Society / Social Partners), Parents/Guardian/Educators, and Teenagers.

MEMBER STATES / LAW ENFORCEMENT AGENCIES AND CIVIL SOCIETY / SOCIAL PARTNERS

Recommendations under this category cover regulatory issues, collection of statistical data with regard to cases of misuse and follow up on privacy breaches. An important part of the recommendations is about strengthening law enforcement agencies with additional knowledge and resources. By means of recommendations made to the groups below, Member States should consider the possibility of issuing soft rules regarding the identification of privacy risks for all applications that might process the data of minors. Similarly, the development of online rating schemes should be supported.

Although no recommendations for activities at international level have been made, it is obvious that European/international efforts can/should be started to prepare the ground for necessary international agreements and good practices/recommendations, especially in the area of legal framework and international cooperation issues.

It is recommended that civil society and social partners should develop knowledge sources regarding the use internet and online services to support various target groups. Furthermore, target group oriented campaigns should be developed in relation to online grooming and cyber bullying and made available to corresponding channels. In order to increase efficiency, sponsoring schemes should be considered beforehand.

PARENTS / GUARDIANS / EDUCATORS

Recommendations made for this group aim to enhance the knowledge both of online behavioural patterns of teenagers and the technological awareness required in order to carry out their tasks securely. Furthermore, technological skills will be necessary in order to overcome differences in the level of knowledge between themselves and the teenagers. In order to enhance trust relationships with teenagers, a continuous dialogue on this subject is part of the issued recommendations, together with offering support for schools regarding identification of misuse patterns in online interaction.

TEENAGERS

Numerous recommendations in this category cover mitigation measures for the identified risks. In short, the recommendations include:

- Use of specialised teenager security controls
- Adaptation of existing security controls to teenager needs
- Development of rating schemes for online content
- Performance of privacy impact assessment for applications processing teenager data
- Development of mechanisms to allow deactivation of all active (online) components
- Enhancement of age oriented access control mechanisms

1.3 Top risks

A series of risks have been identified within this work. Similarly to recommendations, risks have been grouped in categories according to the stakeholder who is mainly exposed to each particular risk.

MEMBER STATES / LAW ENFORCEMENT AGENCIES

The risks identified for state organisations and mainly law enforcement agencies concern potential weaknesses in identification and follow up of misuse cases. In particular:

- Being unable to follow misuse cases due to missing resources and knowledge
- Being unable to follow misuse cases due to international investigations being required - that is, falling outside the sphere of national influence
- Failures in investigations due to varying levels of maturity of relevant legal frameworks in different countries

PARENTS / GUARDIANS / EDUCATORS

Risks identified for this group (7 in total) concern the conditions under which an effective duty of care can be performed. In particular:

- The risks that teenagers will develop activities and behaviour patterns that escape the sphere of influence of guardians, such as second life, cyber activities, uncontrolled virtual meetings etc.
- The risk that adults will not have the knowledge and tools to control online activities

- The risk of failing to provide and maintain a secure digital environment for teenagers to use
- Inability to fulfil the care duties within school
- Risk of failing to defend oneself due to lack of knowledge, evidence and legal framework

TEENAGERS

Several risks have been identified for this group. At this point we refer to the highly prioritised ones, by explicitly stating that the rest of the identified risks (i.e. 13 in total) are also of high importance. Major risks teenagers are exposed to with regard to online grooming/cyber bullying include:

- Suffering serious loss of physical or mental health
- Irreversibly exposing themselves to the internet by publishing important personal information
- The risk caused by imbalance between technical and social skills
- Discrimination based on behavioural patterns
- Misuse as a result of data loss

2 Introduction

2.1 Background

Given the (current and upcoming) penetration of digital devices and services in the target group of young individuals, it is imperative to elaborate on measures designed to protect them from the misuse that can take place in cyberspace. On-going discussions about the privacy requirements of minors carry enormous importance, especially when considering technological developments in data mining and profiling that can be applied to vast amounts of data that are available online.

Combined with observed changes in behaviour of young individuals (8), the use and misuse scenarios of digital devices and online services come into focus. Hence, assessing the risks of online grooming and cyber bullying seems to be an important step. It is clear that the exposure of teenagers to these and similar risks will potentially increase in the near future, given that digitalisation and cyber-activities have arrived in children's rooms and school classes and are here to stay.

The purpose of this work is to assess those risks, issue recommendations and deliver detailed evidence about the existence of multiple vulnerabilities in the corresponding environments and the infrastructure components used.

With the work on this scenario, we aim to complement the work already done in this area ((9), (10), (11), (12)) by assessing risks and by issuing recommendations that embrace both technical and societal issues of information security and protection. In order to avoid duplication of work, we have taken into account various developments in this area and have performed some knowledge transfer through our expert group and through discussions with other colleagues, both within and outside ENISA.

This work is an attempt towards demonstrating a systematic way of combining both technical and non-technical knowledge to identify emerging security risks and proactively propose recommendations that will lead to actions from all relevant stakeholders, such as parents/educators, civil society, state organisations and the European Commission (13).

2.2 A case scenario

The present scenario has been developed within the work described in ENISA Work Program 2009 under Multiannual Program (MTP) 3. After its initiation in 2009, the work was completed during 2010. Following initial assessment of areas to be addressed, ENISA committees and stakeholders have prioritised data mining / profiling as one area to develop and assess a dedicated scenario.

A team of subject matter experts has been assembled in order to support ENISA in this task. The selected experts cover the various areas of expertise that were deemed necessary to achieve an interdisciplinary view of the issue. The selected experts bring skills in technology, applications, telecommunications, social and ethical issues, forensics, security issues, data privacy/data protection and legal issues.

Given current developments in the areas of internet usage and, in particular, child protection issues, the experts involved have proposed a scenario in the area of cyber bullying and online grooming. Indeed, this area is the focus of various activities at national (14), European (12) and international levels (10), (11), (14).

This assessment is one of a series of risk assessments performed by ENISA and utilises the ENISA Emerging and Future Risk (EFR) Framework that was developed in 2007-2008 (1). Part of the ENISA EFR Framework consists of the EFR Stakeholder Forum that supervised the project in 2009, providing valuable comments and advice about the work undertaken.

2.3 Why a cyber-bullying / online grooming scenario?

Children are the most valuable part of every society, regardless of culture, religion and national origin. They depend on the care they receive from their parents, the school and their social environment. Duty of care makes parents worry about any of their children's activities that might carry risks, such as extreme sports, or the use of technology. This last topic particularly concerns parents, as they often they do not feel as confident with technology as their children, who:

- Have fun in using technology/gadgets
- Use technology intuitively
- Develop an understanding for usage of technical features very easily
- Become very familiar with innovations
- Use ICT as a learning tool
- Use technology in communicating with their friends

Children love the internet and go online to have fun, do homework, stay in touch with friends, or sometimes buy things such as books, games or music. Most of the time, children's internet use is perfectly safe and enjoyable. But like everything in life, there are some risks. The misuse cases of online grooming and cyber bullying have been selected because they seem to introduce significant harm to victims and their social environment. At the same time, these misuse cases seem to require some additional elaboration, especially in connection with the future use of new technologies.

2.4 Target audience

The intended audiences of this report are:

- Teenagers, parents/guardian/educators who would like to get informed about the combination of these misuse cases and the internet
- All stakeholders who are active in the protection of minors, especially in the area of online protection. Furthermore, all relevant stakeholders in the area of education and training but also civil society and the various social partners

- Industry, in order to encourage them to secure their technologies and services, to make transparent to all concerned parties (i.e. teenagers, parents, educators, law enforcement agencies) their purposes and practices in collecting and processing personal data and to identify any third parties with whom they share such data
- Individual Member States that are in the process of developing protective measures, awareness raising campaigns and policies for the protection of teenagers in cyber space
- Member States, the European Commission, EU Institutions, in order to assist them in deciding on appropriate policy incentives, legislative measures, awareness-raising initiatives in the area of child online protection; and to assist them in identifying future research actions (i.e. to develop technologies that mitigate identified risks)

2.5 Scope, overview and rationale of the scenario

In this section, we provide the scope and an overview of the developed scenario. Our scenario is narrative and takes place in the near future, that is, in 2-3 years from now. Most of the technology involved in the scenario is available today. Similarly, the described behaviour of the participating actors almost fully corresponds to today's patterns.

Similarly, the assumed misuse cases of grooming and bullying have been widely recognised in teenage environments for many years now. Almost everyone has directly or indirectly had experience of these misuse cases while at school, in the family or within a circle of friends. To this extent, the selected scenario is based on a rather 'traditional' pattern of interaction between the involved actors. The novel issue in the scenario, however, is the use of technology that increases the exposure of actors to risks, as potential perpetrators can apply novel techniques to identify victims and can better maintain anonymity during their interaction.

Having said that, we use the following existing definitions for grooming and bullying:

- Grooming: "*The purpose of grooming is to make a victim. Grooming is done to choose a victim, to see if the person may cooperate with sexual abuse because of the imbalance of power and coercion.*
  Grooming is done to make a potential victim feel comfortable enough to be close to an offender, to be alone with an offender, and after the ABUSE, to keep the behaviour a secret." (15).

- Bullying: "*One definition views bullying in terms of its negative impact on the victim, and sees it as the negative and damaging treatment of another in such a manner that is causes the target to suffer and feel humiliated or vulnerable, and which has a detrimental and stressful effect on him/her.*

As with harassment, bullying is defined largely by the impact of the behaviour on the recipient, not its intention.
Bullying may therefore be seen primarily in terms of aggression, or long-standing violence, physical or psychological, conducted by an individual or a group, and directed against an individual who is not able to defend him/herself in the actual situation." (16).

Significant efforts have been devoted to finding the scenario and setting it in the 'reality' of 2-3 years' time, with regard to the social, technical and behavioural framework of the actors, their life style, their technological assets and ways of using them. In other words, attention has been paid to how far the scenario will meet the reality of teenagers, parents and teachers in 2-3 years' time.

The figure below gives a graphical overview of the developed scenario in terms of participating actors and assumed interaction.

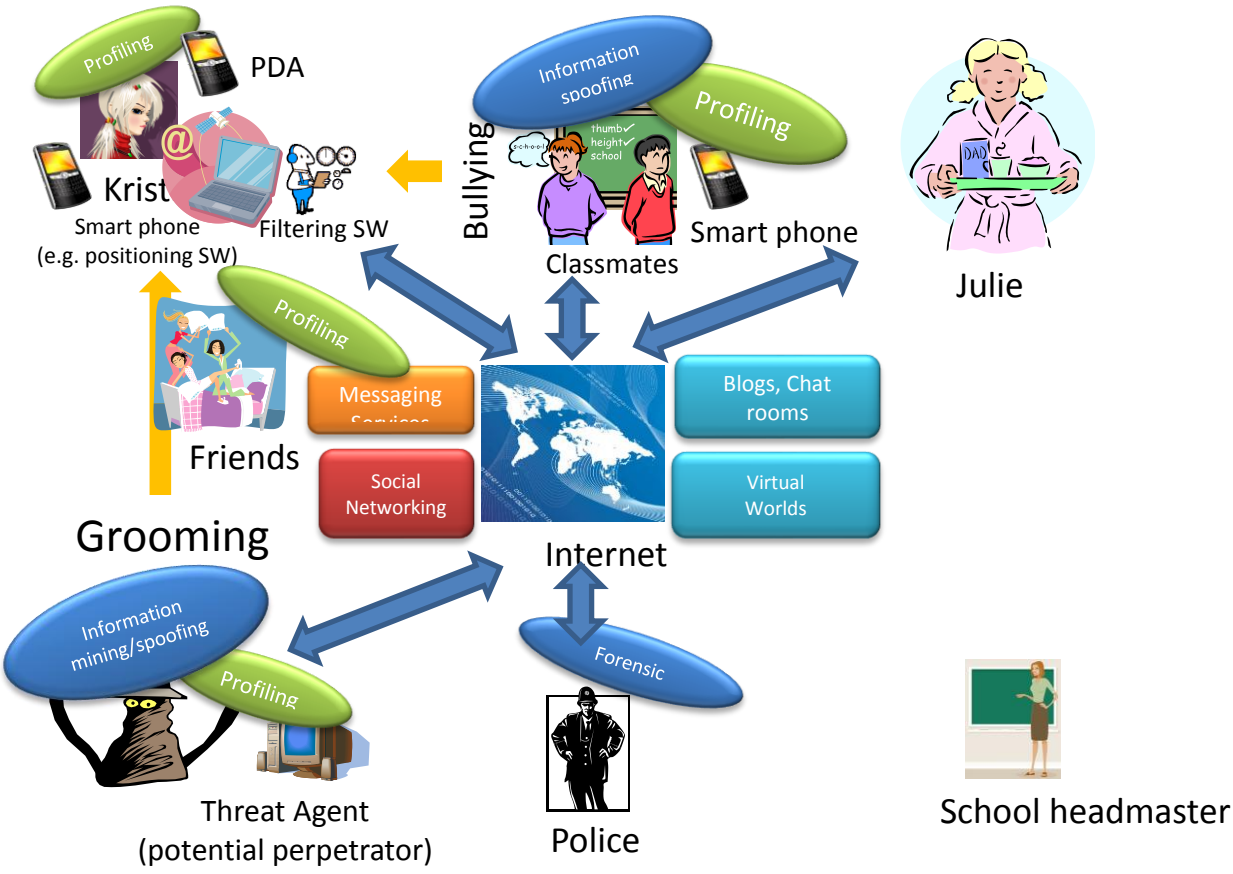


Figure 1 – Schematic representation of the involved actors and the interaction taking place within the analysed scenario

2.6 Assumptions made

In the developmental phase, the expert group formulated the 'environmental' conditions under which the scenario takes place by means of a set of assumptions. The assumptions are one of the main elements driving the risk assessment: certain decisions during identification of risks have been based on the assumptions below. It is worth mentioning that if these assumptions are changed, other risks might eventually have been assessed, or the assessed risks would be differently prioritised.

Last but not least, assumptions help better understanding of the background of the developed scenario, as they provide important details about the 'environment' in which the scenario takes place. The assumptions made are the following:

1. We believe that in a few years' time, more and more teenagers will be equipped with smart phones and devices with advanced applications and services that go beyond those found in simple mobile phones. This is because teenagers will inherit out-dated smart phones from their parents, as well as other computing devices, such as ultra-mobile computers. The possession of such devices opens new interaction possibilities and the opportunity to use various apps. On the other hand, these devices carry the risk that their underlying operating systems/software is not maintained any more, with the obvious consequent vulnerabilities.

2. The term 'Data Mining' is used according to the definition: "Data mining is the process of extracting patterns from data. As more data are gathered, with the amount of data doubling every three years (17) , data mining is becoming an increasingly important tool to transform these data into information. It is commonly used in a wide range of profiling practices, such as marketing, surveillance, fraud detection and scientific discovery (18) .

3. Data profiling and data mining are distinct technologies.

4. According to (19) , the term 'Data Profiling' is considered as one of the main methods to perform Data mining, that is, to turn data into information by looking for certain patterns.

5. The main assumption of this scenario is that participating actors use large amounts of data available for legal use on the internet (e.g. social networking sites, blogs, location data, cookies, etc.). Depending on the nature of the data used (private or public) and the goal of the activity (beneficial or malicious), involved actors could potentially use this functionality both legally and illegally.

6. Data profiling techniques are used in order to scan this information with the objective of finding individuals that share common interests and/or belong to certain groups (e.g. teenagers).

7. Parents of the teenager involved have managed to maintain access to the relevant technology components (i.e. laptop and/or smart phone belonging to the teenager, installed monitoring software, etc.).

8. Covert surveillance should only ever be undertaken in extreme circumstances. The parents of the participating teenager felt such circumstances had arisen. They had become so concerned about the behaviour of their daughter that they felt justified in taking a detailed look at what had been happening during her online transactions.

9. In order to create two separate social networking accounts, all that is required are two separate email accounts; typically, social networking sites currently have no way of knowing whether an individual has created more than one account.

10. The social networking site used provides privacy and data protection functionality for various types of information stored. The function provided s are detailed and for the privacy of some fields, the explicit consent of the user is required (e.g. date of birth). Although many data protection and data privacy issues are covered by both the functionality and the terms of use, users need to be very knowledgeable to cope properly with privacy and security issues.

11. Mobile access to the web, and in particular to social networking sites will increase in the near future; consequently all concomitant threats to the security of mobile information will become relevant for personal information involved in social networking (and vice versa).

12. Location based services are already available, and will become more widespread in the future as penetration of smart mobile devices with integrated GPS increases.

13. At the level of the operating systems, it is expected that functional convergence will be further implemented, although the specific means to implement it may be different (i.e. open source (Linux variants) and closed systems (MS-Windows and OS/X) will remain as competitors on the market for the foreseeable future).

14. Authentication is achieved through email address validation (i.e. registration is completed after an exchange of emails).

15. There is no contractual or subscription relationship between the social network provider and the user of the network.

16. There are no contractual relationships or ownership dependencies between companies delivering services described in the scenario.

17. Social networks do not enforce rigid age and sex claim verification but rely only on self-assertion of the user.

18. Social networking sites do not perform active policing of 'friend' relationships to determine if they are suitable (i.e. they do not act "*in loco parentis*" for child subscribers).

19. Social networking sites are fashionable and whilst the function may not change, the location may do so (c.f. the bar/restaurant/club of choice in normal (i.e. not online) social networking)

20. Not all social networking avenues are publicly declared as social networking sites and many other avenues (e.g. instant messaging hosts, chat lines, blogging sites) may fulfil the same function (c.f. the bus stop or park bench used as a meeting venue for offline teenage networking).

21. The concept of 'minor' in law and in provision of service will remain (i.e. those under a specific age will be disallowed access to some services and may need to provide authoritative age verification before accessing such services (including banking)).

22. Many search machines e.g. Google, provide access to details kept on social networking sites without requiring an account, or to be a friend of an account holder.

23. EU legislation context. Processing of personal data should conform to the requirements of the Directives of the EC and the National Laws of the Member States concerning the protection of personal data and the protection of privacy. These European Directives are:

    Directive 95/46/EC1 of the European Parliament and of the Council of 24 October 1995 concerning the protection of individuals with regard to the processing of personal data and on the free movement of such data.

    Directive 2002/58/EC2 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

24. National legislation contexts. The processing of special categories of data ('sensitive data'), is usually prohibited. This prohibition may not apply if the data subject has given his/her explicit consent to the processing of those data, except where the laws of the Member

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

State provide that the prohibition may not be lifted by the data subject's giving of consent. Additionally, subject to the provision of suitable safeguards, both Directives and Member States' national laws lay down exemptions to the above prohibition, for substantial public interest reasons. In some Member States, the collection and processing of sensitive data are allowed only when the Data Protection Authority has granted a permit to the Controller, as well as for the establishment and operation of the relevant file, upon request of the Controller (Controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data).

25. Children, institutionalised persons or others who are vulnerable are entitled, on grounds of human dignity, caring, solidarity and fairness, to special protection against abuse, exploitation or discrimination. Ethical obligations to vulnerable individuals will often translate into special procedures to protect their interests.

26. From sociological and psychological viewpoints, 'child' and 'youth', as such, is seen as a social construction, but definitions vary across countries, cultures and over time. Most of the definitions are more related to the life situation of being in transition rather than being a clear cut age range. In fact the ages in policy or welfare programmes for youth often refer to persons between 14 and 27 years (see (20)). The United Nations span the period of youth from the age of 13 to 24. A UN act refers to teenagers as being in the ages 13 to 19 and young adults between 20 and 24.

3 Cautionary Tale – Cyber Bullying and Online Grooming

ENISA convened a group of independent experts to develop and analyse a scenario, the context of which was the use of gadgets, communication and online services in the everyday life of teenagers. The group has analysed the scenario using ENISA's methodology, in particular to identify assets, vulnerabilities, threats, risks and mitigation actions, as well as eventually recommendations to all relevant stakeholders.

3.1 Kristie "online"

It is the year 2012; Kristie is an extrovert 13 year old child, intelligent with many hobbies and a lot of friends. She is, in particular, a fan of the 'Kyoto Inn' band. Kristie has a laptop that she uses at home, for homework and to go online (see below). She also has a PDA and two mobile phones; one is a cheap basic pay-as-you-go phone that she pays for out of her pocket money; the other – a gift she specifically requested from her parents for her 13th birthday – is a cutting-edge smart phone on a combined voice and data contract that her parents pay for. Her school used to have a 'no phones' policy, but that has been changed, after pressure from parents, and the children are now allowed to take a mobile phone to school, but it will be temporarily confiscated if they use it during lessons. Kristie is somewhat embarrassed and annoyed that her parents do not allow her to take her smart phone to school. They imposed this rule because, some months earlier, one of Kristie's friends had her new phone stolen on her way home from school by a gang of older children. However, Kristie is allowed to take her PDA and basic phone to school. On a few occasions Kristie has defied her parents and 'accidentally' left her smart phone in her coat pocket on a Sunday evening and 'accidentally' taken it to school the next day.

Kristie's parents have a home computer, a laptop and an electronic book reader of their own, as well as smart phones, and the family share a games console with various multi-player peripherals. They make wide use of e-Commerce sites. The family are reasonably technically literate and endeavour to keep their home systems secure. Kristie's school ran an awareness session for parents about online safety issues and they restricted her use of online systems, in line with the guidance they were given, but have slowly relaxed their rules a little since she is now a teenager. As part of their own approach to computer security, Kristie's laptop is backed up once a month and auto-updates the operating system and security tools. Her parents have also set up a filtering system, designed as a child protection tool, in an attempt to manage the websites that she has access to. Kristie does not take her laptop out of the house, except when she goes to her best friend's home to work on a project together – they are building an online fanzine for their favourite band, having told their parents this is as an extension project for their ICT class (it isn't). Kristie's friend's parents also have a home wireless system and home computer, but they are less inclined to keep it secured and up-to-date with security patches and often ignore warning messages when using their computer.

Kristie feels at ease with the technical devices, using both her smart phone and her laptop fluently. She has mastered the offered functions and uses them all. She has also explored many downloadable apps for her phone, mostly focusing on free apps, but she has also

bought a handful of interesting ones after reading reviews and hearing about them from friends. Kristie enjoys being active on social networking sites and has a profile that contains, besides personal data (demographics and contact data), her music preferences, places she would like to visit and fashion items. Kristie actually has two social network profiles, only one of which is known to her parents. Her parents also have social network profiles and Kristie is 'friends' with them in one system, as well as with several of her school friends. The same group of school friends all have secondary accounts under other names in the same system, and are careful not to link those accounts to any of their parents. They have all lied about their age in their second accounts (saying they are 18 rather than 13) and these accounts are not as tightly locked down as Kristie's parents would hope and expect. Kristie's online magazine (basically a simple website with links to interesting resources) is linked from her second social profile and she's identified in the magazine as the editor. Kristie also participates in other 'Kyoto Inn' fanzines and discussion groups online. She likes playing online games (though her idea of which ones are cool to play changes frequently), and sometimes participates in discussion sites for her currently-favoured games.

Kristie used to post regular status updates on both her social network accounts, but now considers that to be 'sad'; she also went through a brief phase of sending short text updates to a network of followers on a different service. At the moment, however, she and several other friends with smart phones have decided that location-based apps are the in-thing. When Kristie is out with friends or family she uses the GPS-based apps on her smart phone and maintains a near-permanent connection to her social networking provider. Although she has no way to restrict those friends broadcasting that data to a wider group of friends, she communicates location based information to a number of selected friends, and her current location appears as her status in her online profile. It's a cool application, but also a useful way to find the whereabouts of friends.

Kristie enjoys uploading pictures, from places, people and events as they take place, and often uploads pictures of herself and her mother when they are shopping or visiting friends. Kristie recently went to a 'Kyoto Inn' concert, where - with the aid of a mobile device – she formed a social network of 'Kyoto Inn' lovers with people she has met at the concert venue, and she subsequently uploaded it to her preferred social networking site. Kristie enjoys all of the social networking because it's dynamic and it's a great way of making new friends with the same interests. During her summer vacation, Kristie enjoyed her time on a Greek island with her parents. Looking for some extra entertainment, without her parents' knowledge, she logged-in with her smart phone onto the mobile version of her social networking site (they subsequently found out because of the roaming charges on the bill). She was looking for teenagers that were on the same island, and also liked 'Kyoto Inn', as being with her parents continuously for 10 days was a bit boring, especially when they wanted to visit a museum. Her parents did not, however, allow her time away on her own, so she didn't get to meet the people she connected to online.

In addition to all these functions, Kristie uses the internet for shopping for music, videos and apps for her phone, as well as DVDs of her favourite TV shows and films and memorabilia for 'Kyoto Inn'. These items are either paid for by her parents, using their credit card when she's ready to finalise her purchases, or through an online account into which her parents put a small amount of spending money for her each week. She has also used the internet to browse for clothes, including following links from online fashion magazines, but she has only ever bought accessories, not clothes, online. Kristie greatly enjoys the recommendation features of online shops, where suggestions and offers are made to her, based on her buying behaviour. Some of the online shops allow for interfacing to her social networking site to provide her with bonus points that give her the right to participate in special offers (usually sent to her by e-mail). Kristie has also downloaded an app for her phone that allows her to read barcodes using the camera and some dedicated optical scanning software when she's out with her friends and immediately access online reviews and comparison prices for products.

However, while all these are positive, Kristie has recently gone through a negative experience: she has been bullied by a group of her classmates (21), (22). Recently, in a private group on a social networking site, messages containing incorrect, defamatory statements, mixed with correct but personal information about her, have appeared. Subsequently, she has received SMSs from unknown senders referring to those assertions, threatening to disclose this information to school management and her parents. In particular, the bullies have threatened to expose the existence of her second online profile.

Initially the bullies contacted her via the social networking site, pretending to be a group of friends, and asking her to join. The information they gained has then been misused to humiliate her.

Kristie does not know what would be the best way to react to this bullying. She has visited various anti-bullying web sites, but she is still not yet sure what would be the best course of action. She believes she cannot tell her parents because they would be upset that she had created a hidden secondary online life, and she is worried about her real friends' reactions, as they also risk being exposed and might blame her. Then she meets a new online friend called Jeffrey.

3.2 Kristie's parents

Kristie's parents have been aware of the high volume of internet usage for some time, and occasionally tease her, suggesting she is becoming a techno-junkie. Kristie's parents were concerned about this attitude anyway. Julie, Kristie's mother, has discussed it with friends.

One of Julie's friends, Lucy, recommends filtering software. Lucy had purchased this software after seeing a demonstration at a parents' online safety course that she had taken the previous year. She explains to Julie how this software monitors her children's conversations over internet telephony, visited websites, searched websites and much more. Lucy advises Julie to purchase the software to get answers. Typically, such software provides a remote view of the user's computer screen, keystrokes live monitoring, web site visit history, list of applications processes that have been activated on the PC, emails sent and received, and a log

of instant messaging (IM) chats. All this information will be recorded and catalogued according to time and date.

Kristie's parents are aware that the use of monitoring software can be very corrosive of trust within a family, which is quite contrary to Lucy's view. It could be seen as being a very clear statement that parents do not trust that the actions of their children are honest. They also understand that monitoring software should not be used covertly by parents without very good grounds for believing that their child is in the hands of a cult, or is already in the grips of a paedophile, or something along these lines - a very extreme situation which means the child is truly incapable of being reached and of being truthful. Kristie's parents are unwilling to put the trust within the family at stake. Moreover, they are convinced that such an action would be ineffective; if their child is doing something she doesn't want her parents to know about, she will just continue, but make efforts to do so covertly.

Hence, they decide to apply the principle that they only have a right to access data about their daughter and to exercise their rights of due care while Kristie consents to her parents being informed. Taking into account all that, they decide to inform Kristie about this option and get her consent. Their intention is to install the filtering software at the lightest level of monitoring, only to get automatically informed on detection of keywords in her traffic and in any other case to use it with care and while Kristie is present.

As an additional measure, they request Kristie to lock her social networking profile, so that only existing friends can locate her and her personal data is protected against unsolicited use by strangers. This functionality is offered by the social networking site for the protection of minors. Her parents explain to Kristie that they will seek to engage her in a conversation about each and every person on her existing list, as well as any new ones that might be added.

They also install some software on Kristie's netbook and smart phone to protect against malware (e.g. by means of systems like (23)) and activate a service from the provider to deliver records about her internet usage over her smart phone. This material arrives, together with the bill and is shared with Kristie[3]. Her parents also talk to their daughter about the potential dangers of the internet and convince her that the filtering is for her own protection, acting as an additional preventive measure against various kinds of misuse that could happen during online activities.

During the installation of this software Julie and her husband notice there are numerous options. However, they set it to instantly report on emails/instant messaging conversations and online activities containing some of the keywords which they have customised the software to pick out.

Finally, Kristie's parents have an open channel to the class teacher, exchanging information about the teenager in a regular manner, but also on demand (i.e. in cases of exceptional

[3] *The bill goes to the bill payer and as a minor she will not be allowed to enter such a contract. The CSP/ISP does not have a billing relationship with minors.*

issues that might come up). This usually happens over e-mail and, in more urgent cases, over the phone.

3.3 Exposure of online users

The danger of users (and in particular children) befriending malicious strangers[4] in cyberspace in the mistaken belief that such friends are benign stems in part from confidences shared by extant (trusted) online friends, either deliberately or by accident, and/or from the content of the user's publicly available profile. The ultimate intention for the purposes of this case study of such malicious strangers is to manipulate (or physically meet) the targeted victim (for the purpose of this case study a child), whose profile (i.e. picture, interests, hobbies) they have spotted on a social networking site and who, in the belief of the attacker, presents a viable target (i.e. one that can be reasonably manipulated with low likelihood of determining the attacker's real intent). To do so, they have to gain the child's trust, which can be achieved by gathering information about, and to position themselves as a friend of, the child's friend, as a member of a group in which the child participates, or as someone sharing the same interests (e.g., hobbies, music, sports, social behaviour, etc.), and same problems (e.g., bullying, etc.). This is a pattern that may be indistinguishable from a non-malicious potential friend and relies on the attacker suppressing their own identity in favour of the masqueraded identity. The attacker may work alone or in concert with others to establish the trust required to exploit the victim in the planned manner.

To achieve their aims, the attacker collects data concerning the activity of his target group (children) in cyberspace by browsing profiles, posts and other digital traces left by the target's activities (e.g. avatars, blogs,.) and by seeding the areas the target uses with data that may encourage contact (e.g. spoofed information), as well as by collating data with other attacker groups to enable better victim profiling. A number of examples of attacker behaviour are listed below:

- From knowledge gained that the target participates in 'Kyoto Inn' social groups. They could use advanced versions of meta-search engines to discover children participating in the web site: 'Avatars owners'.

- By using data mining techniques. With the seed data obtained, additional information can be retrieved (tools exist for this purpose in the legitimate business world and may be

[4] *We rightly recoil from the idea of paedophile behaviour, i.e. older men or women seeking to engage in illegal sexual activity with persons below the age of consent. There is something particularly repulsive and obnoxious about the degree of manipulation and abuse that this implies. However it would be wrong to think that only older people are a source of worry or danger to people like Kristie. A lot of sexually predatory behaviour is carried out by other legal minors, and bullying - which in rare cases can lead to suicide - is almost entirely the prerogative of younger people. However, it is very important to stress that not all strangers are bad (i.e. Good Samaritan principle.)*

exploited for criminal gain). Such tools, e.g. a tool called SocNetMiner[5] have been made available from various internet sites/service providers offering mining software for social networks. Such tools provide information on the whereabouts of a specific social group (in this case children), i.e. based on their musical preferences and other personal information by integrating information from their friends. SocNetMiner produces results which are quite accurate in most cases. In other words, a lot of information about an individual can be inferred from his/her friends, even though his/her profile may be locked. Thus information about community formation, trend development, and spread of news can be extracted (24)[6].

Other tools might be used to trace behavioural aspects of online users. For example, one such tool available on the net is called Behaviour Analyser, also known as AnalyseThem[7]. This tool analyses behavioural data of specific users; such data represent a totally different class of data from those explicitly posted by the user. They concern communication patterns of the current user; for example, they might indicate, the time, date, and recipient of chatting, instant and e-mail messages. Given that a potential individual could maliciously hold and analyse this material, he could indeed get information about the acquaintances, close friends, etc., of potential victims and, by exploiting location information, also where they like to spend their time.

Such tools may bypass the data locking functions of some sites (i.e. by often running at a privileged level on the host server).

- They could acquire information from the mobile devices of their potential victims, in various ways, i.e. by remotely installing malicious software on the victim's smart phone. This could happen via an insecure wireless internet access point, or via malicious software download via an internet web application (25) . Additional misuse might happen with the aid of a wireless communication protocol such as Bluetooth, in an area frequented by teenagers. This could be during a school festival, during the concert of a music band, or simply by being close to the school yard.

---

[5] *SocNetMiner is a fantasy name of a tool that by that time is being made available on the net and implements the mining functions on social networking information to identify various kinds of individuals given a specific behaviour pattern. The reference gives information about such a functionality that has already been validated within a research project.*

[6] *The information that can be derived is not available yet as a commercial product, however it refers to research taking place now, including research funded by EU.*

[7] *AnalyseThem is a fantasy name for a tool that by that time is being made available on the net and implements functions enabling the identification of available associations among various individuals on a social networking site, based on mentioned contacts and friends. The reference gives information about such a functionality that has already been piloted within a research project. Obviously, the use of this kind of software without previous consent of the data owners is illegal and the perpetrator is aware of his illegal activities.*

- Combining available personal data that has been both legally and illegally obtained from various sources, which is then analysed by the use of these mining/profiling functionalities, offers a very powerful tool for identifying individuals, including such information as: banking accounts, phone numbers, e-mail addresses, postal addresses, location data (e.g. from mobile GISS applications, connected to social networks) and all kind of digital traces in the net (26) , (27) .

Armed with all this information, about who the friends of individuals are, about their communication behaviour and about the places they frequent, allows for the posting of messages on the social networking site of their potential victim; posing as a close friend, someone liking the things their friends enjoy, or suffering similar problems at school[8].

3.4 The incident

In June 2012 Kristie's mother, Julie, notices a significant behavioural change in Kristie. Usually a very boisterous teenage girl, she has lately become very introverted and quiet. Her parents realise that she is spending more of her time on her laptop in her bedroom, minimising the time she spends with them, and is also spending less time out with her friends. At first they put this down to her being a 'typical teenager'. After several discussions with the school headmaster, no answers are forthcoming to explain Kristie's poor attitude and falling grades.

This behaviour leads them to pay a greater degree of attention to the reports they receive from Kristie's online activities. They decide to temporarily 'break' the arrangement they made with their daughter and activate additional functions in the filtering software, i.e. provision of filtering logs in real time.

After closer monitoring of Kristie's online activity for some days, her parents realise that she is no longer playing online games and that there is far too little activity on her social network (the one they are aware of) to explain the time she's spending online. It is clear, however, that she is spending time chatting online. At several points during the monitoring period the logging systems do not seem to behave quite as expected, and the malware and virus logs also show that there have been a couple of problems with Kristie's laptop.

Eventually, after her parents find an abusive SMS message on Kristie's phone one day, their daughter breaks down and explains what has been happening. Initially dismayed that their daughter had been betrayed by people she thought were her friends, they become increasingly concerned when they realise that Kristie has been spending large amounts of time talking online to a boy she has never met. He looks pleasant enough in the photographs Kristie has of him (where he appears to be in his mid-late teens), but he seems to have been encouraging her not to trust her existing friends and not to tell her parents or teachers, or indeed anyone but him, about the bullying. Instead they have been spending more and more

[8] *Not only adults might potentially misuse this kind of information. Any individual having some basic technical skills will be in the position to (illegally) obtain such information.*

time together online, to the point where Kristie has also been neglecting her studies, with the boy strongly encouraging her to become ever more isolated. After further investigation of her laptop they find travel information which suggests that Kristie is planning to skip school and go to a nearby town. When challenged about this, Kristie eventually admits to having arranged to meet the boy the next day for a date.

Kristie's parents then take control of her laptop, logging in as Kristie, and use stored credentials on the machine to access Kristie's email. Amongst a collection of messages that Kristie thought she had deleted, they find disturbing evidence that Jeffrey, the boy Kristie has been talking to, may actually be rather older than she realises (Kristie claims he is 16 and that she has told him she is 13), and that he may have predatory intent, as the mailed exchanges have clearly taken a rather adult turn.

Kristie's parents are by now becoming extremely concerned about Kristie and contact the police to explain their fears for their daughter, passing on the information collected about Kristie's cyber-activities and what they have found out. The police visit Kristie's parents and interview Kristie herself. They proceed to investigate further after warning her parents that they suspect this may be a case of child grooming and providing them with advice about how to safeguard their daughter.

After an initial analysis of the information provided, the police officer says that they have had similar cases in the past. The police will treat the matter as suspected child grooming too, meaning that a police investigation will be started to verify the identity and intent of the possible perpetrator. He states that in the remaining time until the meeting between the girl with the 'friend' takes place, he has to perform this identification and verification task[9].

The police have therefore decided they will go the pre-arranged meeting between Kristie and her online 'friend'.

A few days later the police inform Kristie's parents that officers have attended the planned rendezvous and that no-one aged 16 or thereabouts was present, but they have arrested, on suspicion, a much older adult male who was loitering at the scene, based on additional evidence they had acquired in the intervening period.

The arrested person, identified as a male aged 35, is already known for suspected offences of child abuse. A search is conducted at his home address and sufficient evidence is found through forensic examination of the seized items (computers, peripherals, various devices and gadgets).

---

[9] *In cases of this type there are procedures for expediting these requests. Most of the large US based social networking sites have a 24/7 emergency contact procedure that does not involve going through Interpol. We don't know what country Kristie lives in but in most European countries the police ought to know how to access these US numbers. I believe many of the European sites have similar arrangements.*

Getting access to information about the content of communications - as opposed to information about when different communications happened and between whom - is more complicated, and can take months, but for an investigation of this type, operating within the timeframe given, the police already have enough to go on.

Throughout the forensic examination of the suspect's computer and laptop, the computer forensic analysts find a large number of children have had contact with the suspect. They are able to find many leads to other adults who were possibly sharing information with Jeffrey. This information has been fed to appropriate profiling tools that help the police to find additional leads to other similarly minded suspects in social networking sites, blogs and other web sites.

They find, for example, that the suspect regularly uses chat software on his laptop and that his conversations are saved. His web mail account has a number of contacts and, on further investigation, it appears that some of these are family/friends and some are young children. The analysts concentrate on the saved conversations between the suspect and his younger contacts, finding that these conversations have the same pattern as those conducted with Kristie.

On searching the suspect's internet history they find that he has also been viewing illegal images of children and has been talking to others about images and videos of young girls.

4 Risk assessment results

In this chapter we give an overview of the various results developed during the risk assessment phase. The purpose of this presentation is to inform the reader about identified assets, major risks and measures (also called controls) that are used for the mitigation of the risks. Furthermore, this discussion provides a non-expert view of the assets (i.e. values that are involved in the developed scenario) and the risks to which these assets are exposed. Consequently, we give an overview of existing measures to make clear how risks can be mitigated. We have devoted a significant part of the total effort to achieving these results and held intensive discussions among the experts involved.

We believe that information about these issues comprises the central part of this assessment and that it will prove to be very valuable for interested individuals. Those who would like to understand the values that are behind this and similar scenarios will find this information useful. Furthermore, it may also be useful for the better understanding of the context of this work and might be re-used within related studies, awareness material, further assessments, policy decisions, technology reviews, etc.

4.1 Assets – what are we trying to protect?

We discriminate between intangible and tangible assets as being the elements of the scenario that are worth protection. While tangible assets consist of information and devices that are part of the scenario and, as such, are easier to identify, intangible assets are values derived from ethical, societal and political issues of the environment of the developed scenario. Often intangible assets are difficult to identify and quantify.

Intangible assets

A1 - Right to be treated with dignity and respect

The right to be treated with dignity and respect is considered to be one of the fundamental rights of our societies. Respecting this fundamental right can play a central role in creating a fairer society for all, including the reduction of violence. It embraces the right neither to be bullied nor harassed, nor to be discriminated against on the basis of personal characteristics including sex, race and religion. This right is treated as being an asset of the maximum value level used within this assessment.

A2 - Reputation

“Reputation is the opinion (more technically, a social evaluation) of the group of entities toward a person, a group of people, or an organisation on a certain criterion. It is an important factor in many fields, such as education, business, online communities or social status. Reputation can be considered as a component of the identity as defined by others.” (17) .

It is remarkable that reputation accounts for a great deal of the way people perceive each other and is fundamental for the social evolution of a person. It is a very important value to safeguard for minors and their families, social networks, school, police, etc. Both the online reputation and physical world reputation should be considered.

A3 - Right to privacy and protection of personal data

The right to privacy of all individuals is a fundamental one in our society. It is considered as a factor in dignity and respect and contributes to a person's sense of self-respect. It might be materialised by respecting people's personal space, privacy in personal interactions and confidentiality of personal information. This asset carries very high value and importance, both at the level of EU and Member States. This right is anchored in national constitutions.

A4 - Effective and efficient law enforcement and policy investigation process

An effective and efficient law enforcement and policy investigation process is of great value for society. However, the principle of proportionality has to be maintained, that is, keeping a fair balance between the right of control and surveillance through the law enforcement bodies and the right of privacy of the citizen (A3).

A5 - Sense of security

Sense of security is the sense of protection from any kind of hostile actions. In the context of this work, sense of security is related to the feeling of security in the home, in social networks, online with regard to the individual's own devices, applications and data, to control over online activities and data and to the ability to judge other people's intent when protecting one's child, etc.

A6 - Right to Safety

The right to safety is considered as the right of individuals to actual security/safety from physical and mental harm. A broader definition of this term is "Everyone has the right to the highest attainable standard of protection against natural and man-made hazards" (19) .

Individuals have the right to safety with regard to consumed goods and services and to their environment (private and public). Producers of hardware, software and services should not make available or sell products that endanger the health and wellbeing of consumers.

A7 - Parental duty of care

Ordinarily, parents have the right to the custody and supervision of their child. In addition, parents have a duty to care for and look after their offspring. The child has the right to receive this care and the obligation to yield to reasonable parental guidance and supervision. The scope of the duty changes as societal values change. Similarly, the scope of the parental duty of care changes as the child's level of maturity and resilience develop.

A8 - Added value online services (i.e. Online Shopping, social networking, etc.)

Provided (added value) online services contribute to positive customer experience, that is, experience and feelings that the customer has in relation to online services, such as online shops. That includes, for instance, the positive online shopping experience derived from a tailored interface and/or customised offers based on profiling.

A9 - (Online) Social networking / socialising

This asset refers to the acts of meeting people and building communities online. The selection of meeting partners can be based on ages, personal interests, professional drives etc.

Tangible assets

A10 - Identification and authentication data (credentials)

These are credentials used for access to various devices and services such as:

- Computer devices
- Smart phones
- Monitoring SW
- Communication infrastructure
- Access to social networking data
- Access to services

A11 - Publicly available Personal Data

All the information that is deliberately and willingly made public by an individual. These might be IP-address, name, postal address, e-mail address, etc.

A12 Personal data with restricted access

These are data with access that is restricted to a limited group of people, or specific individuals. This access restriction is not explicitly imposed by the individual who generated them, but rather is applied by the recipients of the information. To this extent, there is no guarantee that the assumed restriction will always apply. Such data include, for instance:

- Personal data on a social networking site, such as:
- Data on PCs, laptops, netbooks
- Data on smart phones
- Data from filtering software
- Data from telecommunication providers regarding traffic from smart phones, fixed line phones, internet

A13 - Inferred Data

Inferred data/information are data achieved by cross-linking of various, independently generated data. According to some Data Protection Acts, such data are the result of “data matching” (i.e. in Greece) and are explicitly regulated (e.g. in UK). Such data are:

- E-shop profiles, social networking profiles, etc.

- Proximity networks of contacts: (i.e. rough estimation of the distance between two contacts)
- Communication patterns
- Relations to friends

A14 - Police investigation data

All the data and their interpolations used by police in preventing crime and conducting investigations. These data can come from various sources, e.g. monitoring activities on the internet, e-discovery and subpoenas, forensics etc.

A15 - End user computing devices

Computing devices are considered to be PCs, laptops and netbooks with an installed operating system, having internet access via LAN or WLAN. In the assessment, we consider that these devices store and process data as mentioned above (i.e. mentioned in A10, A11 and A12, A13 and A14).

A16 - Mobile personal devices

Such devices are communication devices including smart phones, PDAs, mobile phones, partially having internet access via LAN or WLAN. Mobile personal devices allow for location aware functionality, are versatile (they can be carried everywhere) and can be used for voice, email, MMS/SMS communication and broad band internet. In the assessment, we consider that these devices store and process data as mentioned above (i.e. mentioned in A10, A11 and A12, A13 and A14).

A17 - Communication infrastructure

Communication infrastructure consists of devices and systems aiming at the provision of telecommunication and broadband services. Via this infrastructure relevant data from A10, A11, A13 and A14 are being transmitted/processed. Communication infrastructure may include:

- Mobile (3G) communication infrastructure
- Fixed line communication infrastructure (both user and provider ends)
- Infrastructure for location based services
- Wireless communication infrastructure
- Infrared communication
- Bluetooth communication

- Configuration data of devices and services

A18 - Storage media

These are devices where data are being stored. The storage could be persistent and non-persistent. In the assessment, we consider that these devices store and process data as mentioned above (i.e. mentioned in A10, A11 and A12, A13 and A14). Examples of storage media are:

- Several USB thumb drives (USB Sticks)
- External hard disk drive
- Various SSDs (Smart phone, Camera, etc.)
- Data storage media for professional users (including buffered/replicated information)
- Cloud hosted services: data stored in the cloud and services provided over cloud

A19 - Application Provider Systems

These are applications operated by various online providers and offered as a service to users. In the assessment, we consider that these applications/services store and process data as mentioned above (i.e. mentioned in A10, A11 and A12, A13 and A14). Examples of such applications are:

- E-mail
- Instant messaging
- SMS/MMS
- Ad hock communication via mobile connections (peer-to-peer)
- Social networking sites
- e-commerce systems and services
- Other online software/applications

A20 - Data Collection and profiling tools

These are tools supporting the derivation of various conclusions/views out of a vast amount of unrelated information. It is worth mentioning that although the existence of such tools is legal, in the present scenario they are supposed to be used illegally. Within this scenario, they are considered as ‘assets’ although are ‘valuable’ only for the perpetrator, thus holding a kind of negative value.

A21 - Filtering tools/functions

These are monitoring services either installed on private computers or offered by the ISP. The former is software that has been set to gather all relevant data from the online activities of users of a computer. The latter is functionality offered by ISPs to gather information about internet usage and traffic of smart phones. With this kind of information, (adult) users may monitor the usage of online services initiated by computing or other smart devices.

4.2 Major risks

In this section we present the major risks identified. We have divided the risks into three categories according to the 'risk owner', that is, the individuals who are mainly exposed to these risks. However, the risks presented are not independent from each other, nor generally speaking do they refer to a single category of individuals. To this extent there are interdependencies among the identified risks that also span the categories used for their classification. The interdependencies among the risks will be mentioned within the description of each identified risk below. The categories identified are:

- *Teenagers*, meaning risks that apply to teenagers as individuals
- *Parents/guardians/teachers*, meaning risks that are related to the duty of care
- *Member State/law enforcement*, meaning risks that have to be addressed by states and law enforcement bodies/agencies

Within each category, we present the risks according to their severity level, that is, likelihood and impact on valuable assets upon materialisation. The risks have been identified and prioritised by means of a qualitative approach based on the assessed assets, their vulnerabilities, their threat exposure and impact. This has been performed by ENISA and distributed to the participating experts who provided their view/amendments/extensions. This information has then been consolidated into the final lists presented below. Besides the scenario formulation, this was one of the main tasks of the risk assessment for the presented scenario.

The detailed information on assets, vulnerabilities, threats, controls, etc. that has been used as the basis for the assessment can be found in Annexe I. This information might be of interest to experts wishing to reuse parts of it for relevant/future assessments.

As in other ENISA risk assessment reports (see (28), (29), (30)), together with the description of identified risks we give some additional information with regard to:

- **The affected assets** : those which have been identified in the previous section
- **The relative vulnerabilities and threats**: you can click on each item to navigate to Annexe I for more information

- **Reference to other risks**: most of the risks identified are highly interrelated, so specific reference to other relevant risks is made. Again, you may click on the item to navigate to the corresponding risk within the document.

The overall classification of each particular risk is not given. However, as mentioned above, within every category risks are prioritised according to their severity.

Teenagers

R1. Risk of suffering serious loss of physical or mental health as a victim of grooming/bullying

This risk embraces the worst impact on the most valuable assets of a victim, namely mental and physical health and, consequently, life. Although this is not an easy risk to materialise, it has been ranked as the highest one due to the fact that it has the maximum impact possible. Reported loss of life of victims of bullying and grooming proves that this risk can unfortunately have fatal outcomes and although such an eventuality has a relatively low likelihood, it is still very relevant.

Almost all of the risks mentioned below may contribute to increase exposure of a subject to this particular risk. Therefore the risk is considered to be a compound one and has dependencies to many of the risks identified (see table below).

It is worth mentioning that although this risk is assigned to teenagers, it might affect parents and educators too (especially with regard to mental health).

Affected assets	A1, A2, A3, A4, A5, A6, A7
Vulnerabilities	V1, V2, V3, V4, V8, V9, V10, V12, V13, V15, V16, V18, V19, V21, V24, V26, V 28, V30, V31, V32, V34, V35, V36, V37, V38, V39, V40, V41, V42, V43, V44, V45, V46, V47, V50, V51, V52, V53, V54, V55, V56, V57
Threats	T1, T2, T3, T4, T5, T6, T7, T8, T9, T10, T11, T12, T13, T14, T15, T16, T17, T18, T19, T20, T21, T22, T23, T24, T25, T26, T27, T28, T29, T30, T31, T32, T33, T34, T35, T36
Related risks	R2, R3, R4, R5, R6, R7, R8, R9, R10, R11, R12, R13, R15, R16, R18, R19, R20, R21, R22, R23

R2. Risk of teenagers exposing themselves to the internet by publishing information/content that may stigmatise their later lives (both intentionally and unintentionally)

Many subjects have stored information about themselves online (i.e. digital traces). In most cases, this information has a lifecycle that cannot be influenced by the subject who generated the information. In other words, the logical information owner is not in a position to control this information. Given that large amounts of information are

gathered / disseminated without the consent of users, a loss of self-determination of information takes place.

Teenagers are greatly exposed to this risk, as they exchange information intensively and they do not necessarily pay attention to its quality and quantity. Moreover, they do not have the appropriate social skills/experience to consciously and/or intuitively protect themselves from this risk. This information might create significant problems in their current and future lives (see (31), (32), (33)).

Affected assets	A1, A2, A3, A4, A5, A6, A7, A8, A10, A11, A12, A18, A19
Vulnerabilities	V1, V7, V8, V9, V12, V13, V15, V16, V17, V18, V21, V24, V25, V26, V27, V28, V29, V30, V31, V32, V33, V36, V37, V38, V39, V40, V41, V42, V43, V45, V46, V48, V49, V50, V51, V53, V55, V57
Threats	T1, T2, T3, T4, T5, T6, T7, T8, T9, T10, T11, T13, T14, T15, T16, T19, T20, T22, T28, T29, T30, T31
Related risks	R1, R3

R3. Risk caused by the imbalance between technical and social skills of involved subjects that are potential victims (teenagers' view)

Minors are often more advanced in dealing with new technology than adult generations. This gives them the impression that they are better managers of new technology devices, yet they often disregard operational and social issues connected with the use of such devices.

Hence, by being more advanced in technology than their parents and educators, they overestimate their knowledge and often feel that general advice from such adults can be ignored. This is regardless of whether the advice has a general, social or ethical context, or is related to the use of devices and applications. To this extent, they erroneously transfer their dominance in the area of technology to other areas covered by the advice of adults. The result is to disregard the opinion of adults and act on their own. This exposes minors to the risk of performing online actions that might be abused by potential perpetrators. Due to the long 'memory' of the online world, it can be the case that past actions might be misused at a later point in time (see also R2).

Affected assets	A1, A2, A3, A4, A5, A6, A7, A8, A9, A15, A16, A17, A18
Vulnerabilities	V1, V7, V8, V9, V12, V13, V15, V16, V17, V18, V21, V24, V25, V26, V27, V28, V29, V30, V31, V32, V33, V34, V36, V37, V38, V39, V40, V41, V42, V43, V45, V46, V48, V49, V50, V51, V52, V53, V55, V56, V57
Threats	T1, T2, T3, T4, T5, T6, T7, T8, T9, T10, T11, T13, T14, T15, T16, T19, T20, T21, T22, T28, T29, T30, T31
Related risks	R1, R2

R4. Risk to be discriminated against based on behavioural patterns

If one takes as given that users leave digital traces in the online world, then the risk that this information will be used to derive behavioural patterns becomes obvious. What is considered here as a risk is in fact the daily business of organisations that are engaged in the area of marketing and consumer behaviour. Due to the absence of user consent and relevant regulation, but also due to the unmanaged technical environments of commonly used software, the business of deriving behavioural patterns is definitely a 'grey area' (at least from a legal point of view). This poses a risk for organisations that is often neglected in favour of the achieved profits (i.e. balancing risks vs. opportunities).

Minors are highly exposed to this risk. The group receives a high level of attention when it comes to identification of behavioural patterns. Besides commercial reasons, building behavioural patterns for minors might happen for a variety of malevolent purposes that go far beyond those covered within this assessment (e.g. see (8), (34)).

Affected assets	A1, A2, A3, A5, A8, A9, A11, A12, A13
Vulnerabilities	V1, V7, V8, V9, V13, V15, V16, V17, V18, V19, V21, V24, V26, V27, V28, V29, V30, V31, V32, V33, V35, V36, V37, V38, V39, V40, V41, V42, V43, V50, V51, V52, V56, V57
Threats	T1, T2, T3, T4, T5, T6, T7, T8, T9, T10, T11, T13
Related risks	R1, R14, R16, R17

R5. Risk of being misused as a result of information loss (e.g. loss of personal data, mobile devices, other gadgets)

Minors can be easily distracted and forgetful, thus often losing their belongings. Given the fact that this can even be abused in order to purloin items from minors, it becomes apparent that there is a high exposure to the risk of losing devices and gadgets. Even if measures are implemented in order to protect personal information, loss of devices will lead to loss of the information. In cases where strong mechanisms are in place (e.g. strong encryption, strong passwords) successful human engineering attacks might still help to break this protection.

When a perpetrator obtains access to information from a personal device, it is very easy to start harmful activities against the owner of the device and his or her social environment.

Affected assets	A1, A2, A3, A5, A6, A9, A10, A11, A12, A13, A15, A16, A18, A19
Vulnerabilities	V1, V2, V9, V10, V12, V16, V18, V19, V24, V25, V26, V28, V29, V31, V33, V37, V45, V46, V49
Threats	T6, T8, T11, T12, T14, T15, T20, T22, T28, T31, T32, T33

Related risks	R1, R3, R5, R6, R8, R9, R11, R13, R16, R17, R20

R6. Risk that teenagers become victims of grooming/bullying activities from their social environment

Bullying is a negative treatment of individuals from the wider social environment. As with harassment, bullying can be defined largely by the impact of the behaviour on the recipient, not its intention. In varying intensiveness, bullying is a very common phenomenon, especially at schools and within groups of teenagers. Almost anyone might have school memories that are connected to bullying activities (either as victim or even participating in bullying of other classmates). Given all this, bullying is a phenomenon most teenagers have experienced and, as such, they are exposed to the risk of being bullied.

Minors might be exposed to grooming too. Grooming is the process of selecting an individual as victim with the intention of carrying out sexual abuse. Although, by comparison with bullying, exposure to grooming risk might be lower, the impact of grooming on a victim is definitely higher.

Although neither risk is new, cyber space radically expands their potential sphere of influence and the possibilities for contacting potential victims.

Affected assets	A1, A2, A3, A5, A6, A7, A9, A11
Vulnerabilities	V1, V2, V8, V9, V12, V13, V14, V15, V16, V17, V18, V19, V21, V24, V26, V27, V28, V29, V30, V31, V32, V33,V34, V35, V36, V37, V38, V39, V40, V41, V42, V43, V45, V46, V50, V54, V55, V56, V57
Threats	T1, T2, T4, T5, T6, T7, T8, T9, T10, T11, T14, T19, T20, T28
Related risks	R1, R2, R3, R5, R7, R12, R14, R15, R16, R17, R19

R7. Risk that teenagers become the subject of malicious attacks from adult individuals on the basis of digital traces they left on the internet

Teenagers are particularly exposed to this risk. It is an explicit consequence of the risks R2, R3and R4mentioned above. This risk is mentioned in this assessment in order to underline the fact that teenagers are a potential target group for malicious adult individuals. Furthermore, teenagers might be more 'receptive' with regard to human engineering, as they are not always in the position to recognise malicious intent. Cyber space, together with existing tools, offers such adult individuals the opportunity of massive, qualitative attacks.

Affected assets	A1, A2, A3, A5, A6, A7, A9, A11, A12, A13, A20, A21

Vulnerabilities	V1, V2, V7, V8, V9, V11, V12, V13, V15, V16, V17, V18, V21, V24, V26, V27, V28, V29, V30, V31, V33,V34, V35, V36, V37, V38, V39, V40, V41, V42, V43, V44, V47, V50, V51, V53, V55, V56, V57
Threats	T1, T2, T4, T5, T6, T7, T8, T9, T10, T11, T14, T22, T28
Related risks	R1, R2, R3, R4, R5, R6, R9, R10, R12, R14, R15, R16, R17, R19

R8. Risk of failing defending oneself due to lack of knowledge/evidence/legal framework

In the case of disputes concerning bullying and grooming activities (but also cybercrime in general), it is necessary/important to be in a position to deliver evidence. This is a fundamental need/right with regard to the feeling of security and justice (see also assets A1, A2, A5 *and* A6). The provision of evidence can protect against criminalisation/victimisation directed at both adult and teenage individuals.

When developing cyber space activities, it is often impossible to obtain or maintain evidence. This is mainly due to segmentation of information when an end-to-end point of view is taken. Examples of this segmentation are: multiple storage of personal and derived data, different levels of responsibility (logical, physical/geographical), different operators involved in the delivery of services, different management and legal regimes within countries, etc.

Affected assets	A1, A2, A3, A4, A5, A6, A8, A9
Vulnerabilities	V7, V18, V26, V36, V40, V43, V44, V45, V53, V54
Threats	T1, T2, T3, T5, T12, T14, T15, T16, T17, T18, T20, T21, T22, T23, T24, T25, T26, T27, T28, T29, T31, T32, T33, T34, T35, T36
Related risks	R1, R7, R11, R18, R20, R21, R22, R23

R9. Confidentiality/integrity risks for the used identification data and possible misuse resulting from these risks

As with any individual acting online, teenagers are exposed to confidentiality and integrity risks with regard to their identification data. This information can be stolen and misused, thus leading to other related risks, such as R5, R6, R7, and R8.

Although this risk might be considered as a special case of risk 5 (R5) above, the assessment team decided to explicitly state this risk in order to underline the value, security relevance and impact connected to identification data (such as credentials, passwords, PINs, etc.). It is imperative to protect this information in order to mitigate many risks mentioned in this assessment.

Affected assets	A1, A2, A3, A4, A5, A6, A7, A8, A9, A10, A11, A12, A13, A14, A15, A16, A18, A19

Vulnerabilities	V1, V2, V8, V9, V10, V12, V13, V15, V16, V17, V18, V19, V26, V27, V28, V30, V31, V32, V33, V34, V35, V44, V45, V46, V49, V55, V57
Threats	T2, T4, T5, T6, T7, T8, T11, T12, T14, T15, T16, T22, T28, T31, T32, T33
Related risks	R1, R3, R5, R6, R7, R8, R11, R13, R16, R17, R19, R20

R10. Risk that teenage children are sceptical about the capabilities of their parents to advise on something they know and understand very little about

It is a fact of life that new technologies are more widely adopted and used by newer generations. For this reason, teenagers have a better knowledge of new technologies and are more interested in new/emerging developments. This advancement in comparison with adults gives them an important role in families with regard to installation, management and usage of technological devices. Eventually, adults do not see themselves as being in a position to provide advice to teenagers with regard to new technologies. Similarly, teenagers would not accept advice from their parent in that area.

This situation is risky, since advice from adults regarding the risks of internet usage might be seen as advice about technology and would be ignored. This would happen even if the advice of an adult is not on a purely technical issue. As a result, teenagers would disregard the opinion of adults and act on their own.

Being a specialised aspect of R3, this risk has been adopted because it clarifies reasons for R3to happen. The assessment team decided to formulate this risk in order to indicate a possible cause of potential opinion mismatch between teenagers and parents. Furthermore, this risk related to purely technical assets (as opposed to R3).

Affected assets	A1, A2, A3, A4, A5, A6, A7, A8, A9, A10, A11, A12, A13, A19
Vulnerabilities	V1, V9, V16, V21, V24, V27, V28, V29, V30, V31, V33, V35, V42, V45, V46, V48, V55, V56, V57
Threats	T1, T2, T3, T4, T6, T7, T8, T9, T10, T11, T13, T14, T15, T16, T19, T20, T22, T28, T31, T32, T33
Related risks	R1, R2, R3, R4, R5, R6, R7, R9, R15

R11. Risk of being accused of actions that were not one's own (e.g. due to manipulation and inability to provide evidence)

Individuals involved in the assessed scenario are considered to be exposed to the risk of being accused for actions that were not their own. That is, independent of their intention, (a group of) offenders might try to generate evidence that an individual has been involved in deceptive activities in order to assassinate the victim's character. This is a common method used by bullies.

Seen in combination with the difficulty of providing evidence for online activities (see risk R8), the exposure to this risk is significant and might be a starting point for other assessed risks (e.g. R4, R6, R1).

Affected assets	A1, A2, A3, A4, A5, A6, A7, A8, A9, A10, A11, A12, A13, A14, A15, A16, A18, A19
Vulnerabilities	V1, V2, V7, V9, V12, V13, V15, V16, V17, V18, V19, V21, V24, V26, V27, V28, V29, V30, V31, V32, V33,V34, V35, V36, V37, V39, V40, V41, V42, V43, V44, V45, V46, V47, V48, V49, V50, V54, V55, V56, V57
Threats	T2, T5, T6, T8, T11, T12, T14, T15, T16, T22, T32, T33
Related risks	R1, R4, R6, R8, R11, R13, R18, R20

R12. Risks arising from unavailability of services

Teenagers may be exposed to some risks resulting from the unavailability of services. Mainly, these risks relate to the unavailability of location based services, telecommunications services or additional online services that are used by adults to exercise their duty of care. Such services might be useful in maintaining the contact with teenagers to monitor their online behaviour, etc.

Affected assets	A5, A6, A7, A9, A10, A11, A12, A17, A19
Vulnerabilities	V2, V4, V6, V10, V11, V14, V32, V54
Threats	T21, T27, T29 , T30, T34, T35
Related risks	R1, R2, R3, R4, R5, R6, R7, R15, R17, R19

R13. Risk of being excluded from digital developments (e-exclusion)

For a variety of reasons that are related to potential misuse in cyber space, the risk of being excluded from digital development seems to be relevant for teenagers. Excess of parental care, overestimation of exposed risks, over-reaction of parents to online usage patterns of teenagers, unfounded fear of online activities and distrust of the digital environment might lead to hesitation by teenagers to use new technologies. This would be an unfortunate development for a young individual, as technology is one important tool in knowledge transfer, social networking, exchange of ideas and experiences. On the other hand, such exclusion equals a limitation in liberties and in possibilities for personal development.

Affected assets	A8, A9, A13

Vulnerabilities	V1, V2, V9, V12, V13, V16, V17, V18, V19, V21, V24, V26, V27, V28, V30, V31, V32, V33, V34, V35, V36, V37, V39, V40, V41, V42, V43, V44, V45, V46, V47, V48, V49, V50, V52, V54, V55, V56
Threats	T1, T2, T3, T4, T5, T6, T7, T8, T9, T10, T11, T14, T14, T15, T16, T17, T19, T21, T22, T23, T26, T27, T28, T29, T32, T33 Louis
Related risks	R1, R14, R15

Parents / guardians / teachers

R14. Risk related to behavioural patterns of teenagers, affecting the effectiveness of parental care (e.g. by developing a second life in cyber space, by uncontrolled virtual or physical meetings with cyber friends)

By being more acquainted with technology and by being more receptive to newly developed ideas and concepts, teenagers tend to develop activities that are beyond the sphere of the culture, influence and control of their parents/guardians. Hence, online activities and cyber space introduce a major cultural change in the modern era that amplifies differences between the two generations in comparison with previous times. This is a behaviour that is natural to new generations and is often part of the 'gap' between teenagers and adults.

Due to its nature, exposure to this risk is inevitable and has to be managed by adults in order to avoid its materialisation, thus leading to significant impact on the teenager's current and future life (especially with regard to cyber bullying and grooming).

Affected assets	A1, A2, A3, A5, A6, A7, A8, A9, A11, A12, A13
Vulnerabilities	V1, V2, V8, V9, V12, V13, V15, V16, V17, V18, V19, V21, V24, V27, V28, V34, V36, V37, V39, V40, V41, V42, V43, V44, V45, V51, V52, V53, V55, V56, V57
Threats	T1, T2, T3, T4, T5, T6, T7, T8, T9, T10, T11, T13, T14
Related risks	R1, R2, R3, R4, R6, R7, R13, R15, R16

R15. Risk of inability to control online activities of teenagers (information hiding, unavailability of knowledge of the systems used, inability to control online interaction)

Based on the risk R14 and also on the fact that adults often have difficulties in understanding the behavioural patterns of teenagers, their ability to control online activities shrinks. Often, exposure to this risk increases due to absence of knowledge regarding the involved technology, its interconnections and interdependencies. The reduction of adults' ability to control online interaction also results from the fact that

teenagers often act ad hoc, are inventive/creative, invest more time and energy, and tend to hide information from their parents/guardians.

Affected assets	A1, A2, A3, A5, A6, A7, A8, A9, A10, A11, A12, A13, A19
Vulnerabilities	V1, V9, V13, V15, V17, V19, V51, V53, V56, V57
Threats	T1, T2, T3, T4, T5, T6, T8, T9, T10, T11, T13, T14, T15, T16, T21, T22
Related risks	R1, R2, R3, R4, R5, R6, R7, R10, R13, R14, R16, R17, R19

R16. Inability to provide and maintain a secure digital environment for teenagers to use (including the computing and communication infrastructures used)

Given that even in professional environments vulnerabilities related to ineffective patch management exist, a similar situation will prevail within private digital infrastructure environments. Such vulnerabilities can be easily abused and can lead to the materialisation of this risk. A similar situation exists for various gadgets that also have online access (e.g. mobile phones, smart phones, smart devices, etc.).

To this extent, the exposure to this risk is high for all of the devices that are used by teenagers and maintained either by them or by their parents. (At least) a similar exposure will exist at schools, where the school network is more complex and maintenance requires higher levels of expertise.

Affected assets	A1, A2, A3, A4, A5, A6, A7, A8, A9, A10, A11, A12, A13, A14, A15, A16, A18, A19
Vulnerabilities	V1, V2, V10, V16, V18, V24, V27, V28, V29, V30, V31, V32, V33, V35, V40, V45, V46, V47, V54, V55, V56, V57
Threats	T2, T3, T4, T5, T6, T8, T9, T10, T11, T12, T13, T14, T21, T22, T23, T24, T25, T26, T27, T28, T30, T31, T32, T33, T34, T35, T36
Related risks	R1, R2, R3, R4, R5, R6, R7, R9, R15, R17, R19

R17. Inefficiency in fulfilling the care duties within school (inability to control digital habits of children, insufficient knowledge of the related issues, both from the technical and educational point of view)

This risk is an extrapolation of the risk R16 to school environments. The reason for providing an additional risk with similar content is due to the fact that a school environment is a place where children spend most of their time, but also due to the increased complexity of the school infrastructure. (At least) a similar exposure will exist in schools, where the school network is more complex and maintenance requires higher levels of expertise.

Given the bigger number of infrastructure components at school, the likelihood of vulnerability is higher, thus leading to a potentially higher exposure than in home environments. On the other hand, due to the larger accumulation of electronic, digital devices (i.e. brought in by pupils), a larger potential for misuse is to be expected in the school and in the vicinity of schools. This is a fact that further aggravates the fulfilment of care duties in school environments and poses a significant risk to educators.

Affected assets	A1, A2, A3, A5, A6, A8, A9, A10, A11, A12, A13, A15, A16, A18, A19
Vulnerabilities	V1, V2, V5, V6, V9, V16, V18, V19, V24, V26, V27, V28, V29, V30, V31, V32, V33, V35, V36, V40, V41, V42, V43, V44, V45, V46, V47, V49, V54, V55, V56, V57
Threats	T2, T3, T4, T5, T6, T8, T9, T10, T11, T12, T13, T14, T15, T16, T17, T18, T21, T22, T23, T24, T25, T26, T27, T28, T30, T31, T32, T33, T34, T35, T36
Related risks	R1, R2, R3, R4, R5, R6, R7, R9, R12, R14, R15, R16, R19

R18. Risk of failing to defend oneself due to lack of knowledge/evidence/legal framework

This risk is similar to R8 just extrapolated to parents/guardians/educators. The reason for explicitly mentioning that risk in this category is that parents/guardians/educators are exposed to the risk that they might be maliciously victimised as an act of revenge stemming from unpleasant educational/teaching experiences and/or defamation.

Similarly to R8, the collection of evidence with regard to cyber activities is very difficult to perform. Equally, attacked individuals are often lacking the knowledge to defend themselves. The awareness regarding applicable regulation in that area is very low.

Affected assets	A1, A2, A3, A4, A5, A6, A8, A9, A10, A11, A12, A13, A14, A15, A16, A18, A19
Vulnerabilities	V2, V7, V8, V9, V12, V13, V15, V16, V17, V18, V19, V21, V24, V26, V27, V28, V29, V30, V31, V32, V33, V34, V35, V36, V37, V38, V39, V40, V41, V42, V43, V44, V45, V46, V49, V50, V51, V52, V53, V54, V55
Threats	T1, T2, T3, T4, T5, T6, T7, T8, T9, T10, T11, T12, T13, T14, T15, T16, T21, T22, T28, T30
Related risks	R1, R8, R11, R20, R21, R22, R23

R19. Risk from unavailability of services (mainly used to exercise duty of care)

Unavailability of security, monitoring and control functions of the computing environment may lead to a complete inability of parents/guardians/educators to exercise their duty of care with regard to the online activities of their children. Eventually, additional control functions might suffer as well.

Unavailability risks may result from failure in the provisioning of communication services (e.g. ISP, mobile provider, fixed line provider, etc.). Such failures may occur either by mistake or when attackers abuse existing vulnerabilities of the computing environment to compromise the systems and running functions.

Another source of risks emanates from teenagers themselves; given the advancement in technology knowledge of teenagers and their genuine interest to escape the control of adults, they might try to overcome existing controls in numerous ways.

Affected assets	A1, A2, A3, A5, A6, A7, A8, A9, A17, A19
Vulnerabilities	V1, V2, V4, V5, V6, V8, V9, V10, V12, V13, V14, V15, V16, V17, V18, V19, V22, V23, V27, V29, V32, V33, V35, V40, V48, V54, V55, V56, V57
Threats	T1, T2, T3, T4, T5, T6, T8, T9, T10, T11, T13, T14, T15, T22, T30, T34, T35, T36
Related risks	R1, R2, R3, R4, R5, R6, R7, R12, R13, R14, R15, R16, R17

R20. Risk of being accused of actions that were not one's own (due to manipulation, absence of traces/inability to provide evidence)

This risk is an extrapolation of risk R11 for the groups of parents/guardians/educators. The risk has been repeated here because it has a different impact for these groups. Obviously, the group of potential perpetrators behind this risk is rather wide (e.g. pupils, parents, criminals, colleagues, etc.). To this extent, this risk is considered to be a serious one, especially for this group. There are strong motives for attackers to try to materialise this risk, such as harassment, defamation, challenging guardianship, etc.

Seen in combination with the difficulty of providing evidence for online activities (see risk R18), the exposure to this risk is significant and might be a starting point for other assessed risks (e.g. R1, R4, R6, R15, R16, R17).

Affected assets	A1, A2, A3, A4, A5, A6, A7, A8, A9, A10, A11, A12, A13, A14, A15, A16, A18, A19
Vulnerabilities	V1, V2, V7, V9, V12, V13, V15, V16, V17, V18, V19, V21, V24, V26, V27, V28, V29, V30, V31, V32, V33,V34, V35, V36, V37, V39, V40, V41, V42, V43, V44, V45, V46, V47, V48, V49, V50, V54, V55, V56, V57
Threats	T1, T2, T5, T6, T8, T11, T12, T14, T15, T16, T22, T32, T33
Related risks	R1, R4, R5, R6, R11, R15, R16, R17, R18, R21, R22, R23

Member State/law enforcement

R21. Inability to follow misuse cases due to missing resources and knowledge

Recent experiences reported within the group of experts indicate that curricula with cyber-crime skills are rather rare within law enforcement agencies. Rather, people from conventional crime fighting units are assigned to cyber-crime, often after attending some relevant seminars. Furthermore, no internationally recognised curricula for cyber-crime investigation/forensics exist and skills related to this area are still not well defined. This situation is exacerbated by the short innovation cycles of technology. Available knowledge might quickly become out-dated if recent developments are not properly followed up (see also (10)).

This fact highlights the existence of and exposure to this risk, especially when considering the levels of resource and knowledge availability within law enforcement agencies. Given that staff with sufficient experience will be a key element for the fight against cyber-crime, shortage of resources will significantly reduce the effectiveness of law enforcement.

Furthermore, gaps in organisational interfaces among various law enforcement agencies are often misused by criminals in order to succeed in their attacks. Experience from recent successful attacks shows that communication/coordination gaps between authorities have been major vulnerabilities abused by the attackers. This mostly happens intentionally, but in some cases unintentionally.

Affected assets	A1, A2, A3, A4, A5, A6, A8, A9, A10, A11, A12, A13, A14, A15, A16, A18, A19
Vulnerabilities	V2, V7, V9, V10, V12, V13, V14, V15, V16, V18, V24, V26, V27, V28, V29, V32, V33, V35, V36, V37, V40, V41, V43, V44
Threats	T1, T2, T3, T4, T5, T6, T8, T11, T12, T14, T20, T21, T22, T23, T24, T25, T26, T27, T28, T29 , T32, T33, T35
Related risks	R1, R2, R3, R4, R5, R6, R7, R8, R11, R16, R17, R18, R20, R22, R23

R22. Inability to follow misuse cases due to multinational investigations being required (i.e. outside the sphere of national influence/law enforcement)

In many cases, cybercrime and especially cyber bullying and online grooming will involve IT-platforms that span national borders. Therefore, any investigation concerning misuse cases will most probably involve multiple organisations from various countries. Differences in national regulation turn international co-operation into a rather slow and ineffective interaction.

Due to the diversity of the organisations involved, misuse cases often cannot be followed up promptly due to time consuming communication between entities involved at global/multinational level (i.e. Telcos/ISPs, state agencies, law enforcement, etc.). By being unable to meet time constraints, international investigations in the area of cyber bullying and online grooming will tend to be quite ineffective.

Both these facts lead to a high exposure to this risk. Seen in relation to R21 and R23, this is a significant risk that has to be mitigated through national and international regulation and multinational co-operation agreements between competent bodies and organisations.

Affected assets	A1, A2, A3, A4, A5, A6, A8, A9, A10, A11, A12, A13, A14, A17, A19
Vulnerabilities	V1, V2, V7, V12, V13, V14, V17, V26, V32, V36, V37, V40, V43, V55
Threats	T1, T2, T3, T5, T6, T8, T11, T12, T14, T21, T22, T32, T33, T35
Related risks	R1, R2, R3, R4, R5, R6, R7, R8, R11, R16, R17, R18, R20, R21, R22, R23

R23. Inability to follow misuse cases due to varying levels of maturity of relevant regulations in different countries

Varying levels of maturity in national regulations make it difficult to follow up cases that span national borders. Legal grounds for starting investigations of a case in a certain country may not be sufficient in another country involved in the case. Similarly, the conditions for starting and following up prosecution may be different in various countries. A typical example is data protection legislation that widely varies between countries (e.g. Europe, US, China, etc.).

Seen in relation to R22 the exposure to this risk is significant and may lead to difficulties in rendering justice in cases of cyber bullying and online grooming that involve organisations, persons and authorities at global level.

Affected assets	A1, A2, A3, A4, A5, A6, A8, A9, A10, A11, A12, A13, A14, A17, A19
Vulnerabilities	V1, V2, V7, V12, V13, V14, V17, V26, V32, V36, V37, V40, V43, V55
Threats	T1, T2, T3, T5, T6, T8, T11, T12, T14, T21, T22, T32, T33, T35
Related risks	R1, R2, R3, R4, R5, R6, R7, R8, R11, R16, R17, R18, R20, R22, R23

5 Recommendations

In this section we provide recommendations to mitigate identified risks. We have assigned a title to every recommendation in order to give an overview of the topic addressed. The proposed recommendations have been grouped according to the target groups they concern. The target groups envisaged are:

- *Member States/law enforcement agencies and Civil society/social partners*: these recommendations concern mainly legal frameworks, personnel and knowledge issues, practices for application of existing legislation etc.

  As regards Civil Society / Social partners, measures that should be taken in order to generate the social conditions and will facilitate protection of minors using the internet are being taken into account.
- *Parents/guardians/educators:* these recommendations concern the support of guardians in facing the challenge of online protection of minors. They include measures to enhance knowledge, promote a sense of privacy and foster interfaces with other target groups

- *Teenagers:* these recommendations relate to a collection of actions for strengthening the online security posture of teenagers. Furthermore, several proposals are made (e.g. for industry) in order to take into consideration the specialised needs of minors in their protection schemes, both from the passive (e.g. automated protection) and active (e.g. facilitating the use) point of view.

The proposed recommendations are ideas that need to be further elaborated and can be taken up by organisations/authorities/Member States to further enhance protection of minors in cyber space. Similarly, these recommendations can lead to applied research in the area of online protection measures/controls, particularly tailored to the needs of minors. Finally, it is worth mentioning that the issued recommendations are not overlap free; that is, some of those, although assigned to a certain group, might have consequences/depend on recommendations assigned to another group.

Member States / law enforcement agencies and Civil Society / Social Partners

RC1 - Establish balance in relevant regulations/laws

Balance of the legislation regarding online and real life crimes seems to be necessary (i.e. online grooming and meetings with minors). Legal practices for both kinds of crimes may not differentiate in essence. Furthermore, homogenisation of legislation at international level has to be accounted for (see (35)). This seems to be necessary in order to follow up cross border cases. Legislation balance and homogenisation might prove to be laborious and very time consuming.

RC2 - Collect statistical data

Governments should collect information regarding known cases of misuse (i.e. online grooming and cyber bullying observation). Relevant information should be collected by law enforcement agencies, reported and shared with concerned parties (e.g. governments, educators, parents, etc.). Subsequently, this information should be used in combating these crimes. Experience about perpetrator practices, weaknesses, capabilities and motives will help in advancing security controls and thus protecting all involved individuals.

RC3 - Strengthen law enforcement agencies

Enable law enforcement by performing investigation and enforcement activities promptly and effectively. This is of fundamental importance for the kind of misuse mentioned in the present scenario, where timeliness is a key issue for the protection of victims, both in cyber bullying and online grooming. In order to achieve this, engagement of additional resources within law enforcement agencies - both in terms of personnel and skills - has to be taken into account.

RC4 - Follow up privacy breaches

The generation of user profiles without their consent is in most cases not possible, that is, it is deemed illegal within the terms of current data protection regulation (36). Similarly, the generation and use of user profiles for underage persons should not be possible in general. In special cases this could be made possible by explicit request from their parents/guardians. In such cases, regulations are flouted (and particularly in the case of minors), penalties should be such that the companies involved can be seriously impacted, both financially and in the context of their image. Hence, we recommend reconsidering existing fines for violation of data privacy issues and better streamlining the application of existing legal frameworks. Some Member States have identified this necessity (37). However, the issue is still at the level of initial discussions. Companies who trade extensively in personal data without the consent of users, or pursue irregularities with regard to data protection law, should be fined in ways that would have significant impact on their market presence (38).

RC5 – Develop knowledge and provide support

Community services should consider maintaining and offering technological knowhow to all involved target groups regarding the use of gadgets, online activities, use of services, etc. This should happen in the most effective way (e.g. within schools, but also outside schools as a leisure activity on a voluntary basis). The approach taken to this could be to make technological knowhow part of formal, non-formal and informal education. Similarly, capabilities to take care of victims and other concerned parties (e.g. parents, educators) should be put in place and cooperate with other relevant care services and agencies (i.e. through 'multiplier' roles, such as law enforcement, youth and social workers).

RC6 – Develop target group oriented awareness campaigns

Awareness raising activities should be part of the knowledge transfer process. They should be developed to assist in the understanding of risks faced while using social networking environments. Such activities should be adapted to the age and lifestyle of the target

audience and be disseminated at the levels of families, schools social partners and other relevant organisations and target groups (i.e. teenagers, parents, educators, etc.). Channels that are popular with the respective target groups should be used for the dissemination of such material (e.g. internet television, social networking sites, community centres, etc.). It is particularly important to develop sponsorships for these kinds of awareness campaigns and to consider creating public partnerships for greater impact and efficiency.

Parents / guardians / educators

RC7 – Enhance level of behaviour knowledge

Enhance skills of parents and educators with regard to knowledge of the online behavioural patterns of minors. Keep continuous communication with parents/educators. Discuss irregularities and consult experts in that area (behavioural psychologists) and participate in knowledge sharing activities relating to that area. This kind of knowledge sharing should be part of a general campaign about the protection of children, both in physical and cyber space.

RC8 – Enhance knowledge on technology

Undertake knowledge transfer to parents/educators with regard to technical issues. Depending on the role in duty of care/education, different levels of knowledge would be necessary. Relevant programs have to be offered to these individuals according to their needs and roles. The knowledge transfer should include awareness material and also (i.e. on demand) technological knowledge.

RC9 – Enhance privacy posture

Teenagers, parents and educators should be kept informed about privacy issues with regard to the cyber world. For teenagers and teachers, this should be part of their education. For parents, this knowledge should be transferred through awareness activities supported by the state/school/police/other social organisations/partners.

RC10 – Trigger knowledge exchanges

Technological knowledge should be regularly exchanged between parents and minors. By keeping an open channel with teenagers on technological issues, it easier to assess their knowledge, level of interest, level of use and usage patterns. It is recommended that this exchange should take place as with any other discussions between parents/educators and teenagers. Special fora at schools might be a channel to facilitate these kinds of knowledge exchanges.

RC11 – Use of specialised security controls for parents/educators

Consider using security controls that are especially customised for use by parents/educators. In the same manner, use interaction paradigms with security/privacy controls that are better suited to these target groups. This will help them to understand the purpose of the controls and better master their use/customisation and maintenance.

RC12 – Offer support for teenagers at schools

It is important to identify potential cyber bullying and online grooming attacks as early as possible. For this reason, teenagers should have immediate access to specialised advice points that are located at schools, to which they can turn in cases where support is required. Such advice may include information for the family or other social organisations that might be supportive to the individual. The possibility of being able to check the validity of potential complaints should also be considered. In such cases, law enforcement might be involved as well. We recommend that schools check the feasibility of offering this advice/support to minors by engaging appropriate skills (i.e. by cooperating with other social partners).

Teenagers

RC13 – Use of specialised security controls for teenagers

Consider the deployment of security controls for devices used by teenagers in order to prevent easy access to information (e.g. when devices are lost, in cases of misuse, eavesdropping, etc.). This might be a low cost alternative that will significantly enhance the security of the devices used and of communication.

RC14 – Adapt existing security controls to teenagers

Currently, in many areas of everyday life, there are security/safety controls that are adapted to children (e.g. cars, planes, ships, toys, etc.). A similar approach should be introduced in cyber space. We therefore recommend considering the deployment of security controls that are specially customised for use by teenagers/minors. In the same manner, use interaction paradigms with security/privacy controls that are better suited to the teenage generation. This will help them to understanding the purpose of the controls and also to better master their use/customisation.

Hence, we recommend considering the expansion of the security features in applications with functions that implement special protection needed by minors, such as privacy, anonymity and specialised access control. Such security features would allow for a better (fine grained) assignment and management of user profiles, including access rights to personal information.

RC15 – Develop online rating Schemes

In the TV and film industries, parental guidelines exist in order rate television programmes in terms of explicit sexual content, graphic violence and strong profanity. In the area of computer and video games, similar guidelines exist to score/classify them accordingly. Similarly, the establishment of parental guidelines for online content (services, web sites, social networking applications, etc.) could be considered. Such a function could co-exist with additional (automated) trust enhancing controls such as Web of Trust, reputation systems for online content providers, etc. Eventually, access to content with an acceptable rating could be part of browsers' parental control functions and other gadgets/applications.

RC16 – Perform Privacy Impact Assessments

Numerous web applications/services process significant amounts of personal data (e.g. social networking sites). Given the assessment of this report and other assessments performed

(ENISA Refs), significant risks to individual and society might emerge from misuses of such data. It is therefore recommended that criteria should be developed in order to identify application areas where a Privacy Impact Assessment needs to be performed prior to the deployment of the service. Such an assessment should identify potential privacy risks for the individuals using the service (similarly to Privacy Impact Assessment recommendation for RFID applications, see (39)).

RC17 – Deactivation of all active components

Various handheld devices, portable computers, etc. may have applications installed that have active components, that is, they communicate/process data (e.g. location data, movement data, etc.) in the background. We recommend that users are equipped with functions allowing them to stop any background functions communicating personal data to some service/application providers. This function is important for teenagers and parents, as the activity of devices can be explicitly/selectively switched off (e.g. during class lessons). This recommendation resembles the principle expressed as 'right to the silence of the chips' by the European Commission (see (40)) and represents the right of individuals to explicitly request suspension of processing that might affect their privacy.

RC18 – Enhance age oriented access control

We recommend that the age of users becomes an integral part of their credentials throughout the entire infrastructure and in particular the authentication/authorisation mechanisms used. Currently, not all links in the authorisation/authentication chain use age as an element (e.g. various operating systems). This leads to a fragmentation of the management of access rights and makes their management an intensive and error prone task. This leads in turn to parents/guardians/educators experiencing difficulties in exercising parental care.

6 Bibliography

1. **ENISA.** Emerging and Future Risks Framework - Introductory Manual . *European Network and Information Security Agency (ENISA).* [Online] ENISA, 1 March 2010. [Cited: 3 February 2011.] http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/emerging-and-future-risks-framework-introductory-manual/at_download/fullReport.

2. Children more savvy with computer skills than life skills, report suggests. *bee-it.* [Online] bee-it, 20 January 2011. [Cited: 3 February 2011.] http://bee-it.co.uk/faq/484.html.

3. Technology tots: The children who can use a mouse but can't tie shoelaces. *Daily Mail Online.* [Online] 20 January 2011. [Cited: 3 February 2011.] http://www.dailymail.co.uk/sciencetech/article-1348786/Children-use-mouse-tie-shoelaces.html.

4. **NA.** Apple accused of secretly collecting data from iPhone, iPad users. *biz.thestar.com.my.* [Online] The Star Online, 22 April 2011. [Cited: 07 June 2011.] http://biz.thestar.com.my/news/story.asp?file=/2011/4/22/business/20110422073307&sec=business.

5. **Arthur, Charles.** TomTom satnav data used to set police speed traps. *guardian.co.uk.* [Online] The Guardian, 28 April 2011. [Cited: 7 June 2011.] http://www.guardian.co.uk/technology/2011/apr/28/tomtom-satnav-data-police-speed-traps.

6. **Gaudin, Sharon.** Sony warns users of data loss from PlayStation network hack. *computerworld.com.* [Online] Computerworld, 26 April 2011. [Cited: 7 June 2011.] http://www.computerworld.com/s/article/9216191/Sony_warns_users_of_data_loss_from_PlayStation_network_hack.

7. **Kageyama, Yuri.** Nintendo says US server breached, no data lost. *yahoo.com.* [Online] Yahoo, 5 June 2011. [Cited: 7 June 2011.] http://finance.yahoo.com/news/Nintendo-says-US-server-apf-2415988336.html?x=0.

8. Sarah Kershaw, Sharing Their Demons on the Web, New York Times. *http://www.nytimes.com/2008/11/13/fashion/13psych.html?fta=y.* [Online]

9. *Briefing on the internet, ecommerce, children and young people.* [www.chis.org.uk] Watford, UK : children's charities' coalition on internet safety (CHIS), 2010.

10. *Four sets of Guidelines developed specifically for a particular stakeholder group: Children, Parents&Educators, Industry and Policy Makers.* [ITU Web Site:] s.l. : International Telecommunications Union (ITU). http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html.

11. **UNESCO.** Anticyberbullying Chapter. *Cyberbullying - conflict of modern school.* [Online] 14 January 2011. [Cited: 3 February 2011.] http://aces.lupacovka.cz/.

12. INSAFE. *Safer Internet.* [Online] European Network of Awareness Centres. [Cited: 3 February 2011.] http://www.saferinternet.org/web/guest/home.

13. **Commission, European.** *Proposal for a Directive on combating sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA.* Brussels : s.n., 29 March 2010. MEMO/10/107.

14. **DENHAM, ELIZABETH, ASSISTANT PRIVACY COMMISSIONER of CANADA.** *REPORT OF FINDINGS INTO THE COMPLAINT FILED BY THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST against FACEBOOK INC.* July 16, 2009.

15. **Carr, John.** Desiderata: Helping parents understand how their children use technology. *Desiderata .* [Online] Twenty Ten Blog at WordPress.com, 2011. [Cited: 3 February 2011.] http://johnc1912.wordpress.com/.

16. **M.A., Tim Horton.** Grooming Paranoia. *Healthy Choices.* [Online] 2008. [Cited: 2011.] http://www.healthychoices4dd.com/Grooming%20memo.pdf.

17. **Hazlett Lynch, Ph.D,.** What is Bullying? *ezinearticles.com.* [Online] ezinearticles.com, 29 March 2009. [Cited: 3 February 2011.] http://ezinearticles.com/?What-is-Bullying?&id=2111708.

18. Reputation, Wikipedia. *http://en.wikipedia.org/wiki/Reputation.* [Online]

19. Data Mining, Wikipedia. *http://en.wikipedia.org/wiki/Data_mining.* [Online]

20. **Twigg, J.** *The right to safety: some conceptual and practical issues.* 2003.

21. **COMMISSION STAFF WORKING DOCUMENT.** *EU YOUTH REPORT.* [http://www.google.co.uk/url?sa=t&source=web&cd=1&ved=0CBkQFjAA&url=http%3A%2F%2Fec.europa.eu%2Fyouth%2Fnews%2Fdoc%2Fnew_strategy%2Fyouth_report_final.pdf&rct=j&q=EU%20youth%20report%20%202009&ei=xrZKTf3hF8mdOuaZuQk&usg=AFQjCNF9OVJy8tYvOq_-WrHb2A3QEUyHgA] Brussesl : European Commission, April 2009. SEC(2009) 549 final.

22. Cyber-bullying Cases. *http://www.citmedialaw.org/subject-area/cyberbullying.* [Online]

23. The Megan Meier bullying case. *http://en.wikipedia.org/wiki/Suicide_of_Megan_Meier.* [Online]

24. Avira, professional virus and malware defence for Pocket PCs and smart phones. *http://www.avira.com/en/products/avira_mobile_products.html.* [Online]

25. *Challenges in mining social network data: processes, privacy, and paradoxes.* **Kleinberg, J. M.** s.l. : International Conference on Knowledge Discovery and Data Mining, 2007.

26. Security in twitter clients. *http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_est_twitter_clients_securityen.pdf.* [Online]

27. Writer Evan Ratliff Tried to Vanish: Here's What Happened. *http://www.wired.com/vanish/2009/11/ff_vanish2/1/.* [Online]

28. Wikileaks says it has half a million 9/11 pager messages. *http://www.wired.co.uk/news/archive/2009-11/25/wikileaks-says-it-has-half-a-million-911-pager-messages.aspx.* [Online]

29. Cloud Computing Risk Assessment. *European Network and Information Security Agency (ENISA).* [Online] ENISA, 20 November 2009. [Cited: 3 February 2011.] http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.

30. **Catteddu, Daniele.** Security and Resilience in Governmental Clouds . *European Network and Information Security Agency (ENISA).* [Online] ENISA, January 2011. [Cited: 2 February 2011.] http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds.

31. **Daskala, Barbara.** Flying 2.0 - Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology. *European Network and Information Security Agency (ENISA).* [Online] ENISA, 12 April 2010. [Cited: 3 February 2011.] http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology-2/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-t.

32. Court Rules Against Teacher in MySpace 'Drunken Pirate' Case. *http://voices.washingtonpost.com/securityfix/2008/12/court_rules_against_teacher_in.html.* [Online]

33. Google and the Search for the Future . *http://online.wsj.com/article/SB10001424052748704901104575423294099527212.html?KEYWORDS=schmidt.* [Online]

34. Google-boss sorgt sich um die gläserne Generation. *http://www.spiegel.de/wirtschaft/unternehmen/0,1518,712572,00.html.* [Online]

35. Mind Games, Washington Post. *http://www.washingtonpost.com/wp-dyn/content/article/2007/01/10/AR2007011001399_2.html.* [Online]

36. Sexueller Misbrauch von Kindern. *http://www.spiegel.de/kultur/tv/0,1518,724906,00.html.* [Online]

37. Psycho-Profile alarmieren Verbraucherschützer. *http://www.spiegel.de/wirtschaft/unternehmen/0,1518,727293,00.html.* [Online]

38. De Maizière will Datenschutz-Regeln verschärfen. *http://de.news.yahoo.com/2/20101201/tbs-de-maizi-re-will-datenschutz-regeln-f41e315.html.* [Online]

39. Bußgeld gegen Haspa verhängt. *http://www.datenschutz.de/news/detail/?nid=4633.* [Online]

40. European Commission recommendation on implementation of privacy and data protection principles in applications supported by radio-frequency identification. *http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf.* [Online]

41. European Commission, Internet of Things — An action plan for Europe. *http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf.* [Online]

42. ISO/IEC 27005:2008 Information technology-Security techniques-Information security risk management. *http://www.iso.org/iso/catalogue_detail?csnumber=42107.* [Online]

43. Clive Thompson on Remembering Not to Remember in an Age of Unlimited Memory. *http://www.wired.com/techbiz/people/magazine/17-08/st_thompson.* [Online]

44. KDnuggets home. *http://www.kdnuggets.com/software/.* [Online]

45. Guidelines for Policy Makers on Child Online Protection. *http://www.itu.int/cop.* [Online]

46. **Matt Richtel.** Growing Up Digital, Wired for Distraction . *New York Times.* [Online] New York Times, 21 November 2010. [Cited: 3 February 2011.] http://www.nytimes.com/2010/11/21/technology/21brain.html.

47. **Arthur, Charles.** TomTom satnav data used to set police speed traps. *guardian.co.uk.* [Online] The Guardian, 28 April 2011. [Cited: 07 June 2011.] http://www.guardian.co.uk/technology/2011/apr/28/tomtom-satnav-data-police-speed-traps.

ANNEX I ENISA EFR framework

The European Network and Information Security Agency (ENISA), has undertaken the development of a framework for the analysis and reporting of emerging and future risks in the area of information security. ENISA defines emerging risks as those that may have an impact between one and five years in the future; and future risks as those that may have an impact more than five years in the future.

6.1 The EFR Framework: concept and purpose

The EFR Framework is based around the use of predictive, narrative 'scenarios'. The concept behind scenario planning is essentially simple: it facilitates the telling of realistic stories about possible (or probable) future events, based on extrapolation from present trends.

In the EFR Framework , the use of scenarios, rather than any other form of analysis, is intended to ensure that the extrapolations are both realistic and can be understood and appreciated by the decision makers. When building the scenario, a single technology, or prospective use of that technology, is selected for consideration. This is then built into a unique scenario that describes a situation in the future in which that technology, or its functionality, has been deployed.

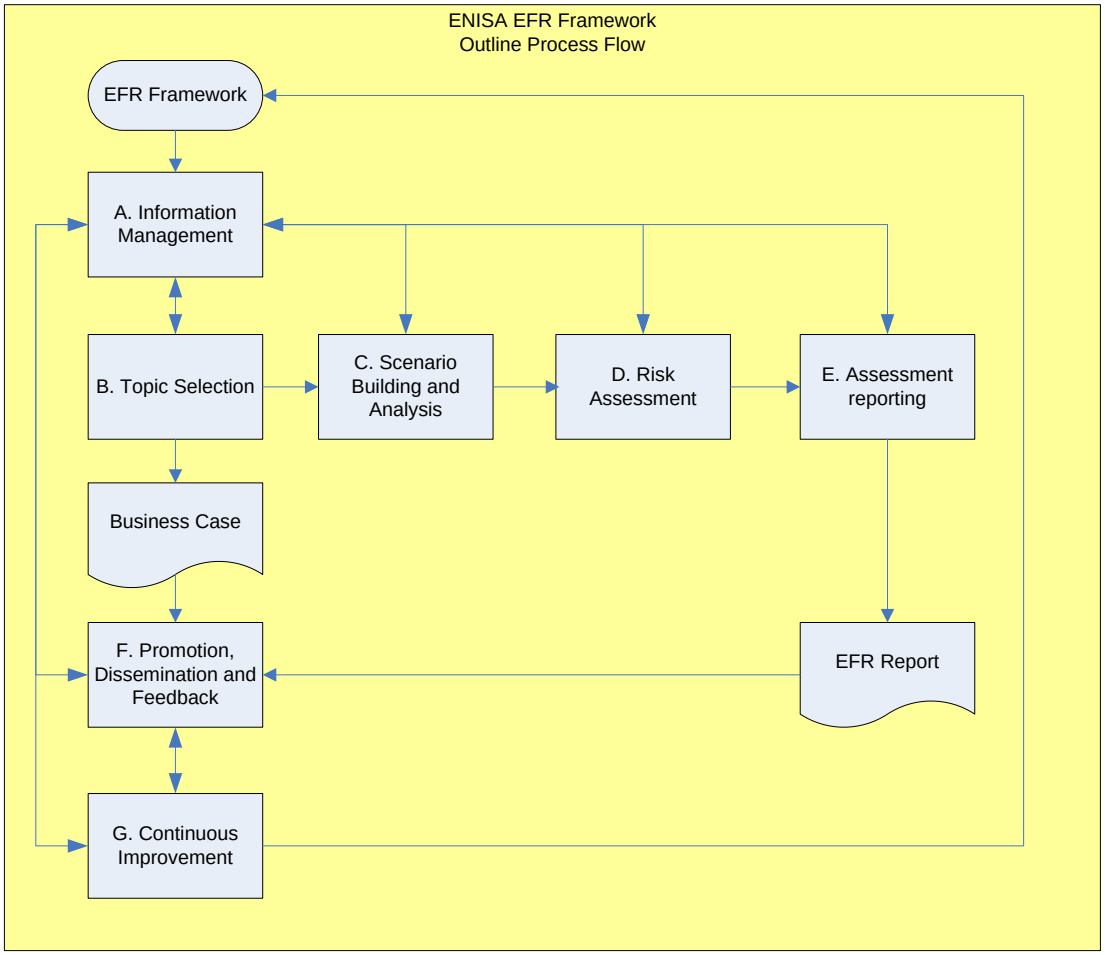
Once an area of EFR interest has been selected, a narrative story or 'scenario' is written. The concepts underlying the story are then subjected to a risk assessment process, more information on which is given in the next section. This looks at the technology and its use, as described in the narrative, in order to identify possible threats and vulnerabilities. From these, the assessment deduces the potential risk to the assets mentioned by the narrative.

The purpose of the ENISA EFR Framework is similar to that of classical scenario planning, in that it alerts those reading the report to possible future outcomes of current trends. However, the EFR Framework is both more narrowly targeted and more structured, in that it delivers a reasoned assessment of the risks inherent in the technology and its use.

EFR assessment reports should be read by appropriate target audiences in order to ensure that the risks (both positive and negative) inherent in a technology and its use are recognised and understood. If considered necessary and appropriate, comprehension of the risks will enable decision makers to take appropriate steps to manage and mitigate them, where possible.

At figure 1, below, is a simplified, outline flow diagram showing the processes of the EFR Framework. These are as follows:

A. Information management
B. Topic selection
C. Scenario building and analysis
D. Risk assessment
E. Assessment reporting
F. Promotion, dissemination and feed-back
G. Continuous improvement.



For more information on the EFR Framework, please refer to the *ENISA EFR Framework – Introductory Manual [EFRMan]*

6.2 Risk assessment methodology

The methodological approach used in this project to identify and assess emerging and future risks was based on the standard **ISO/ IEC 27005:2008 Information technology — Security techniques —Information Security Risk Management** (42) ↗→. In this endeavour, the ENISA team was supported by a group of external risk management specialists from Ernst & Young Greece.

The evaluation scales and metrics have been customised to fit the project's requirements.

The following major steps were performed in the process of assessing the emerging and future risks:

- Assets identification and valuation

- Vulnerabilities identification and assessment
- Threats identification and assessment
- Identification of existing/implemented controls
- Identification of final risks

6.2.1 Identification and valuation of assets

In this step, we identified the major assets to be protected in the scenario and estimated their value.

For the purposes of our analysis, asset identification was performed at the composite asset level, meaning that personal and other types of data were identified as part of a physical asset (e.g. a smart device, a health monitoring device, a database etc.) and not as a separate asset. As such, the estimation of the value of the physical asset considered also the value of the data that resides on this asset.

To estimate the asset value, we identified and considered the certain impact areas. Using a scale from 1 to 5 (Very low to Very high), we estimated the impact in each area for each asset. The final asset value was the maximum of these values.

6.2.2 Identification and assessment of vulnerabilities

The purpose of this stage was to identify and assess vulnerabilities of the assets. A 'vulnerability' refers to an aspect of a system/process (the assets) that can be exploited for purposes other than those originally intended, typically weaknesses, security holes, or implementation flaws within a system that are likely to be threatened. These vulnerabilities are independent of any particular threat instance or attack.

In the evaluation of the vulnerabilities, a scale from 1 to 5 (Very low to Very high) was used and the following attributes were considered:

- **Severity**: The severity of impact that will be incurred if the particular vulnerability is exploited. This includes the scope of the impact and the escalation potential (e.g. where the exploitation of the particular vulnerability would subsequently lead)
- **Exposure**: The ease of exploiting the particular vulnerability through physical or electronic means (required knowhow, required resources).

It should also be noted that the vulnerability value was assigned when related to a specific asset, since the same vulnerability had different value in different assets. The vulnerability assessment also considered possible existing/implemented controls identified or assumed in our scenario.

6.2.3 Identification and assessment of threats

This stage involved the identification and assessment of possible threats that could exploit the vulnerabilities of the assets identified. It should be noted that threats exist regardless of the vulnerabilities, and there are two major categories of threats to be considered: **man-made** and **natural** threats, namely threats due to humans (either accidentally or intentionally) and threats due to natural events (e.g. adverse weather conditions).

Using the same scale of 1 to 5 (very low to very high), the threats are evaluated, considering the following parameters, especially for man-made threats:

- **Capability**: The amount of information available to the threat agent (knowledge, training, technological sophistication etc.) and the availability of the required resources
- **Motivation**: The threat agent's perception of the attractiveness of the assets, danger of apprehension and, in general, motive to violate standards and procedures

Please note that the function of these two parameters provides the **likelihood** of this threat to occur.

6.2.4 Identification and assessment of implemented controls

As controls we identified measures for protection and effective operation of the assets such as: policies, procedures, organisational and technological manual or automated mechanisms. Controls can be categorised as:

- Preventive controls
- Detective controls
- Deterrent controls
- Corrective controls
- Containment and recovery controls

As our scenario is plausible, existing (implemented) controls have been identified in the form of assumptions in the scenario development.

The expert group considered existing controls in the evaluation of vulnerabilities and threats, the values of which have been decreased in some cases due to the existence of these controls.

6.2.5 Risk identification and assessment

In practice, after identifying and assessing the vulnerabilities for every asset, the group followed these steps:

- **Mapping threats to vulnerabilities**: In this step, the group identified possible threats that could exploit each vulnerability of each asset. It is the unique pairs of vulnerability and threat for a certain asset that produces a risk for this asset.

- **Risk value**: As mentioned above, the value of the risk is a function of the asset, vulnerability and threat values. The asset values, and the threat and vulnerability levels, relevant to each type of consequence, are matched in a matrix such as that shown below, to identify for each combination the relevant measure of risk on a scale of 1 to 13. The values are placed in the matrix in a structured manner.

6.2.6 Risk mitigation – identification of controls and recommendations

Following the identification and assessment of risks, the group ranked the risks from very high to very low. Therefore, as the next step, the group identified possible controls and safeguards that could reduce those risks. For the purposes of this analysis, the risk mitigation step has been limited to the recommendation of potential controls to mitigate the risks identified. For example, acceptance levels have not been identified, as is the case in a usual risk mitigation exercise.

ANNEX II – Vulnerabilities and Threats list

6.3 Vulnerabilities

This section presents the vulnerabilities identified by the expert group. Vulnerabilities become risks only when they are exploited by a threat (see next section).

V.1 Assigning extensive responsibility for security functions to end users

Involve some form of user intervention and control; users (with the best of intentions) sometimes make bad decisions, they also make bad decisions deliberately.

V.2 Weakness in operations of devices, systems and networks

Dependency on humans.

V.3 Dependency on power systems

Power systems/suppliers can usually guarantee availability during short power cuts.

V.4 Network failure (technical)

Normally very reliable, however technical defects/errors and errors in operation might happen (i.e. resilience).

V.5 Lack of back-up/failover and recovery procedures

The hardware is normally very reliable; however both professional and private users might lack continuity and recovery controls.

V.6 Insufficiently robust system design

Design of systems is such that failures can happen both at the level of single systems, as well as by means of cascaded failures due to system dependencies.

V.7 Lack of harmonisation of procedures (interfaces, information)

Procedures themselves are not always interoperable. Their technical implementation is often not interoperable. Gaps in procedures implementations (both organisational and technical) cause a lot of problems in service provisioning, protection and law enforcement.

V.8 Flawed/inadequate design (both at logical and technical levels), inappropriate/incomplete implementation

Omissions in functionality of social networking sites introduce weaknesses that can lead to

risks for the involved individuals. The ability of potential perpetrators to misrepresent themselves to Kristie appears to be an important weakness that put her at risk. Whilst acknowledging the practical difficulties it is still a fault that creates exposure to threats. For example, such a vulnerability may enable application developers to obtain inappropriate and unauthorised access to third party information e.g. of access to personal data of friends of individuals who use their applications (as in the decision of the Canadian Privacy Commissioner's adjudication on Facebook).

V.9 Lack of accountability of performed user actions

Used services and functions often do not provide support for accountability of performed user actions, even if data concerning those have been stored.

V.10 Extensive dependency on IT systems and networks

More and more vital functions for safety and security depend on IT systems and networks.

V.11 Insufficient capacity/resources (technical components)

Supported by the statement from Nemertes Research that has reported that by 2012 bandwidth demand would outstrip capacity, and that "bandwidth limitations will throttle back innovation, as users become increasingly frustrated with their ability to run sophisticated applications over primitive access infrastructure".

V.12 Insufficient/untrained personnel

Individuals who themselves are criminals or paedophiles being hired by the companies. Inadequate supervision of processes can contribute to this. Untrained personnel can lead to insufficient data protection procedures and misuse of data collection.

V.13 Highly complex procedures

Complex procedures can lead to users not fully implementing the highest standards of data protection.

V.14 Lack of interoperability between devices and/or technologies and/or systems

The transferability of profiles is a market, and perhaps in the foreseeable future also a legislative, requirement.

V.15 Unfriendly user interfaces and/or increased complexity or error proneness

Unfriendly user interfaces can lead to users not fully implementing the highest standards of

data protection. Very often the lack of transparency, accessibility, simplicity puts people off from reading or learning about different vulnerabilities or potential risks.

V.16 Changing security perimeter/chain of trust

Adding new security subjects in the security perimeter (human, technical components) brings additional exposure, as the security of new subjects is not always validated according to the existing security context of the perimeter.

V.17 Complex system design

Complex system design can lead to overly complex procedures for data privacy protection.

V.18 Insufficient protection/security measures

Insufficient protection and security measures can lead to exposure of personal data and misuse of data collection and data profiling tools. A failure to present the right information in the right way at the right time counts as a failure of this type.

V.19 Insufficient knowledge of procedures for using available functions, tools and technical components

Insufficient knowledge can lead to exposure of personal data and misuse of data collection and data profiling tools. Users may simply not know/be aware of the different procedures/policies that deal with protecting data.

V.20 Limited battery life

Unavailability of function may cause failures of protection mechanisms.

V.21 Access to location data by many actors

Users may not be aware that their GPS-equipped gadgets also transmit their exact location, which poses a great threat to the child. General location data, if available, are central in user profiling. E.g. the fact that Kristie discloses her location on her social networking site could be exploited in several ways, including by the people who later bullied her.

V.22 Electromagnetic interference

The open nature of wireless communications makes them susceptible to interference.

V.23 Radio jamming

The open nature of wireless communications makes them susceptible to radio jamming.

V.24 Exposure of user's personal information

Personal data can be inferred by analysing the socialising activity of a user, as well as by examining his/her network of friends and by inferring novel and unpublished information about the individual. The exposure of personal information, including the second 'secret' profile, contributed towards Kristie's predicament, e.g. one or more of the bullies knew that Kristie's parents were unaware of its existence. However, exposure does not necessarily confer the right to correlate; however this distinction is rarely made in practice.

V.25 Loss of assets

It is especially the case that mobile assets and the information they contain might be lost. This is particularly so for teenagers carrying gadgets to their environment (school, gym, socialising, etc.).

V.26 Lack of or low awareness/training in security, usage and management/maintenance issues

Lack of or low awareness/training can lead to exposure of personal data and misuse of data collection and data profiling tools. In professional environments in particular, a lack of direction/guidance by senior management on developing staff awareness is commonplace.

V.27 Devices and equipment used in unprotected/outdoor environments

The use of mobile devices in unprotected environments (see V48) exposes them to threats related to loss, eavesdropping, spoofing, etc. Mainly this is due to the change in the security context/environment (see V55).

V.28 Weak links are part of the chain of trust or are responsible for critical security functions

To date the issue of minor data protection rights has not attracted much legal theory or interest – this is considered as an extremely interesting field for further research. This is effectively the whole point of the story. If Kristie had behaved differently the scenario would not have arisen.

V.29 Devices communicate over unprotected or publicly accessible channels

This can lead to exposure of personal data and misuse of data collection and data profiling

tools.

V.30 Lack of or inadequate identification and authentication controls

This can lead to exposure of personal data and misuse of data collection and data profiling tools. On the other hand, it has to be assumed that if Kristie had known more about Jeffrey from the very beginning she would have avoided becoming entangled with him. This is not absolutely guaranteed, by any means.

V.31 Lack of or inadequate logical access control

Information concerning individuals is stored on devices that lack logical access control and as such are subject to mining activities.

V.32 Unmanaged IT Equipment: susceptible to OS and application vulnerabilities, susceptible to malware, susceptible to firmware substitution allowing backdoors and key loggers, covert channels etc.

Malware installed on mobile devices via Bluetooth, mms or email could install a Trojan horse and subsequently divulge all data stored in the mobile device.

V.33 Unencrypted/unprotected data storage

This can lead to exposure of personal data and misuse of data collection and data profiling tools.

V.34 Multiple actors have access to data (parent, classmate, friend, providers, etc.)

Social network sites are meant to be 'social' so, inevitably, they involve multiple actors accessing the same data. That is not really the issue although, obviously, the more there are the greater the risk that a bogus actor will find their way into the friendship or social circle. Especially within small social groups (e.g. families, classes, friends), multiple access to the same data might be misused.

V.35 Wireless networks' inherent security weaknesses (susceptible to interceptions, insufficient security controls/protocols)

This can lead to exposure of personal data and misuse of data collection and data profiling tools. An attacker might use this vulnerability to install a Trojan or any other kind of malware to help him locate Kristie, or to enable him to target her.

V.36 Lack of common legislation/interpretation of laws worldwide (and in some cases in transposition/enforcement of law in EU Member States).

Lack of standardised legislation can lead to deficiencies for law enforcement actions across country borders in the case of international internet crime. Many of the companies providing relevant services are based outside of the EU in any case, principally in the USA.

V.37 Lack of informed consent in the technical environment

The principle of informed consent is not applied in technical systems, thus leading to situations where users cannot and do not provide their consent for storage/processing of their data (e.g. because they are hidden EDO).

V.38 Informed consent statement that the user has to agree is too intrusive and inappropriate

Consent for data collection by online service providers needs to be transparent and fully understandable by users, online service providers need to provide different levels of data use consent, such as:

– Data collection only for operations, such as collection of address data to be able to send goods

- Data collection for marketing purposes

- Data collection for analysis purposes. Users usually do not read them anyway, because they are too complex and often inaccessible

V.39 Lack of data traceability and transparency. The user cannot be aware when his or her data were accessed, by whom and why

If users don't know who might be tracking or following their data it can be very hard to know what best to do to keep them safe.

V.40 Different levels of security/regulations in different countries

Social networks usually reside in countries (i.e. USA) with no (or not strong) data protection laws. What is considered 'confidential' and the resulting security policies may differ substantially in different jurisdictions. Although steps for international cooperation among security agencies have been taken, a lot remains to be done in this field.

V.41 Huge amounts of data (personal, behavioural) collected and stored in databases

As users create public profiles and publish public data in social networking sites, this information is persistent. But this should not pose a great threat as it concerns public data. Other data, however, that are pertinent to the security of the access, need to be protected accordingly.

Furthermore, users should always be able to control the storage of data or get sufficient information about the location of storage (i.e. legislation domains).

Big collections of data enhance the motivation for potential attacks, as the benefit of a successful attack will be huge.

V.42 Data easily accessible and linked/connected

Temporary data stemming from user actions are easily accessible and linkable to individuals. Equally, data from social networking, blogs, etc. can be assigned to physical persons.

V.43 Insufficient interpretation of legal requirements in technical implementation (low compliance)

Legal compliance is not always a primary objective of developed software/services. On the other hand, legal shortcomings of existing services appear long after deployment.

Telecommunication infrastructure is often subject to legal compliance and is therefore less relevant for this vulnerability.

V.44 Inappropriate/inadequate identity management

Identity management is still a weak point of user interaction with systems and services. Poor identity management opens doors to attacks and misuse.

V.45 Insufficient protection against misuse of accounting and logging information

In technical devices, misuse of accounting and logging information is feasible with some technical skills. It is likely that teenagers might find means to manipulate this kind of information in devices they are using.

V.46 Lack or inadequate authorisation for accessing data

Even if the access to data is being controlled properly, by using malicious software (e.g. installed in a PC or a mobile phone) disclosure of personal data is feasible. However, devices may have ill-defined access rights.

V.47 Inadequate network access control

Network access control is often an issue that is neglected, even in professional networks. In the area of private networks (e.g. home networks) it is likely that network access control mechanisms (e.g. wireless networks) are not properly used.

V.48 Easy to lose devices, equipment used in unprotected environment

Mobile devices are easily to lose, especially if used by teenagers who might be temporarily distracted when using them in crowded locations (schools, buses, trains).

Private or professional equipment might be located in unprotected environments.

V.49 Easy to copy/forge

Technical and organisational vulnerabilities for used (storage or transmission) devices and software allow easy copying and forging of information, identities, technical data, etc. (i.e. device-ID-masquerade, DNS poisoning, etc.).

V.50 Lack of respect for data minimisation and proportionality principles

The principles of data minimisation and proportionality are not the main concern during development and operation of services. Combined with the low cost of storage, application systems tend to store much more data than needed. Pure maintenance (e.g. retention of unused data) aggravates the problem (see also (43) ↗ →).

V.51 Insufficient definition of the purpose of data collection

Often, for deployed services and applications, there is no clear justification for the purpose of the collection of data. Combined with the low cost of storage, application systems tend to store much more data than needed. Pure maintenance (e.g. retention of unused data) aggravates the problem.

V.52 Insufficient /incomplete collected data, lack of adequate correction controls at data entry

Mistakes made during data entry are not discovered due to absence of corresponding controls. In combination with V50 and V51, this might have negative consequences for the involved individuals, as they will not be able to detect and correct data once entered.

V.53 Low manageability of collected data from data owner

Existing services often do not foresee sufficient management functions for user data.

Furthermore, user data are collected, often replicated and redundantly stored. This reduces manageability of this information by its owner (see also V50, V51 and V52 above).

V.54 Reliability of used devices/equipment (software, hardware)

Due to complexity, quality and dependencies, used components have varying reliability. Technical defects and failures might cause serious disadvantages for users, especially in cases where these devices serve protection and/or control purposes.

V.55 Changed security context by moving components to another environment

Due to their mobility, involved gadgets can easily be moved between environments (physical and logical) with varying level of security. This is often a reason for security breaches, as assets of high value might be transferred to an environment with low security protection measures and become vulnerable.

V.56 Tendency for individuals to hide information

Teenagers tend to develop activities that they keep secret from those with parental control. This is an attitude that can lead to serious problems as far as their general security is concerned, particularly in the context of the bullying and grooming scenario.

V.57 Weak/ineffective parental control

Parental control may be ineffective due to restrictions stemming from the social environment of the family (e.g. low level of education and care, reduced availability of parents, isolation of individuals within a family, etc.). Weak parental control can lead to serious problems as far as their general security is concerned, particularly in the context of the bullying and grooming scenario.

6.4 Threats

T.1 Inappropriate/illegal use of data mining and profiling tools

Illegal use is very likely to happen, especially by threat agents with significant capabilities (i.e. the attacker would be likely to access a site such as (44) ↗ → to download the appropriate software mentioned in the scenario.

T.2 Inappropriate use of collected data (both personal data and inferred data - secondary use of data).

Following the illegal use of collection tools, data will be likely to be used with similar malicious

intentions.

T.3 Large-scale and/or inappropriate data mining and/or surveillance and/or profiling

Numerous actors in ICT service provisioning gather large amounts of data, building user profiles and using these data to make profit. In many cases, this data collection is legal, as it happens via interpretations of existing laws (e.g. Telco regulation) or is illegal, as there is no consent from the data owner.

T.4 Insecure/incomplete deletion of data (from social network profile, provider's database, cloud computing-based providers, etc)

Data are stored on devices that can persist deletion actions from users. Even when flowing, or when virtualised, data are often replicated and temporarily stored. In these cases, users might be unable to delete all data replicas.

T.5 Inappropriate/illegal location based services

It is feasible to install and set up illegal (free) services that are based on wireless communications, in order to attract users.

T.6 Loss of trust (in the parents, friends, etc)

Misuse from the social environment is likely, especially in cases of abuse/hostility. On the other hand, parents over monitoring their children are almost forced to be discreet and secretive about their activities.

T.7 Unfair, inappropriate social networks/services providers' ToU - terms of use do not adequately consider the interests of the user (e.g. barriers when removing information or deleting a profile, closing an account, etc.)

Terms of use are often unclear and, even in cases that follow relevant legislation, they leave space for misuse/misinterpretation. Users need to be aware when they publish information of the possible consequences of misuse. On the other hand, companies are beginning to improve their practices, although there will always be rogues.

T.8 Trust misplaced

It is possible to develop trust relationships with human actors that under normal circumstances would not be trusted. For teenagers, this might happen in cases of difficulties within a social environment. To a certain extent, this can happen with regard to technical

components/service providers (e.g. phishing, Trojan horses, etc.).

T.9 Accidental information broadcasting

Threat might be materialised when using various services, such as publishing personal information on social networking sites, or including it in emails and chat messages while using insecure wireless network connections for both laptop and mobile devices.

T.10 Excessive personal information sharing

Users tend to put information online about themselves that facilitates the building of personal profiles. Government statistics have identified that 47% of bullying now involves the use of electronic media. Teenagers in particular tend to expose personal details to various user groups without prior consideration of the negative consequences of this action. Personal details such as schools, classmates etc. can be used as introductions to try and build inappropriate relationships.

T.11 Discrimination – data (including that which is legally classified as anonymous) may still be used to discriminate against individuals (for example, extracting psychological profiles from click-stream data.)

By using various behavioural, social and other criteria, user profiles can be generated that can be misused to discriminate against users/user groups that meet these criteria.

T.12 Misinterpretation of data by the police

Evidence generated by online activities might be difficult to interpret due to extensive segmentation of data and absence of trails. Furthermore, malicious individuals might misuse this fact and generate false evidence to accuse innocents.

T.13 State surveillance on citizens

State surveillance is an issue that is practised by governments around the globe with various motives (e.g. prevention, censorship, unfounded suspicion, etc.).

T.14 Social engineering attack

Social engineering attacks are likely to happen to bully, harass or abuse an individual. This happen quite often within teenage groups. The flavour of on-line social engineering attacks taking the form of phishing and other methods is quite frequent, even today. Another form is Trojan programs. The end-user is led to believe that the software he/she is downloading, or the form used for providing user name and password is legitimate. This threat and abused

vulnerabilities are based on humans willingly relinquishing control to a false entity.

T.15 Identity theft

Identity theft is a threat that is very likely to be materialised, especially when devices and network traffic are not appropriately secured.

T.16 Eavesdropping (breach of confidentiality and/or integrity)

Eavesdropping is likely to succeed, especially if mobile devices are part of the scenario and users are involved who can be easily distracted (i.e. teenagers).

T.17 Traffic analysis/ scan/probe

By use of proper, quite easily obtained, tools, user interaction can be analysed/scanned, mainly at the level of the network. This is particularly easy for devices operated in low security environments.

T.18 Modifying network traffic

Modification of network traffic requires some extensive skills and capabilities. This threat can be materialised by attackers investing quite high criminal effort.

T.19 Device theft

Theft of (mobile) equipment is one of the most common threats that can be materialised, especially for the user group in question (teenagers in crowded places).

T.20 Loss or misuse of devices

Loss of (mobile) equipment is one of the most common threats that can be materialised, especially for the user group in question (teenagers in crowded places).

T.21 Worms, viruses and malicious code

Infection/manipulation of devices is a major threat that will be materialised the more networked the systems are. Likely to happen when mobile devices (i.e. not managed) are part of the network.

T.22 Compromise of authentication process (theft of credentials, password crack, spoofing of credentials, bypass authentication, phishing, etc)

With some criminal effort, this threat can be materialised, especially for the teenage user

group that is receptive with regard to manipulative actions (e.g. phishing, grooming).

T.23 Man in the middle attack

The materialisation of a man in the middle attack requires significant technical skills and capabilities. It is a threat that is usually initiated by professional threat agents.

T.24 Side channel attack

The materialisation of a side channel attack requires significant technical skills and capabilities. It is a threat that is usually initiated by professional threat agents.

T.25 Blocking attack

The materialisation of a blocking attack requires significant technical skills and capabilities. It is a threat that is usually initiated by professional threat agents.

T.26 Jamming

The materialisation of a jamming attack requires technical skills and capabilities. It is a threat that is usually initiated by professional threat agents.

T.27 Denial of service attack/flood/buffer overflow

Denial of service attacks can be materialised with some IT knowledge and considerable skills and capabilities. In the context of the scenario, threat agents with significant motivation might be the source of such an attack.

T.28 Unauthorised access to/deletion/modification of devices/data etc.

Given the weaknesses of used devices (especially mobile), it is feasible to obtain unauthorised access/modify device settings and stored data.

T.29 Malicious insider (social network/online shop/online service provider/person from narrow social environment)

Malicious insiders are common threat agents that can effectively pose a threat, especially in the context of the scenario.

T.30 Human error (e.g. software and hardware misconfiguration, online service provider administrator error, etc.)

Given the complexity of devices, systems and software, as well as the level of involved users,

the possibility for human error is rather high.

T.31 Backups stolen

The probability for this threat to materialise is rather low, as threat agents need to get access to backup files. Given the target group of this scenario (i.e. teenagers in crowded places) this might happen to some extent for some of the data that are stored in mobile storage media (e.g. USB sticks, cameras, mp3 players, etc.).

T.32 Loss or compromise of operational logs

Manipulation of logs requires some expertise and, for threat agents outside the family members, significant capabilities. Thus, the probability of materialisation of this threat is considered as rather low.

T.33 Loss or compromise of security logs (manipulation of forensic investigation)

Manipulation of security logs requires expertise and, for threat agents outside the family members, significant capabilities. Thus, the probability of materialisation of this threat is considered as rather low.

T. 34 Malfunctioning/breakdown of systems/devices/equipment

Due to systems complexity, malfunctioning can occur.

T.35 Network breaks

Network unavailability is considered as a threat with low probability to be materialised. In the case of malicious breaks, threat agents need sufficient capabilities (except for incidents in the near social environment that are easier to materialise).

T.36 Traffic Loss

To materialise this threat, sufficient capabilities are required. The probability for this threat to materialise is considered as low.

.

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu