Children Protection Online: Uneasy Steps towards a Balance between Risks and Freedoms

Federica Casarosa[*]

I. The web grows "younger"

Nowadays the Internet has become a digital universe accessible within the comfort of one's household. Although it was originally created as a means of communication in the scientific community, [1] it has developed into an extraordinary diffused medium used in homes, offices, schools, businesses and public administrations.

Moreover, Internet penetration and use of new technologies is still growing considerably in the European Community. This situation is not only due to qualitative improvements of technologies, but it is also related to the wider access of youngsters to this medium. As a matter of fact, a recent survey of the Eurobarometer provided evidence about the rising share of Internet usage by children up to 16 years, (for instance, in European countries, the percentage of children using Internet has reached the rate of 51% in 2006, while the first contact with new technologies lowers down to 6-8 years old). [2]

As a matter of fact, children and young people are more and more often the first to take up and use new technologies; yet, they are not always aware of both risks and ways of dealing with them, or, whether they are, they are not always mature enough to evaluate the situations that they encounter and the possible consequences their decisions can have.

At the end of the day, new technologies can improve the quality of life for children and young people, providing them better access to knowledge and widest possibilities to socialise and experiment social skills. But, at the same time, such resources could also lead minors to decide on issues that normally they would not have to decide in real life, in particular concerning their own safety.

---

[*] Research Fellow, Università di Trento (I)

[1] In reality, the first usage was a default communication network among military service nodes in the whole United States, and then the technical structure was devoted to the connection of Universities.

[2] See the **OPTEM REPORT**, *Safer Internet for Children – Qualitative Study*, May 2007, requested by the DG Information society and Media, where the rate of less than 6 years-old children using the Internet is 9%, and from 6-7 years jumps up to 34% (growing further as age increases).

Recent studies shows that new risk situations arise for children with the further diffusion of new Internet enabled end-user devices, like "3G" mobile phones and new practices such as social networking[3] (where chatting includes also the possibility to use web-cams), Internet blogging[4] or file sharing.[5] Moreover, possible future technological developments and user options can increase this risky environment, also through convergent services and new modes of communication. This increase in connectivity by children will see a corresponding increase in benefits for them, but also in risks of "collateral damage". Dangers, especially for children, and abuse of the technologies continue to exist and new threats and abuses are emerging.

This paper will address, in part II, European interventions concerning children protection online distinguishing the main objectives of such interventions and the preferred tools to achieve an acceptable level of protection; part III will be then devoted to the identification of potential risks for children online, while part IV will analyse the advantages and disadvantages of the tools proposed by European institutions. In part V, a case study will be proposed, concerning social networking, in order to verify if technical and legal tools can be effective in practice. Finally, preliminary conclusions will be presented.

II. EU intervention

The European Union has been a forerunner in tackling children protection issues: the first steps date back to 1996, when the Green Paper on the protection of minors and human dignity in informational and audiovisual services was published.[6] It presented a three-part analysis about the existing background concerning the fight against the dissemination of content offensive to human dignity, and the protection of minors against exposure to content that is harmful to their

[3] A social network service focuses on building online communities of people who share interests and activities, or who are interested in exploring the interests and activities of others. Most social network services are web based and provide a variety of ways for users to interact, such as e-mail and instant messaging services. The main types of social networking services are those which contain directories of some categories (such as former classmates), means to connect with friends (usually with self-description pages), and recommender systems linked to trust.

[4] A blog (a contraction of the term "Web log") is a Web site, usually maintained by an individual, with regular entries of commentary, descriptions of events, or other material such as graphics or video. Many blogs provide commentary or news on a particular subject; others function as more personal online diaries. A typical blog combines text, images, and links to other blogs, Web pages, and other media related to its topic. Most blogs are primarily textual, although some focus on art, photographs, sketches, videos, music, audio, which are part of a wider network of social media.

[5] File sharing refers to the providing and receiving of digital files over a network, usually following the peer-to-peer (P2P) model, where the files are stored on and served by personal computers of the users. Most people who engage in file sharing on the Internet both provide (upload) files and receive files (download).

[6] 16 October 1996, COM (96) 483.

development. Firstly, it described the evolution of audiovisual and information services from a centralised mass media model to a decentralised and individual communication model. Secondly, it analyses the current legislation and policies at national, European and international level, and finally, it pushed forward some guidelines to provide a more flexible regulatory framework capable to face the characteristics of new services.

In particular, the Green Paper stressed the fact that: "*The full potential of such developments* [i.e. audiovisual and informational services] *will depend on society as a whole striking the right balance between freedom of speech and public interest considerations, between policies designed to foster the emergence of new services and the need to ensure that the opportunities they create are not abused by the few at the expense of the many*".

At the same time, the Commission published a Communication on Illegal and Harmful Content on the Internet, [7] which provided short-term measures required to deal with specific Internet related issues that go beyond the field of protection of minors and human dignity. In particular, it defined the difference between illegal and harmful content. The former may be banned for everyone, regardless of the age of the potential audience or the medium used (e.g. child pornography, extreme gratuitous violence and incitement to racial or other hatred, discrimination, and violence). The latter, on the contrary, can be defined as "*content that is legal, but liable to harm minors by impairing their physical and mental development*",[8] thus, access to it can be allowed only for adults.[9] The key difference between harmful and illegal content is that the former is subject to personal choice, "*based on one's beliefs, preferences and social and cultural traditions*",[10] while the latter is a matter of state choice. This distinction is essential not to confuse the different objectives and different problems which each of them raises, and consequently the different solutions chosen in each case. With regard to illegal content, the state decides which content should be considered illegal and what consequences should be linked to this classification (for instance, prohibition of publication and distribution). [11] When tackling with

[7] Communication on illegal and harmful content on the Internet, COM(96) 487
[8] Ibidem, par. 17.
[9] Later, the Safer Internet Action Plan added to this taxonomy also unwanted material, like spam or undesired commercial communications. See *infra* in the Safer Internet Action Plan Plus.
[10] **J.P. MIFSUD BONNICI** and **C.N.J., DE VEY MESTDAGH**, 'Right vision, wrong expectations: the European Union and self-regulation of harmful Internet content', *Information & Communications Technology Law*, Vol. 14, No. 2, 2005, 142.
[11] As far as *illegal content* is concerned, the point of departure is that what is illegal offline is illegal online. It should be ensured that the law is adapted so that it reflects the values of society and deals with new social phenomena. A further area of concern is the degree to which national law can be applied to activities taking place on a global

harmful content, on the other hand, it is argued that the state should create an environment that enables citizens to decide for themselves (and eventually for their children) which content they consider suitable and worth accessing. Moreover, the recommendation underlined that, in this case, a balance must be struck between possible harm to minors and the preservation of the freedom of expression.

These two measures set the ground for the following community interventions that leaded to the current regulatory framework.

The following phase was the adoption of the Council Recommendation 98/560/EC, of 24th September 1998,[12] on the development of competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity, which defined the guidelines for the national legislation on this issue.[13] In particular, it fostered a European and international cooperation, and it encouraged a more systematic coordination between government, industries, the other parties concerned in each Member State in order to enable minors to make responsible use of online audiovisual and information services, by improving the level of awareness among parents, educators, and teachers about the potential of the new services.[14]

In 1999, the aforementioned Recommendation was integrated by the first active intervention in the field: the implementation of a 'Safer Internet Action Plan' (IAP), which identified areas for concrete measures where Community resources should be focused on.[15] The

---

network, whether under application of national rules of conflict of law or in practice. This is difficult if acts are punishable in one country and not punishable in another.

[12] Council Recommendation 98/560/EC of 24 September 1998, OJ L 270, 7.10.1998, p. 48.

[13] It is useful to note that the legal base of this recommendation was Article 130 of the EC Treaty, (actual Article 157 ECT), which requires the Community and the Member States to ensure that the conditions necessary for the competitiveness of the Community's industry exist, with action aimed, *inter alia*, at fostering better exploitation of the industrial potential of policies of innovation, research and technological development. Differently, the following interventions are based on Article 153(2) ECT, on protection of the consumer, since they are focus on the end-user – particularly parents, educators and children – and are intended to promote their safety when using the Internet and new online technologies.

[14] The recommendation was updated in 2006, (*Recommendation on the protection of minors and human dignity and on the right of reply*, 2006/952/EC) following the same objectives. One important difference, however, is the limited role given to self-regulation as a tool to provide effective protection, downgrading it to an additional measure that, alone, cannot be sufficient to protect minors from messages with harmful content; whereas, in the previous recommendation, the role of self-regulation was much more emphasised, also providing the principles on which a self-regulatory intervention should be based (involvement of all interested parties, definition of the objectives in the codes of conduct, cooperation at community level, and regular evaluation of the measures taken.

[15] **European Parliament** and **European Council**, *Decision 276/1999/EC of 25 January 1999 adopting a Multi-annual Community Action Plan on promoting safer use of the Internet and new online technologies by combating*

Action Plan defined four specific objectives: the creation of a safer environment (through a network of hot-lines, and the adoption of codes of conduct), the development of a filtering and rating system, the encouragement of awareness-raising actions, and other supporting action (like the assessment of legal implications and the coordination with other similar international initiatives).

After the positive outcome of this four-year plan, [16] the Commission proposed a new mandate for an extended Safer Internet Action Plan (so called IAP-Plus),[17] and the Council of Ministers has recently adopted the new Safer Internet Programme proposed by the Commission for 2009-2013.[18] This new Action plan is designed "*to be able to take into account currently unknown future developments in the online environment as the resulting threats will become increasingly important in the years ahead*". The actions include again the promotion of a safer online environment and the public-awareness raising action, but these are framed to encompass a better 'user-empowerment' not only for parents and carers but also for children and young people, and to stimulate stakeholders to take responsibility, cooperate and exchange experiences and best practices at European and international level. Moreover, the Action plan acknowledges the need to create and build up an adequate knowledge base for addressing both existing and emerging uses, risks and consequences, and mapping both quantitative and qualitative aspects in this context; thus, it propose the setting of a coordinated investigation activity that will be used immediately in the implementation of the programme, as well as into designing adequate actions for ensuring online safety for all users.

---

illegal and harmful content primarily in the area of the protection of children and minors (OJ L 33, 6.2.1999, p.1) as amended by Decision 1151/2003/EC of the European Parliament and of the Council of 16 June 2003 (OJ L 162, 1.7.2003, p. 1).

[16] See the **European Commission**, *Communication to the Council, the European parliament, the European economic and social committee and the Committee of the regions concerning the evaluation of the multi-annual community action plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors*, COM(2003) 653 final.

[17] **European Parliament** and **European Council**, *Decision 854/2005/EC of 11 May 2005 establishing a multi-annual community programme on promoting safer use of the internet and new online technologies*, (OJ L 149 11.6.2005, p.1).

[18] **European Parliament** and **European Council**, *Proposal for a Decision establishing a multi-annual Community programme on protecting children using the Internet and communicating technologies*, COM(2008) 106 final, 27 February 2008, approved by the Council f Ministers on the 9th December 2008, available at http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1899&format=HTML&aged=0&language=EN&guiLanguage=en

All the European interventions in this field have a non-binding character, moreover, they all support the development and the implementation of technical tools[19] and, among legal tools, they recommends mainly self-regulation as the best regulatory solution. This option is not only due to the fact that technical tools and self-regulation can have a higher level of flexibility and can be better fit with the needs of an ever-changing environment, but also to the general argument – clearly stated in IAPs decisions – that "[r]*eaching international agreement on legally binding rules is desirable but will be a challenge to achieve and, even then, will not be achieved rapidly. Even if such agreement is reached, it will not be enough in itself to ensure implementation of the rules or to ensure protection of those at risk*".[20]

III. The existing risks for children

Having described the current legal framework at European level, it is now necessary to provide the existing threats that children face during online surfing. This will help the analysis concerning the effectiveness of the technical and self-regulatory tools proposed by European and national actors.

A. Child abuse material

In this category are included the cases in which children are harmed directly, as victims of sexual abuse documented through photographs, films or audio files and then transmitted online. In general child pornography refers to material depicting children being in a state of undress, engaged in erotic poses or sexual activity. Child sexual abuse occurs in the production of child pornography when sexual acts are photographed, and the effects of the abuse on the child (and continuing into maturity) are compounded by the wide distribution and lasting availability of the photographs of the abuse. For practical reasons, legal definitions of child pornography generally refer to a wider age range, including any pornography involving a minor, according to jurisdiction.

[19] See infra par. IV.

[20] Proposal for a Decision establishing a multi-annual Community programme on protecting children using the Internet and communicating technologies, cit., whereas (5). Previously also in Decision 854/2005/EC, whereas (6), cit.

B. Child grooming

In this category are included the cases in which children are contacted by people who will befriend them in order to commit sexual abuse. Thus, the act of grooming a child sexually may include activities that are legal in and of themselves, but later lead to sexual contact. Typically, this is done to gain the child's trust as well as the trust of those responsible for the child's well-being. Sexual grooming of children also occurs on the Internet. Some abusers will pose as children online and make arrangements to meet with them in person.

C. Cyber-bullying

In this category are included the cases in which children are victims of bullying in the online environment.[21] Cyber-bullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others. This can occur not only through text message but also through videos being uploaded on open video-sharing website (e.g. YouTube),[22] having an even more distressing effect, because the bullying in online environment has a potentially enormous audience, extending the humiliation and embarrassment of the victim.[23]

D. Unlawful privacy invasion

In this category are included the cases in which children are asked to disclose personal information that can be used to profile them and send them commercial advertising. In this case, the risk is not merely the collection of personal information from children without their, or their parent's, consent.[24] Rather, in wider perspective, the risk involves "*the opening up of the child's*

[21] Despite this definition, the phenomenon is not limited to children, though is more commonly referred to as cyberstalking or cyber-harassment when perpetrated by adults toward adults. Cyber-bullying can be as simple as continuing to send e-mail to someone who has said they want no further contact with the sender, but it may also include threats, sexual remarks, pejorative labels (i.e., hate speech), ganging up on victims by making them the subject of ridicule in forums, and posting false statements gossip as fact aimed at humiliation.

[22] Cyber-bullies may disclose victims' personal data (e.g. real name, address, or workplace/schools) at websites or forums, or may pose as the identity of a victim for the purpose of publishing material in their name that defames or ridicules them.

[23] **Home Office Task Force on Child Protection on the Internet**, *Good Practice Guidance for the Providers of Social Networking and User Interactive Services 2008*, available at http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance?view=Binary, p. 17.

[24] Privacy concerns exist wherever personally identifiable information is collected and stored - in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. Data privacy issues can arise in response to information from a wide range of sources, such as: healthcare records, criminal justice investigations and proceedings, financial institutions and transactions, biological traits, such as genetic material,

private world to the eye of the marketer, who not only watches the child but reconstructs the child's environment in order to manipulate the child's sense of self and security".[25] The possibility to obtain details of children's online behaviour can provide a continuous feedback to marketers, who not only can select easily which product sale to individual children, but also can fine tune with child's online social environment to make the child more vulnerable to advertising messages. This kind of marketing raises serious questions as it constitutes an invasion of privacy because enterprises penetrate child's private space and extracts data for instrumental purposes by manipulating also their online environment.

IV. Technical and legal tools proposed by the EU

Now, we turn to the technical and legal tools proposed and implemented through the Safer Internet Action Plans, in order to analyse which are their advantages and disadvantages.

Hotline networks: hotlines are contact points where end-users can report illegal content on the Internet. All hotlines are intended to work together with police, law enforcement and awareness nodes as well as with Internet Service Providers, industry organisations and other institutions. Under the Safer Internet Action Plan a widespread system of hotlines all over Europe had been developed, coordinated by INHOPE, the International Association of Internet Hotlines.[26]

Advantages	- Better knowledge concerning the rate of illegal content available online. - Cooperation though-out Europe in order to identify child-porn rings. - Centralised reaction in case of multiple jurisdiction issues
Disadvantages	- Difficult cooperation between hotlines and other stakeholders, in particular with police and law enforcement, (effectiveness of procedures in still low). - Lack of feedback from law enforcement authorities in order to improve the process. - Low awareness of the existence of hotlines from end-users.

residence and geographic records, ethnicity. The challenge in data privacy is to share data while protecting personally identifiable information.

[25] **V. STEEVES**, "It's Not Child's Play: The Online Invasion of Children's Privacy", *University of Ottawa law & technology journal*, 2006, 169-188, p. 186.

[26] See the website: www.inhope.org .

Rating and filtering schemes: a rating system is a technological device that can help the user to identify in advance which are the contents of the website to be visited, usually the rating system describes the content in accordance with a generally recognised scheme (for instance, where items such as sex or violence are rated on a scale) and then filtering systems can empower the user to select the content he/she wishes to receive. Ratings may be attached by the content provider or provided by a third-party rating service. There are a number of possible filtering and rating systems.[27]

Advantages	- possibility to filter in advance the content to be viewed by user - flexible tool (e.g. to be adapted to different aged children)
Disadvantages	- Low level of sophistication. - Difficult to achieve a critical mass need to provide accountable results. - Difficult to identify the appropriate labels in order to avoid that innocuous content will be blocked.

Age verification tools: obviously this kind of tool aims at ascertaining in advance the age of online user so as to keep older people away from youngsters, or vice-versa, keep young people away from website designed for adults. To accomplish either of those objectives, such tools must be able to effectively verify everyone's age by consulting reliable records about those looking to create an account on a social networking site. However, if the age verification is posed on adult's identity the proofs can be obtained from many sources,[28] while in case of children proving their age becomes more complicated, as only few can provide a similar set of proofs. Moreover, age verification can provide only a limited security effect, i.e. distinguish who can access or not to a specific website on the basis of its age; whereas no control at all is to be done on the records of the person accepted (e.g. existence of previous sex related crimes, etc.), thus, providing a false perception of security either to parents and to children.[29]

[27] See for instance the Platform for Internet Content Selection (PICS), which is a specification created by World Wide Web Consortium that uses metadata to label webpages to help parents and teachers control what children and students can access on the Internet. See more deeply at: http://www.w3.org/PICS/

[28] See that when government officials or even business seek to verify someone's identify or age, they can rely on birth certificates, Social Security numbers, driver's licenses, military records, home mortgages, car loans, other credit records, or credit cards.

[29] **A. THIERER**, "Social Networking and Age Verification: Many Hard Questions; No Easy Solutions", *Progress & Freedom Foundation Progress on Point* 14.6, 2007, available at www.pff.org/issues-pubs/pops/pop14.5ageverification.pdf

Advantages	- limitation of access to adults in children websites and vice-versa
Disadvantages	- difficult to achieve the perfect age verification - false sense of security for both parents and children - difficult coordination with freedom of speech and privacy

Codes of conduct:

As said before, the European Commission promotes the use of self-regulation to provide a The Commission does not provide a specific model of self-regulation, rather it accepts the existence of multiple choices,[30] including codes of conduct; however, in any model drawn up by the relevant actors, the principles that it should respect are those of effectiveness, fairness, and transparency. [31] Furthermore, in case of codes of conduct, they should provide credible mechanisms for monitoring compliance, taking complaints and sanctions for non-compliance, together with means of making the public aware of their existence.[32]

Advantages	- quick reaction to public concerns - flexible tool - expertise of industry players
Disadvantages	- Limited level of enforceability - Risks of 'private censorship', as commercial organisations can decide what content can be considered harmful - Low awareness of the existence of codes of conduct from end-users.

V. Case study: social networking

We now turn to a case study, taking an example easily available on the Internet: social networking, so as to verify the adaptability of the previously listed tools, and eventually provide the better synergy among them.

[30] See, **J-F. LEROUGE**, "Internet Effective Rules: the Role of Self-regulation", in *The Edi Law Review*, 2001, 199 ff., where the Author lists the different forms of regulation: the "simple" unilateral declaration of will, the adoption of codes of conduct, the contract, the certification or labelling methods, the common practice or the emergence of a "lex electronica".

[31] See the guidelines already defined in the Recommendation 98/560/EC, cit., where the principles on which a self-regulatory intervention should be based were spelled out.

[32] According to a widely accepted definition, self-regulation norms are legal rules voluntarily created by a group of persons or their representatives from a particular sector of activities, accessible to them and therefore susceptible to be known by them and subject to sanctions in case of non-compliance, see **J-F. LEROUGE**, "Internet Effective Rules", cit., 197.

One of the most evident developments of Internet communication is its increasingly dynamic and interactive nature. Social networking is one of the new phenomena that bloomed in this evolved environment.[33] In social networks, users, once registered, can make public their personal data in order to establish a set of contacts with others who went to the same schools or universities (such as in *facebook.com*),[34] or who work in the same sector or firm (such as in *linkedin.com*),[35] or even in order to make self-promotion (such as in *myspace.com*).[36] In all these cases, users make available personal information, including sensitive data, to the entire circle of registered users. This behaviour can simplify the collection and the elaboration of users' profiles, giving leeway also to secondary use by third parties, who can take advantage of such information in different ways.[37]

Potential risks to children and young people using social networking services can include but are not limited to:

- bullying by peers and 'friends';
- exposure to inappropriate and/or harmful content;
- posting illegal or inappropriate content;
- posting personal information that can identify and locate a child offline;
- download viruses and *malware*;
- sexual grooming, exploitation and abuse through contact with strangers;
- exposure to information about self–harm techniques or encouraging anorexia and suicide;
- identity theft;[38]

---

[33] These services are considered to be part of a paradigm shift in the evolution of the Internet, which is now frequently referred to as Web 2.0. Web 2.0 represents a fundamental shift away from this model, towards a more dynamic and interactive Internet where the creation of content is decentralised and more controlled by individuals or communities of users.

[34] See http://www.facebook.com. On this issue see **I. BROWN**, **L. EDWARDS** e **C. MARSDEN**, "Stalking 2.0: privacy protection in a leading social networking site", paper presented at the conference "GiKii returns", London University College, 19 September 2007, available at http://www.law.ed.ac.uk/ahrc/gikii/docs2/edwards.pdf, and more recently **L. EDWARDS** and **I. BROWN**, "Data control and social networking: irreconcilable ideas?", available at http://ssrn.com/abstract=1148732.

[35] See http://www.linkedin.com

[36] See http://www.myspace.com

[37] **G. MACCABONI**, "La profilazione dell'utente telematico fra tecniche pubblicitarie on-line e tutela della privacy", *Riv. Dir. Inf. e Informatica*, 2001, 425; **C. D'AGATA**, ""Self" e "strict" regulation: il trattamento dei dati personali nell'approccio "pluridisciplinare" di tutela introdotto dal codice della privacy", *Riv. Dir. Inf. e Informatica*, 2004, 883; **L. EDWARDS** e **G. HOWELLS**, "Anonimity, consumers and the Internet: where everyone knows you're a dog" in **C. NICCOL**, **J.E.J. PRINS**, **M.J.M. VAN DELLEN** (eds.), *Digital anonimity and the law – Tensions and dimensions*, T.M.C. Asser, The Hague, 2003, 221.

[38] Identify theft is defined as the case in which personal details have been stolen and are used illegally. In most cases identify theft happens through the method of *phishing* (criminally fraudulent process of attempting to acquire

- race hatred; etc. [39]

How can these risks be faced and overcome through the aforementioned tools ?

Technical tools can help limiting the diffusion of children personal data. For instance, an 'age locking' can set profiles of users under eighteen automatically private, thus protect them from being viewed by adult users that they don't already know in the physical world.[40] This can be a useful tool that can bypass some of the aforementioned limitations of age verification *per se*, as it will only define as threshold the over/under eighteen years old.[41] This solution can be useful also to hinder grooming as children personal data (and also photographs, address, etc.) cannot be seen by over eighteen,[42] but it could not limit cyber-bulling, if the bully is in the same age group.[43] In the latter case, the provision of a 'report an abuse' button could be added in the site design, so as to give users the possibility to report any uneasy situation including cyber-bullying, pornography or unauthorised use. This could help in drafting a rating system based on the experience of users, (though the use of children as guinea pig would not be borne as acceptable).

However, the previous solutions are mainly on voluntary basis, as they are default settings coded in the software written for the social networking site (or they are included in clauses of the codes of conduct). In other words, these rules are applied by social networking site as long as they have incentives to do it. On the one hand, the accountability and the sensibility to acceptable children security level can enhance the usage of the website, as for instance parents will not impede to their children to access and participate to such websites. On the other hand, it must be underlined that social networking sites earn revenues through their activity, though services

---

sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication) or *pharming* (a hacker's attack aiming to redirect a website's traffic to another, bogus website).

[39] Other possible threats are glorifying activities such as drug taking or excessive drinking; encouragement of violent behaviour such as 'Happy Slapping'; physical harm to young people in making video content, such as enacting and imitating stunts and risk taking activities such as playing 'Chicken' on railways; leaving and running away from home as a result of contacts made online.

[40] See for the *Joint Statement on Key Principles of Social Networking Safety*, declared by U.S. Attorneys General and MySpace on 14th January 2008, where the website agreed to implement such 'age locking' tools for new profiles so as minors will be locked into the age they provide at sign-up while 18 years old and older members will be able to make changes to their age as long as they remain above the 18 years old threshold.

[41] It must be said that any user can create a fake online profile, so as to get into the adult or children limited space, however, in such networks the evidence given by photographs and alike could clearly give information about real age or at least instil some doubts.

[42] This is also more efficiently achieved through other technical solutions, i.e. restricting 'friend requests' to only those who know email address or last name of the children, imposing 'friends only' group invite as mandatory (or as default) preference in profiles, etc.

[43] This is usually the case, as bulling starts in school, mostly among classmates.

provided to users are (generally) free. As a matter of fact, revenues come primarily via third party advertising served to users.

For instance, a privacy policy can state that: "*We do not provide contact information to third party marketers without your permission. We share your information with third parties only in limited circumstances where we believe such sharing is 1) reasonably necessary to offer the service, 2) legally required or, 3) permitted by you.*";[44] however, this leaves open the question of when exactly the site "*believes*" that you wish to share your information.[45] In practice, the website would allow third party advertisers access to its site and users, permitting them to profile users and send targeted advertising.[46]

On a completely different perspective, we should also take into account children perception of such interventions. As a matter of fact children and young people would interpret those devices as restrictions to their social networking activities. This would be self-defeating if children reaction will be to leave security-sensitive website and participate in other sites where more lax operating restrictions are available. The issue, still without easy solutions, is how to create sensible online policies without encouraging kids to operate completely surreptitiously in a "digital underground".

VI. Conclusions

A conclusion that can be drawn from the preceding case study is that any policy aimed at protecting children, either from illegal and harmful content or from other possible online risk, due to the nature of the subject-matter, should be of a multi-faceted nature.

On the one hand, in order to achieve an adequate level of effectiveness, several measures and actions should be combined in a complementary way, such as creating reporting facilities,

[44] This example is taken by Facebook privacy policy, available at http://www.new.facebook.com/policy.php?ref=pf.
[45] See for a deeper analysis of privacy issues concerning social networking sites, **L. EDWARDS** and **I. BROWN**, "Data control and social networking: irreconcilable ideas?", cit., 14.
See that in the case of anonymised data this could be possible, as for instance Facebook privacy policy clearly admits: "*Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people in a network like a band or movie and personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they're more likely to be interesting to you. For example, if you put a favourite movie in your profile, we might serve you an advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are.*"
[46] See **F. CASAROSA**, "Privacy in search engines: Negotiating Control", on file by the Author.

empowerment of children as users of these technologies, self-regulatory elements and structures for cooperation between different stakeholders.

On the other hand, we should not overestimate the aforementioned solutions. For instance, technical devices will always suffer from inherent limitations and can be circumvented. A different factor that, instead, can last for a lifetime and can build a better online environment is children education.

An important and ever-increasing role should be given to teaching children how to be good cyber-citizens and how to identify and report online threats (predators, bullies, scam artists, etc.). Moreover, as children are now more savvy and sensible about online threats, it is even more important – for institutions, parents and carers – to keep being vigilant about online safety education and etiquette, providing always better and more accountable ways to give children lessons about sensible online behaviour and relations.