Child Privacy Protection Online:

How to Improve It through Code and Self-Regulatory Tools

Dr. Federica Casarosa

Abstract

The accomplishment of an adequate level of privacy is one of the main concerns related to the increasing diffusion of Information and Communication Technologies, due to the expanding possibilities to collect, organise and store thousands of data.

Social studies show that children are more and more interested in new technologies, and Internet in particular offers them new forms of socialisation not available before. When surfing, children leave traces of their passage and provide information about themselves. These pieces of information can be easily organised so as to create a full-fledged profile which would serve for marketing purposes. Thus, websites can monitor and understand what attracts children to the site and then tailor the content and services based on the children's identified interests.

The paper will analyse the changes in the policy approach at European level concerning the protection of children privacy, using a very wide concept of privacy which is interpreted as form of control over personal data. Thus, the analysis will consider in particular the commercial exploitation of personal data, as in this case it is clear that the child lost the control over his/her own data. The analysis will be based on a modified version of the all-embracing matrix developed by Gunningham and Sinclair (1998) concerning the design of the most effective regulatory mix, taking into account the different mechanisms that at European level were put forward. Given the final evaluation of the current regulatory mix, a tentative conclusion will be presented delivering suggestions and comments for further improvement.

Keywords

Children protection; privacy; private regulation; internet.

1. Setting the scenario: children and Internet

The accomplishment of an adequate level of privacy is one of the main concerns related to the increasing diffusion of Information and Communication Technologies, due to the expanding possibilities to collect, organise and store thousands of data (Art 29 WP, 2009).

In particular, Internet has become one of the most important and prolific sources of data concerning users' identities, behaviours and preferences. As a matter of fact, once the computer is connected on-line, any user can reap the benefits of an extremely rich experience but, while surfing on-line, (s)he leaves, consciously or not, footprints on the web. In the worst case scenario, this could allow unlawful exploitation of the information available, and such risk becomes even more critical if the data collected relate to children.

Social studies show that children are more and more interested in new technologies, and Internet in particular offers them new forms of socialisation not available before (Commission 2006). Through e-mail exchanges, on-line games, chats and other services, children are now increasingly able to relate to others living in far away places, to meet different people and learn about their lives, history, games and many other topics which can enhance their own knowledge of reality in unprecedented and unparalleled way (Simpson 2005).[1]

In all these cases, children leave traces of their passage and provide information about themselves. These pieces of information available on-line can be easily organised so as to create a full-fledged profile of any user, being it children or not. The rational to collect such information can be distinguished in marketing purposes and unlawful behaviour.[2] In the latter case, one of the main features of Internet is diverted from its original objective, namely the possibility to connect and get to know people all around the world. Although the ability to get

[1] Statistics concerning children use of Internet do not show a wide change in the last few years: the current average, at European level, of people up to 17 years using the Internet is 50% (Eurobarometer 2007). However, if we split this number with regards to different age references, the picture changes. Analysing the moment for the first baptism of Internet use, it is perceivable that access, although probably available since 6 years, becomes (almost) a rule at the age of 8. Moreover, the average of children between 12 and 18 using Internet significantly overcomes the average that characterize young adults (age 18-24) in a similar age period, as the former rate 87% while the latter only 73%.

[2] See in particular the Declaration of the Committee of Ministers "on securing the dignity, security and privacy of children using the Internet", adopted on 20th February 2008 at the 1018th meeting of the Ministries Deputies, available at https://wcd.coe.int/ViewDoc.jsp?Ref=Decl%2820.02.2008%29&Ver=0001 (last accessed on ***).
The document clearly identify as risks associated with the protection of the privacy of children the traceability of children's activities that may expose them to criminal activities, such as solicitation for sexual purposes or other illegal activities; and also the profiling and retention of personal data regarding children's activities.

in touch with unknown but interesting people is the most intriguing and fascinating character of the World Wide Web, believing that all such on-line users are trustworthy and disinterested is probably naïve. Unfortunately, recurring news warn that users can hide under nicknames or fake identities in order to pursue harmful objectives (Duncan, 2008; Kierkegaard 2008).

This is probably the worst case scenario when speaking about minors, as the wide availability of children information on-line can open the doors to 'grooming' and 'cyber-bulling'. In the first case, children can be 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.[3] Children may encounter contact with paedophiles, with people met in a chat room or via ordinary e-mail, which may exploit children's innocence to harm them. During teenage years, minors increase the use Internet for social purposes such as talking to distant friends or playing on-line games with chat facilities.4 Offenders can pose as sympathetic peers and trap or induce unsuspecting children.

Cyber-bullying, instead, 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[5]. This can occur not only through text message but also through videos being uploaded on open video-sharing websites, having an even more distressing effect, because the bullying in on-line environment has a potentially enormous audience, extending the humiliation and embarrassment of the victim. Cyber-bullies, which are usually peers or schoolmates in this case, may also harm children indirectly through the disclosure of 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

[3] See that while the number of teens who have been made uncomfortable by an on-line experience with someone they do not know is relatively small, there are certain traits and activities that are more likely to attract interactions with unknown individuals, namely the creation of profiles on social networking sites, and the posting of personal photos on-line. (Pew Internet & American Life project, *Teens and on-line stranger contact*, 2007).

[4] Moreover, young people start to use Internet also as a tool to explore their identity, for instance, to create a different (often ideal) version of themselves which would also entangled an experimentation of sexual limits (Simpson, 2005, 120 ff.).

[5] Despite this definition, the phenomenon is not limited to children, though is more commonly referred to as cyber-stalking 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.

defames or ridicules them.[6] Given the width of such issue it will not be dealt within this paper.

The other rational for data collection is based on the use of internet technology to enhance business activity, i.e. for marketing purpose. As a matter of fact, e-commerce has had a strong impact on business and society within the last decades (Picker 2008).

The information collected by a website is likely to be used either directly to benefit the website or sold to assist market research companies or direct marketing services. The more favourable interpretation says that a better knowledge concerning user interests can provide more personalised services. This, translated into economic terms, means that better profiling can provide consumers better advertisements thus push to better purchasing choices, and this consequently end up in higher profits for business (Church and Kon 2007; Casarosa 2008). Under this perspective, Internet offers advertisers and marketers the unique opportunity to gain direct access to children.

Thus, websites can monitor and understand what attracts children to the site and then tailor the content and services based on the children's identified interests (Stevees 2008, Edwards 2008). For example, website can specifically ask children for feedback about the site, or send directly to them newsletters and notices about on-line contests and opportunities to win prizes. Therefore, knowing children's preferences gives the website a competitive advantage because it can tailor its content and activities to suit its specific audience.

Moreover, children are perceived as influential consumers: on the one hand, they do have their own spending power; on the other hand, they also have a strong influence on their parents' spending. Thus, websites have a business incentive to collect information, and technological advances provide excellent means to gather unlimited amounts of personal information.

Given this framework, the paper will analyse the changes in the policy approach at European level concerning the protection of children privacy, using a very wide concept of privacy which is interpreted as form of control over personal data (Rauhofer 2008; Lugaresi and Bertazzo

[6] Recent surveys show that about one third (32%) of all teenagers who use the internet say they have been targets of a range of annoying and potentially menacing on-line activities – such as receiving threatening messages; having their private emails or text messages forwarded without consent; having an embarrassing picture posted without permission; or having rumours about them spread on-line (Pew Internet & American life project, *Cyberbullying and Online teens*, 2007). See also on this issue, 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 (last accessed on ***).

2009). Thus, the analysis will consider in particular the commercial exploitation of personal data, as in this case it is clear that the child lost the control over his/her own data.

The analysis will be based on a modified version of the all-embracing matrix developed by Gunningham and Sinclair (1998) concerning the design of the most effective regulatory mix, taking into account the different mechanisms that at European level were put forward. Given the final evaluation of the current regulatory mix, a tentative conclusion will be presented delivering suggestions and comments for further improvement.

2. The current regulatory mix for children privacy protection

In order to evaluate the level of protection of children's privacy, the current regulatory mix in force at European level will be defined. As the separate use of one single mechanism would be ineffective, due to the fact that "*all instruments have strengths and weaknesses, and […] none are sufficiently flexible and resilient to be able to successfully address all […] problems in all contexts*" (Gunningham and Sinclair 1998, 50), the different tools in force will be analysed as a coordinated strategy. Through this regulatory mix, it will be possible to verify also whether the selected instruments are complementary, i.e. reciprocally enhancing positive effects, or counter-productive, i.e. negating or diluting other instruments effect.

The general instruments that can be possibly used include command and control regulation (hereinafter C&C), economic instruments, private regulation,[7] and information strategies. All of them can be also distinguished into sub-categories, that in case of C&C include design, performance and process standards (Gunningham and Grabosky 1998); in case of economic instruments include broad-based instruments, supply-side incentives and legal liability; in case of private regulation include both self-regulation and co-regulation (Cafaggi, 2006) and also voluntary decisions by single firms to self-restraint their own activity (through, for instance, codes of conduct); and finally information strategies include education and training, posting of databases and reports, etc.

Given the aforementioned matrix, the current regulatory framework at European level for the protection of children privacy would be framed as the following table show.

[7] The original categorisation by Gunningham and Sinclair there were two other general tools: self-regulation and voluntarism, the latter interpreted as the case in which "*the individual firm undertaking to do the right thing unilaterally, without any basis of coercion*" (Gunningham and Sinclair 1999, 54). However, in this paper we will include both tools under the private regulation heading, in which not only self-regulation and co-regulation can be included, but also the possibility of a self-restraint by an individual firm (e.g. code of conduct).

Table 1. European current regulatory framework

Command & control	**Economic instruments**	**Private regulation**	**Information strategies**
- Data protection directive[8] - Electronic communication directive[9]		- Safer Internet Action Plans; - Social networking principles; - FEDMA code of conduct	- Safer Internet Action Plans

Although the European Union has been a forerunner in tackling children protection issues, as the first step date back to the Green Paper on the protection of minors and human dignity in informational and audiovisual services,[10] the current framework does not directly address in any intervention the problem of children's privacy.

If we look at the C&C interventions, the basic framework concerning privacy at European level is the Data protection Directive 95/46/EC (Bennett 1992). The Directive requires that data is processed fairly and lawfully. This implies a high level of transparency in the process. Companies collecting and processing personal data must publish their data protection policy. Data must only be collected 'for specific, explicit and legitimate purposes'. However, such obligation does not receive any additional specification in case of children data, where the children ability of understanding privacy policies presented by the websites can be more limited, or at least can be different given the class of age (Bartoli 2009).

Moreover, the directive adds other principles for any fair treatment of data: the possibility to access and correct the data, the need to keep the data updated, and the possibility to object to the data treatment. Again, no distinction in case of children's data treatment is given by the

[8] Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995 p. 31 – 50.

[9] Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p. 37–47.

[10] 16th October 1996, COM (96) 483. In particular, the Green Paper provided an analysis of the legislation and policies in force at national, European and international level, pushing forward some guidelines to provide a more flexible regulatory framework capable to face the characteristics of the new services. At the same time, the European Commission published a Communication on Illegal and Harmful content on the Internet, in which such concepts were defined (16th October 1996, COM (97) 487 fin). The former may be banned for everyone, regardless of the age of the potential audience or the medium used. 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*", thus, access to it can be allowed only for adults. 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*" (Bonnici and Mestagh 2005, 142), while the latter is a matter of state choice.

directive, thus children has the same rights as adults concerning their data, though usually less knowledge about it.

The directive should be also read with the following intervention directive 2002/58/EC, the so-called Privacy and Electronic communication directive.[11] In particular, the latter comes into play when the third parties store information or gain access to information stored in the terminal equipment of a subscriber or a user (art. 5, par. 3). In terms of children's privacy protection, however, this directive does not help either, as it applies indifferently from the age of the user and imposes uniform rules on data controllers concerning, for instance, the storing of cookies in the computer of the child. Nonetheless, such obligations[12] would provide an indirect positive effect on children's privacy, as usually children will use parents' or schools' computers where such data processing would have been already refused.

Moving to the other regulatory tools on the issue, the first active intervention in the field was proposed by the European Commission in 1998, the so called 'Safer Internet Action Plan' (hereinafter IAP)[13] and its following extensions.[14] The initial IAP actions identified areas for concrete measures where Community resources should be focused on. Since 1999, the Action Plan has been extended and widened in its scope twice[15] in order to take into account

---

[11] See that this directive was part of a package of five new directives that aim to reform the legal and regulatory framework of electronic communications services in the EU, and repealed and replaced directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunication sector. As the latter was deemed outdated, the new directive should clarify the applicability of privacy rules also on communications transmitted with Internet and emails (Debussere 2005, 72).

[12] Remaining in the example of cookies, the two obligations concern the provision of clear and comprehensive information about the processing of the data, in accordance with the data protection directive, and the right to refuse such processing, see art 5 par. 3 of the directive.

[13] European Parliament and European Council, *Decision 276/1999/EC of 25th January 1999 adopting a 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* (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).

[14] See that the IAP actions were developed after the adoption of the Council Recommendation 98/560/EC, of 24th September 1998 (OJ L 270, 7.10.1998, p. 48), 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.

[15] 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; and European Parliament and European Council, *Decision 854/2005/EC of 11th 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).

"*currently unknown future developments in the on-line environment as the resulting threats will become increasingly important in the years ahead*".[16]

The IAP actions are included in the private regulatory interventions, as they do not have a binding character, but they all support the development and the implementation of coordinated codes of conduct and approved self-regulation solution. This option is not only due to the fact that coordinated private regulation can have a higher level of flexibility and can be better fit with the needs of an ever-changing environment (Casarosa 2007), but also to the general argument – clearly stated in IAP actions – 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*".[17]

The more recent IAP action defines four specific objectives: the promotion 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). In particular, the public-awareness raising action is 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.

Although references to privacy can be found throughout the intervention, and in particular in its Impact Assessment,[18] they are not significantly developed. Thus, the consequent actions adopted within this framework show only limited attention to the risks connected with children's privacy.

One of the more recent interventions is the adoption of Safer social networking principles.[19]

---

16 European Parliament and European Council, Decision 1351/2008/EC of 16 December 2008 establishing a multi-annual *Community programme on protecting children using the Internet and other communication technologies*, OJ 24.12.2008, L 348/118.

17 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.

18 See 3.2.2. Specific risks: disclosure of personal information; 3.3. Target groups; 5.2., Analysis of the impact of the policy options, *Impact Assessment – Accompanying document to the Proposal for a Decision establishing a multiannual Community programme on protecting children using Internet an other communication technologies*, 27th February 2008, COM (2008) 106 final.

19 Available at http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf.

The principles were developed by social networking sites in consultation with the European Commission, and a number of NGOs, in order to provide good practice recommendations for the providers of social networking and other user interactive sites, to enhance the safety of children and young people using their services.

In particular, principle 6 provides that social networking site should "*Enable and encourage users to employ a safe approach to personal information and privacy: Providers should provide a range of privacy setting options with supporting information that encourages users to make informed decisions about the information they post online. These options should be prominent in the user experience and accessible at all times.* ***Providers should consider the implications of automatically mapping information provided during registration onto profiles, make users aware when this happens, and should consider allowing them to edit and make public/private that information where appropriate.*** *Users should be able to view their privacy status or settings at any given time. Where possible, the user's privacy settings should be visible at all times.*" (emphasis added). In this case, indirectly the principle addresses the hypothesis of profiling and of possible use of such organised information.[20]

A better analysis of the case of children's data protection is provided an older document: the Federation of European Direct marketing (FEDMA) code of conduct for the use of personal data in direct marketing,[21] adopted by the European association with the Art 29 Working group in 2003.22 The code expressly address children's data collection, underlining that, data controllers should always make every reasonable effort to ensure that the child and/or the parent are properly informed about the purposes of the processing of such data. In particular when using commercial materials directed at children or otherwise knowingly collecting data from children, the information notice should be prominent, readily accessible and understandable by children. The code not only stresses the need for the parent's consent and his/her monitoring activity,[23] but it also take into account the common features use in the sector to attract children and collect their data, as it provides that "*Data Controllers should not make the Child's participation*

[20] More focused attention is given in the case of (mobile operators) code of conduct where, at art 5, par 8, the provision clearly states that "*In case of services exclusively targeting children (the so-called "children's services"), mobile operators signing this Code undertake not to intersperse them with advertising and promotional initiatives*". See the full text of the code of conduct at http://www.gsmeurope.org/documents/eu_codes/italy_child_protection.pdf.

[21] Available at http://fedma.custompublish.com/codes-of-practice.347966-59917.html.

[22] Art 29 WP (2003).

[23] See point 2.6.3. of the code.

in a game, the offering of a prize or any other activity involving a promotional benefit conditional on the Child disclosing more Personal Data than what is strictly necessary for the participating in such activity".[24]

The aforementioned co-regulatory interventions target a performance that is beyond mandatory minimum standards that are set in the data protection directive, and as they are based on such C&C regulation they are inherently complementary. The complementarities arise because the two instruments are targeting different levels of performance: C&C focus on general data protection, while co-regulation goes into detail concerning a specific data owner. In these circumstances, regulation is the rising floor that follows the vanguard of private regulation, rather than the ceiling that gets imposed ahead of, and which limits, the voluntary responses.

Therefore, on the one hand, the co-regulatory intervention acts as specification of the more general data protection directive given the special treatment that should be provided in case of children data, but on the other hand it opens other problems in particular monitoring and enforcement in the application of such regulation.

3. Possible improvements

As clarified above, the current regulatory framework could provide complementary effects between the regulatory tools in force. However, this regulatory mix cannot guarantee the enforcement of all the codes of conduct presented above, as they do not always provide for sanctions or penalties in case of breach.[25]

---

[24] See point 2.6.4. of the code. See also the parent code concerning e-commerce and interactive marketing which also tackled children protection. Again the important feature that is stressed within the code is the educative and monitoring role of parents: "*Marketers should encourage parents to involve themselves in their children's' on-line activities, and where possible should provide parents with information on how monitoring/supervising of these activities can be carried out"*. This is not only a good will provision for parents, as the code underlines that "*Marketers should encourage children to gain consent from their parents/guardians before making any commitment to purchase goods or services"*. Available at http://fedma.custompublish.com/codes-of-practice.347966-59917.html.

[25] See that in art 27 of the data protection directive a European recognition of the national or community codes of conduct is provided. In particular, the directive delegate to the Art 29 WP the task to verify if the proposed codes are in accordance with European rules and whether they are to ensure adequate publicity of them. In their analysis, Art 29 WP explicitly requires that the code should achieve a minimum level of effectiveness, in other words it should include provide effective sanctions, dispute resolutions, easy access to the contact points, monitoring of the system. At the moment only the FEDMA and IATA codes have been adopted following this procedure. See on the point the WiK consult and Rand Europe report, Comparison of Privacy and Trust Policies in the Area of Electronic Communications, 2007, 31 ff., available at http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/final_r

This situation could be improved if such regulatory mix is coupled with another one that is related to the means used for the collection of data from children. This potential improvement descends from the so called code as law approach, which was introduced by Laurence Lessig (1999).[26] In this perspective, technological architecture can shape users' behaviours through the limitation or enhancement of hardware and/or software abilities. Thus, what should be achieved is the privacy by design result (Cavoukian 2009).

In particular, what can be used are Internet filtering and monitoring software, which practically can let parents block access to adult websites and typically let them impose time management constraints on their children's computer and Internet usage.[27] These software packages also include far more robust monitoring tools that let parents see each website their children visit, view every e-mail or instant message that they send and receive, or even record every word that they type into their word processors.[28] Many of these stealth monitoring tools can then send parents a periodic report summarizing their child's Internet usage and communications.

Other technical tools are safe search engine filters which can block a great deal of potentially objectionable content that children might inadvertently stumble upon during searches.[29] Parents can easily customize the settings from a more restrictive filtering to a more moderate one, covering all search results or only those related to image searches.

In some cases, these tools are provided for free, such in the case of safe search engine filters which are embedded in the website search or the 'add-ons' available for web browsers,[30] but in other cases they can be sold on the market, such in the case of filtering and monitoring software. In this case, governments at national level could foster their diffusion and use (particularly in schools) through economic incentives to enterprises which provides them, lowering down their cost on the market. This solution could be included in the economic

---

eport_20_07_07_pdf.pdf.

[26] See a different framing of such concept in terms of 'design', in Murray and Scott (2002).

[27] See Thierer (2009, 120-123) for a wide selection of filtering and monitoring software available on the market.

[28] Though, this could raise different privacy concern in the relationship between parents and their children.

[29] See for instance Google Safe search in which three possible level of control can be defined in advance. See the presentation of this free service at http://www.google.com/support/websearch/bin/answer.py?hl=en&answer=35892.

[30] See the case of Mozilla, which does not offer parental controls directly for the Firefox browser, but allows third parties to devise and offer parental control tools as "add-ons" to the browser. Thus, once the program is loaded onto a user's computer, it locks the Firefox browser such that a password is required before a user can access the Internet. Parents can then establish a user account for their children that only allows them to access to a set of pre-screened, kid-friendly websites.

incentives column above in the form of supply side incentives.

However, also in this case monitoring should not be lowered down as it is been claimed that the same firm providing the filtering software have used the information about on-line surfing experience of children in order to create updated databases to be sold to direct marketing firms.[31]

A similar problem can be found in case of web portals that are expressly focused on children, in particular when related to games and toys well known in real life experience. Obviously, this websites are appropriate for very young web surfers, as they do not link to any potentially objectionable content. However, these websites can collect directly and indirectly children information, asking children to consciously provide the website the requested information, such as name, e-mail address, postal address, telephone number, age or date of birth, and gender through registration forms, order forms, surveys, contests, and games. In some cases, the websites add also trusting schemes so as to reiterate the visits to the websites and keep track of each and every change in the children preferences.

In this case, the privacy enhancing technologies, such as the so called P3P software, could solve, at least partially, the problem. As a matter of fact, P3P or Platform for Privacy Preferences is a project to develop software able to analyse the privacy policies of websites and to compare them with the user's preferences as to the information they wish to release, helps to ensure that data subjects' consent to processing of their data is an informed one.[32] Thus, in this case parents can set the preferences of the P3P software to the stricter or milder ones depending on the age of the child, in order to block access to websites where collection and use of children data is beyond the needs to provide services (e.g. on-line games).

This can be promoted either through economic incentives to software developing enterprises and through better information strategies in order to raise consumer awareness concerning the need and benefits to use such technologies.[33] Moreover, this could have a positive effect in also in terms of incentives to website to behave in a privacy friendly way.

---

[31] See the complaint presented to the Federal Trade Commission by the Electronic Privacy Information Center concerning an enterprise which is claimed to surreptitiously collect information concerning children's on-line behaviour, in order to use the information to "customize the advertising content [children] see," and transfers information concerning children's browsing and on-line chats to marketers. See the complete text at http://epic.org/privacy/ftc/Echometrix%20FTC%20Complaint%20final.pdf.

[32] See more at the project website at http://www.w3.org/P3P/.

[33] See also in this direction Commission (2007).

4. Concluding remarks

In this essay I tried to shed light on the current regulatory mix that is in force at European level in order to protect children's privacy. Although the current regulatory framework can provide a positive outcome in terms of complementary among C&C and private regulatory tools in force, however, not sufficient monitoring and sanctioning efforts have been put forward to support private regulation in this framework.

Institutional, market and social actors never tried to deny that children privacy protection is a priority, given the risks they face on new media. Nonetheless, given the multifaceted issues at stake, a balance is not always easy to attain.

Some suggestions have been presented in order to improve the result giving more space to technology, leading towards a privacy by design direction. On the one hand, such 'architectural' devises can increase the level of control over children surfing on-line, avoiding ex ante dangerous encounters and ex post providing quicker reaction in case of tangible threats. On the other hand, also technical solutions can prove to be an issue from the legal point of view. For instance, it would be the case for stricter monitoring software, who can allow parents to surreptitiously control all the on-line activities of their children, including their communications. In this case, children privacy sphere could be infringed not by unknown users but instead from their own parents.

This framework shows that finding a 'universal' solution for children privacy, though desirable and understandable, is not still feasible. Instead, the search regulatory solutions should take into account a layered approach, involving many tools, methods, and strategies, in which also technical devices can be part of that mix.

Bibliography

ART 29 WP (2009). Opinion 2/2009 on the protection of children's personal data (General guidelines and the special case of schools), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp160_en.pdf.

ART 29 WP (2003). *Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing*, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp77_en.pdf.

BARTOLI, E. (2009). *Children's data protection vs marketing companies*, International Review of Law, Computers & Technology, 23, 1, 35-45.

BENNETT, C. J. (1992). *Regulating privacy : data protection and public policy in Europe and the United States*, Ithaca : Cornell University Press.

CAFAGGI, F. (2006). *Reframing self-regulation in European private law*, Alphen aan den Rijn, Netherlands: Kluwer Law International.

CASAROSA F. (2008). *Privacy in search engines: Negotiating Control*, on file by the Author.

CASAROSA, F. (2008). *Il ruolo delle diverse tipologie di informazione su internet*, Ph.D. Thesis, Florence : European University Institute.

CAVOUKIAN A. (2009). *Privacy by Design … Take the Challenge*, available at http://www.privacybydesign.ca/pbdbook/PrivacybyDesignBook.pdf.

CHURCH, P. and G. KON (2007). *Google at the heart of a data protection storm*, Computer Law & Security Report 23: 461-465.

DEBUSSERÉ, F. (2005). *The EU E-privacy directive: A Monstrous Attempt to Starve the Cookie Monster*, International journal of law and information technology, 13, 1, 70-97.

DUNCAN, S. (2008). *My space is also their space: ideas for keeping children safe from sexual predators on social-networking sites*, Kentucky Law Journal 96, 4, 527-577.

EDWARDS, L. (2008). *Data protection 2.0: this time is personal*, presentation given at the Gikii 2 conference, available at http://www.law.ed.ac.uk/ahrc/gikii/docs3/edwards.pdf.

EUROBAROMETER (2007). *Safer Internet for children – Qualitative study in 29 European countries*, available at http://ec.europa.eu/public_opinion/quali/ql_safer_internet_summary.pdf.

EUROPEAN COMMISSION (2006). Communication 'Towards an EU strategy on the rights of the child'. COM(2006) 367 final.

EUROPEAN COMMISSION (2007). Communication 'Promoting Data Protection by Privacy Enhancing Technologies (PETs)', COM(2007) 228 final.

GUNNINGHAM, N. and D. SINCLAIR (1999). *Regulatory Pluralism: Designing Policy Mixes for Environmental Protection*, Law & Policy 21(1): 49-76.

GUNNINGHAM, N. and P. GRABOSKY (1998). *Smart Regulation: designing environmental policy*, New York, Oxford University Press.

KIERKEGAARD, S. (2008). Cybering, online grooming and ageplay, Computer law & security report, 24, 41-55.

LESSIG, L. (1999). *Code and other laws of cyberspace*, New York : Basic Books.

LESSIG, L. (2006). *Code 2.0*, New York : Basic Books.

LUGARESI, N. and S. BERTAZZO (2009). *La tutela del diritto alla privacy davanti al Garante per la protezione dei dati personali – Profili sostanziali e procedurali*, in DENTE B., LUGARESI N. and RIGHETTINI M.S. (eds.), *La politica della privacy tra tutela dei diritti e garanzia dei sistemi*, Firenze: Passigli Editori.

MIFSUD BONNICI, J.P. and C.N.J. DE VEY MESTDAGH (2005). *Right Vision, Wrong Expectations: The European Union and Self-regulation of Harmful Internet Content*, Information & Communications Technology Law, 14, 2, 133-149

PICKER, R. (2008). *Competition and Privacy in Web 2.0 and the Cloud*, University of Chicago Law & Economics, Olin Working Paper No. 414, available at SSRN: http://ssrn.com/abstract=1151985.

RAUHOFER, J. (2008). *Privacy is dead, get over it! Information privacy and the dream of a risk-free society*, Information & Communications Technology Law, 17, 3,185-197

SCOTT, C. and MURRAY A. (2002). *Controlling the New Media: Hybrid Responses to New Forms of Power*, Modern Law Review, 65, 491-516.

SIMPSON, B. (2005). *Identity Manipulation in Cyberspace as a Leisure Option: Play and the Exploration of Self*, Information & Communications Technology Law,14, 2,115-131

STEVEES, V. (2008). *It's Not Child's Play: The Online Invasion of Children's Privacy*, University of Ottawa Law & Technology Journal, Vol. 3, No. 1, 2006, available at SSRN: http://ssrn.com/abstract=999687.

THIERER, A. (2009). *Parental Controls and Online Child Protection: A Survey of Tools and Methods*, The Progress & Freedom Foundation, available at http://www.pff.org/parentalcontrols.