EUI Working Papers

RSCAS 2011/15
ROBERT SCHUMAN CENTRE FOR ADVANCED STUDIES

PROTECTION OF MINORS ONLINE:
AVAILABLE REGULATORY APPROACHES

Federica Casarosa

EUROPEAN UNIVERSITY INSTITUTE, FLORENCE
ROBERT SCHUMAN CENTRE FOR ADVANCED STUDIES

Protection of Minors Online: Available Regulatory Approaches

FEDERICA CASAROSA

EUI Working Paper **RSCAS** 2011/15

ISSN 1028-3625

Printed in Italy, March 2011
European University Institute
Badia Fiesolana
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu/RSCAS/Publications/
www.eui.eu
cadmus.eui.eu

Robert Schuman Centre for Advanced Studies

The Robert Schuman Centre for Advanced Studies (RSCAS), created in 1992 and directed by Stefano Bartolini since September 2006, aims to develop inter-disciplinary and comparative research and to promote work on the major issues facing the process of integration and European society.

The Centre is home to a large post-doctoral programme and hosts major research programmes and projects, and a range of working groups and ad hoc initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration and the expanding membership of the European Union.

Details of the research of the Centre can be found on:
http://www.eui.eu/RSCAS/Research/

Research publications take the form of Working Papers, Policy Papers, Distinguished Lectures and books. Most of these are also available on the RSCAS website:
http://www.eui.eu/RSCAS/Publications/

Abstract

If the second half of the 20th century saw the flourishing of a wide range of new technologies, the 21st century is the time in which such technologies become ubiquitous. In particular, the Internet, originally designed as a system of communication for military services in case of default of radio systems, is now the most widespread technology globally, providing the easiest and cheapest way to connect users from different parts of the world.

Needless to say, the most prominent users of interchangeable devices for the interactive use of the Internet are minors, either during their childhood or their teenage years. The widening of this new class of users, on the one hand, is a trigger for public policy to "revitalise agendas of informal education, health and lifestyle advice, and civic participation", but, on the other hand, it multiplies the difficulties of policymakers, who have become more and more concerned about the risks and perils that minors face during their online surfing activities. This paper will try to address the regulatory solutions put forward for the different types of risk that minors can encounter online, analyzing their scope and potential flaws in order to provide a set of criteria that could be taken into account in the drafting process of such policies.

Keywords

Regulation, regulatory strategies, children protection, internet, privacy, harmful content.

1. Introduction

If the second half of the 20th century saw the flourishing of a wide range of new technologies, the 21st century is the time in which such technologies become ubiquitous. In particular, the Internet, originally designed as a system of communication for military services in case of default of radio systems,[1] is now the most widespread technology globally, providing the easiest and cheapest way to connect users from different parts of the world.

In recent years, this medium has developed further: The Internet was once confined to personal computers, wherever they were located, either in offices or at home. Now, however, technology has improved, and not only notebooks, but also different types of devices are able to provide access to the web, paving the way for the possibility of uninterrupted online connection. Portable and hand-held devices of this type include mobile phones, televisions, and game consoles.[2]

Moreover, the type of approach to the Internet has changed dramatically in less than a decade, involving users in the so-called 'web 2.0' environment.[3] If the traditional Web 1.0 was focused only on the availability of pre-defined content, the following 2.0 version is based on interactive information sharing, user-centered design, and collaboration among users to create new – again shared – content. Examples of this new generation of online services include the well-known cases of social-networking sites, blogs, wikis, video-sharing sites, etc.[4]

Needless to say, the most prominent users of interchangeable devices for the interactive use of the Internet are minors, either during their childhood or their teenage years. The widening of this new class of users, on the one hand, is a trigger for public policy to "*revitalise agendas of informal education, health and lifestyle advice, and civic participation*"[5], but, on the other hand, it multiplies the difficulties of policymakers, who have become more and more concerned about the risks and perils that minors face during their online surfing activities. Recent episodes in different parts of the world, in which minors were the main victims, have moved Internet regulation to the forefront of the policy agenda,[6] requiring a more coordinated approach that could involve not only national governments as standard setters and enforcers of detailed regulation, but also supranational organizations, industry and nongovernmental organizations as participants in the same process. Through this framework, policy objectives will be defined and regulatory approaches made more effective.[7]

---

1 On the history of Internet see J. Abbate, *Inventing the Internet*, MIT Press, 1999; J. Naughton, *A brief history of the future*, Phoenix, 1999.

2 See D. Tambini, D. Leonardi, and C. Marsden, ***Codifying cyberspace : communications self-regulation in the age of Internet convergence,*** Routledge, 2008; P. Luden (ed.), ***Convergence and Fragmentation: media technology and the information society,*** Intellect, 2008.

3 See "Web 2.0**."**, in Encyclopædia Britannica Online, available at <http://www.britannica.com/EBchecked/topic/1192837/Web-20>, where the popularity of such terminology is based on the series of Web conferences, first organized by publisher Tim O'Reilly in 2004.

4 See Y. Benkler, *The Wealth of networks – How Social Production Transforms Markets and Freedom*, Yale University Press, 2006.

5 S. Livingstone and D.R. Brake, "On the Rapid Rise of Social Networking Sites: New Findings and Policy Implications", Children & Society, 2010, p. 75.

6 See A. Nair, "Mobile phones and the Internet: Legal issues in the protection of children", International Review of Law, Computers & Technology, 2006, p. 179; and S. Duncan, "Myspace is also their space: ideas for keeping children safe from sexual predators on social networking sites", *Kentucky Law Journal*, 2008, p. 527.

7 See N. Villebeuve, "Barriers to Cooperation - An Analysis of the Origins of International Efforts to Protect Children Online", in R.J. Deibert, J.G. Palfrey, R. Rohozinski and J. Zittrain (eds.), *Access Controlled - The Shaping of Power, Rights, and Rule in Cyberspace*, MIT press, 2010, p. 56. In particular, the author provides the concept of 'dynamic cooperation' which "*constitutes not just the outcome of an agreement reached through bargaining, but the ongoing*

This paper will try to address the regulatory solutions put forward for the different types of risk that minors can encounter online, analyzing their scope and potential flaws in order to provide a set of criteria that could be taken into account in the drafting process of such policies.

In particular, the current level of involvement of minors online will be briefly described (par. 2), followed by a taxonomy of the existing risky situations (par. 3). Before approaching the set of examples of different regulatory approaches that have been used by governments and/or industry to tackle one or more of the identified risks, a general introduction on the regulatory approaches available in relation to Internet regulation will be presented (par. 4). The different examples will then provide evidence for the analysis of the advantages and disadvantages of the regulatory strategies adopted (par. 5). These will be followed by tentative conclusions regarding the effectiveness of the presented regulatory approaches (par. 6).[8]

2. Minors online: figures and risks

As stated earlier, the increase of Internet diffusion and the widening of access possibilities through different devices have opened the doors to a steadily growing number of minors accessing the web. Recent researches show the increasing rate of Internet use by children and teenagers, both in terms of time spent and in terms of variety of activities carried out online. An Eurobarometer report provided evidence about the rising share of Internet usage by children up to sixteen years in European countries, where the percentage of minors using Internet has reached the rate of 51% in 2006, while the age of first contact with new technologies has fallen to six-eight years old.[9]

This is supported by the most recent publication of EU kids online project,[10] which widened knowledge of the of use of Internet by minors, providing evidence that children access Internet through a variety of devices, ranging from personal computers to mobile phones.[11] Moreover, the results show the range of activities children and teenagers are involved in: for school work, receiving content produced by others, playing games, communicating, posting images or messages for others to share, using a webcam, visiting file-sharing sites, spending time in a virtual world or writing in own or someone else's blogs.[12]

(Contd.)

practice of cooperation in which actors must rely on each others' capabilities for continual implementation in situations where compliance cannot be achieved solely through unilateral means", ibid. p. 55.

8 Concerning terminology, though different terminology is used in order to define minors under 18 years old, such as tynies, tweenies, children, kids, teenagers, etc. with reference to different age span, in this paper we will stick to a simpler distinction between children and young people, whereby the former category includes all people up to 13 years old, while the latter includes people between 13 and 18 years old. There is no specific reason to differentiate in legal terms, at least in Europe; however, this distinction will help us in particular when dealing with US legislation on privacy, namely the Children's Online Privacy Protection Act, 1998, that provides for different legal consequences in case websites collect data from people under or over 13 years old.

9 See the Eurobarometer 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).

10 See the London School of Economics based porject, *EU Kids Online II: Enhancing Knowledge Regarding European Children's Use, Risk and Safety Online*. See project details at <www.eukidsonline.net>.

11 See that the majority of children (55%) access the Internet via a shared personal computer, or though their own PC (34%). While nearly one third (31%) use their television set, and around a quarter do so via a mobile phone (28%), and another quarter access the Internet via games console (24%), though these last option have only taken up in the recent years. See more deeply in S. Livingstone, L. Haddon, A. Görzig and K. Ólafsson, *Risks and safety on the Internet - The perspective of European children*, 2010, p. 25, available at <http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Initial_findings_report.pdf>.

12 See Livingstone et al., *Risks and safety on the Internet*, cit., p. 37.

The previous results support the view that young people, mainly teenagers, have always been at the forefront of technology innovation, showing curiosity and technical abilities to play and personalize the wide array of electronic gadgets at their disposal. In particular, "*teenagers embrace this new online world with great enthusiasm, responding eagerly to its invitation to share ideas, contribute content, and otherwise place their stamp on a media system that they themselves could create and manage. The Internet played a pivotal role in their lives, influencing their family and social relationships*".[13]

The Internet can increase the knowledge and improve the social skills of minors, but it can also open the door to abuse and misuse. This does not mean we should interpret the Internet as evil, nor should we overestimate the risks online, which, though complex and multifaceted, in most cases are not significantly different from those faced by children offline. Moreover, some of these risks do not necessarily arise from the technology itself, but from offline behaviors that are extended into the online space.[14]

3. A taxonomy of risks

To say that the digital world holds threats as well as promises is a claim that is neither truly novel nor especially exciting. As a matter of fact, the Internet can improve the quality of life for children and young people, providing them better access to information and the widest possibilities to socialise with friends and foreigners. But, at the same time, such resources could also lead minors to decide on issues that normally they would not have to decide on in real life, in particular concerning their own safety. For instance, in the case of social networking sites, young people explore the construction of their identity, allowing mutual recognition in the peer network; however, the same service platform can be the venue for bullying activities by peers and 'friends', or for exposure to inappropriate and/or harmful content, or also provide personal information that can identify and locate a minor offline.[15]

The definition of such harms, however, is not univocally defined in the research studies carried out at national level, which define risks and opportunities quite heterogeneously. The best model available takes into account both the types of risks and the role of the minor user with regard to such risks. The table, then, distinguishes among three possible positions for the minor: recipient of communication (content), participant into a communication (contact), and finally actor providing content or reacting towards other users[16] (conduct). The possible motivations leading to risks, instead (in fact), are potentially problematic aspects that are related to content and services available online.

---

13 K. Montgomery, *Generation Digital Politics, commerce, and childhood in the age of the Internet*, MIT Press, 2009, at p. 106.

14 E. Staksrud and S. Livingstone, "Children and online risk: Powerless victims or resourceful participants?", Information, Communication and Society, 2009, p. 364-387; and from the institution point of view, Home Office task force on child protection on the Internet, *Good practice guidance for the providers of social networking and other user interactive services*, 2008, available at http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance/.

15 See the case study analysed in F. Casarosa, "Children protection Online: uneasy steps towards a balance between risks and freedoms", in M. Fernandez-Barrera, N. Gomes de Andrade, P. De Filippi, M. Viola de Azevedo Cunha, G. Sartor, P. Casanovas (eds), *Law and technology looking into the future – Selected essays*, European Press Academic Publishing, 2009, p. 106 ff.

16 See for instance the case of so-called *sexting*, or self produced child pornography. For a detailed analysis of this case see X. Zhang, "Charging children with child pornography - Using the legal system to handle the problem of 'sexting'", Computer law & security review, 2010, p. 251; and more generally B. Simpson, "Identity Manipulation in Cyberspace as a Leisure Option: Play and the Exploration of Self", Information & Communications Technology Law, 2005, p. 115.

Motives/Role	Commercial interests	Aggression	Sexuality
Content	1. Advertising, exploitation of personal information	2. Violent web content	3. Problematic sexual web content
Contact	5. More sophisticated exploitation, minors being tracked by advertising	6. Being harassed, stalked, bullied	7. Being groomed, arranging for offline contacts
Conduct	9. Illegal downloads, sending offensive messages to peers	10. Cyberbullying someone else, happy slapping	11. Publishing porn

Source: based on Eukidsonline (2009)

Obviously, it would not be feasible to address all the categories of risks included in the previous table; instead, this paper will focus on a limited taxonomy of risks in particular those related to the first two lines of the table, where minors can be qualified as victims instead of as tortfeasors.[17] The current analysis will then deal with: the availability of harmful materials (which addresses boxes mainly 2 and 3), online grooming (box 7), cyber-bullying (boxes 6 and 10) and unlawful invasion of minors' privacy (boxes 1 and 5). These cases will be briefly described in order to clarify the possible legal implications.

3.1. Availability of illegal and harmful materials

This category includes the cases in which children are harmed directly and indirectly: as victims of sexual abuse documented through photographs, films or audio files and then transmitted online, and as recipients of pornographic or unwanted sexual content.

The former can be qualified as child pornography, referring to material depicting children 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 (continuing into maturity) are compounded by the wide distribution and lasting availability of the photographs of the abuse. In this case, the content is deemed as illegal and, for practical reasons, refers to a wider age range, including any pornography involving a minor, according to jurisdiction.[18]

The latter case, instead, is qualified as harmful material. The legal definition of such a case is a difficult task for policy makers, due to the fact that the publication and distribution of harmful or offensive materials is not deemed illegal *per se*.[19] Rather, the definition of harmful is dependent on the cultural traditions and moral beliefs of users, thus, the individual perceptions can change from country to country, or even from community to community. Therefore, the decision on the harmful nature of online retrieved content lies with the individual.

Regulation can provide the legal and technical measures that allow citizens to exercise their right to decide what content is accessed and received, without being importuned by content considered

---

[17] See the coordinated works of M. Martín-Casals (ed.), *Children in Tort Law Part I: Children as Tortfeasors*, Springer link, 2006; and Id. (ed.), *Children in Tort Law Part II: Children as Victims*, Springer link, 2007.

[18] See also the definition given by art. 2, b) of the proposed Directive on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, COM(2010) 94 final, where child pornography includes not only any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of a child for primarily sexual purposes, but also the same materials where the subject appears to be a child, and regardless of the actual existence of such a child.

[19] On the distinction between illegal and harmful materials see Casarosa, "Children protection Online", cit.; and before 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, 2005, p. 133.

harmful. In these terms, policy makers should strike a balance between freedom of expression of citizens to produce and distribute harmful materials and the effects that harmful content can have over children, minority groups, and so on. The difficulty of achieving such a balance and the different cultural traditions involved have hindered the achievement of a coordinated strategy at international level, with a preference towards country based interventions and a wide range of regulatory strategies, ranging from state regulation[20] to different forms of private regulation.[21]

3.2. Online grooming

This category includes the cases in which children are contacted by people who 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. Usually, abusers will pose as children online and make arrangements to meet with them in person.

The most relevant context where such activity can take place is social networking sites, where fake identities can be easily created. Recently, such services have undergone a debate to evaluate the most effective technical tools to improve the level of safety for children and young people. In particular, some service providers have implemented technical restrictions so as to limit the possibility of contacts between minors (and in particular children) and adults.[22]

3.3. Cyber- bullying

This category includes the cases in which children are victims of bullying in the online environment.[23] Cyber-bullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group that is intended to harm others. This can occur not only through text messages but also through videos being uploaded on an open video-sharing website,[24] which has an even more distressing effect, because the bullying in the online environment has a potentially enormous audience, extending the humiliation and embarrassment of the victim.[25]

---

[20] See below the case of Australia, at par. 5.1.

[21] See Council Recommendation 98/560/EC, of 24th September 1998, 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, OJ L 270, 7.10.1998, p. 48. This Recommendation aimed at promoting national frameworks for self-regulation of harmful content for minors.

[22] See A. Thierer, "The MySpace-AG Agreement: A Model Code of Conduct for Social Networking?", available at http://www.pff.org/issues-pubs/pops/pop15.1myspaceagagreement.pdf

[23] 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-mails 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 or gossip as fact aimed at humiliation.

[24] 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.

[25] Home Office Task Force on Child Protection on the Internet, *Good Practice Guidance for the Providers of Social Networking and User Interactive Services*, cit., p. 17.

3.4. Unlawful invasion of privacy

This category includes, on the one hand, cases in which children are asked to disclose personal information that can be used to profile them and send them commercial advertising; and on the other, cases in which the websites collect children information without their knowledge.[26] In both cases the intended result is the creation of a user profile, with their preferences and tastes in terms of searches, and browsing activities.

As a matter of fact, profiling is an increasingly common practice on the Internet: it is based on the use of predictive data mining to establish recurrent patterns (profiles) permitting the classification of individuals into different categories.[27] Tracing the behaviour of Internet users results in the creation of an almost unlimited network of possible profiling practices generating knowledge with an impact upon individuals. In particular, this information collection is used by advertisers to deliver online advertisements that fit with the previous browsing behaviour of the individual user (the so called *behavioural targeting*). This kind of – eventually concealed – data treatment has been recently addressed in the policy agenda on both sides of the Atlantic,[28] due to the possible effects such practices could have on privacy protection.[29]

In this case, the risk is not merely the collection of personal information from children without their, or their parents', consent. Rather, in wider perspective, the risk involves "*the opening up of the child's 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*".[30] The possibility of obtaining details of children's online behavior can provide continuous feedback to marketers, who not only can easily select which products to sell to particular children, but also can fine-tune the child's online social environment, making the child more vulnerable to advertising messages. This kind of marketing raises serious questions, as it can constitute an invasion of privacy when enterprises penetrate the child's private space and extract data for instrumental purposes by manipulating their online environment.[31]

---

[26] See the classic cases of cookies that permit website operators to track user's online activities, also outside of their own websites. Cookies are small computer programs that are used by websites to store information such as username, passwords, and site preferences. Once a cookie is on a user's hard drive, it essentially acts as an electronic tracking device, which keeps a record of every website a user visits and then provides that information to the original website that placed the cookie.

[27] For a wider analysis of the profiling activity, see M. Hildebrandt and S. Gutwirth (eds), *Profiling the European Citizen: Cross disciplinary perspectives*, Springer Science, 2008.

[28] See in US, the Federal Trade Commission Staff Report on *Self-Regulatory Principles for Online Behavioral Advertising*, 2009, available at http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf. While see the recent intervention of European Cnsumer Commissioner M. Kuneva, at the Roundtable on Online Data Collection, Targeting and Profiling, Brussels, 31 March 2009, available at

http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/09/156&format=HTML&aged=0&language=EN&guiLanguage=en.

[29] 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. The challenge in data privacy is to share data while protecting personally identifiable information.

[30] V. Steeves, "It's Not Child's Play: The Online Invasion of Children's Privacy", *U*niversity of Ottawa law & technology journal, 2006, at p. 186; D. Piachaud, "Freedom to be a Child: Commercial Pressures on Children", LSE STICERD Research Paper No. 127, 2007, available at http://sticerd.lse.ac.uk/dps/case/cp/CASEpaper127.pdf.

[31] See A. Reid, "The Rise of Third Generation Phones", cit., p. 91, "*The greatest dangers apply in the cases of very young children who may be unable to distinguish between advertisements and the provision of information, and style-conscious and impressionable teenagers who are inclined to succumb to peer pressure.*" See more generally on the new marketing techniques, R. Sprague and M.E. Wells, "Regulating Online Buzz Marketing: Untangling a Web of Deceit", American Business Law Journal, 2010, p. 415.

4. Regulating the Internet

The regulatory strategies used to address child online protection should be evaluated within the technical context where they are applied: namely, Internet regulation. As a matter of fact, this issue continues to be at the center of an ongoing debate,[32] due to the increasing importance of Internet as a commercial platform. If originally pure self-regulation was the possible and effective choice to regulate the government agencies and research centers and universities which were the unique users of the communication network,[33] the multiple applications now available through online connection require a more deep deliberation over the type of regulatory tools to be used. In this sense Internet regulation is the answer to a clear necessity: on the one hand, the online activities inevitably have an influence on individuals and other entities in the real world; on the other, any user of online services cannot escape his/her own legal system (regardless of anonymity claims).[34] Moreover, the success of many of the most diffused Internet services is based on the availability of a stable and clear legal framework, whether national or international, whether private or public.

The two methods of bottom-up and top-down regulation are the major alternatives for Internet regulation. In bottom-up regulation, the Internet creates its own governance structure, based on the choices of its users and/or technical developers.[35] In top-down regulation, the government promulgates and enforces rules using typical command and control mechanisms.

In the case of the Internet, the hypothesis of direct governmental regulation was strongly criticized, at least at the beginning of its diffusion as a means of communication.[36] As a matter of fact, the Internet was connected with the idea of absolute absence of regulation or, more correctly, that the nature of Internet as a decentralised and non-geographic environment would be best administered by users, rather than by hierarchical controls imposed by governments. The so-called cyber-libertarians could not accept the threat of hard law regulation and emphatically asked, in the words of John Perry Barlow, "*[g]overnments of the Industrial World, you weary giants of flesh and steel* […] *on behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. [...] I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us*".[37]

---

[32] J. Goldsmith and T. Wu, ***Who controls the Internet? Illusions of a borderless world,*** Oxford University Press, 2006; R.J. Deibert *et al.*, *Access Denied*, cit.; R.J. Deibert, J.G. Palfrey, R. Rohozinski and J. Zittrain (eds), *Access Controlled - The Shaping of Power, Rights, and Rule in Cyberspace*, MIT Press, 2010.

[33] See M. MacCarthy, " What Internet Intermediaries Are Doing About Liability And Why It Matters", 2009, ExpressO, available at http://works.bepress.com/mark_maccarthy/1, where the author claims that "*cyberspace is not a separate place. It is simply a communications network that links real people in real jurisdictions with other people who might be in different jurisdictions*".

[34] R. Weber, *Shaping Internet governance: Regulatory challenges*, Springer, 2000, p. 4.

[35] L. Lessig, *Code version 2.0*, 2° ed., Basic books, 2006; C. Scott and A. Murray, "Controlling the new media: Hybrid responses to new forms of power", Modern Law Review, 2002, p. 502.

[36] In the period 1996-2000 the debate on the regulability of Internet was dominated by the cyberlibertarian/cyber-paternalist debate. The cyberlibertarian school linked enthusiasm for electronically mediated forms of living with libertarian ideas on freedom, society and markets. From a legal perspective, this position was most clearly established by David Johnson and David Post in their seminal paper *Law and Borders - The Rise of Law in Cyberspace*. Stanford Law Review, 48, 1996, 1367. The criticisms of this approach were several and opened the age of cyber-paternalism (see in particular J. Reidenberg, "Governing Networks and Rule-Making in Cyberspace", Emory Law Journal 45, 1996, 911; Id., "Lex Informatica: The Formation of Information Policy Rules Through Technology", Texas Law Review 76, 1998, 553). This approach proposed that individual freedom is not guaranteed by the architecture of the network. The illusion of freedom is created within a highly regulated sphere: the regulation coming from the architecture or code which governs the network (see L. Lessig, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999; C. Sunstein, *Republic.com*, Princeton University Press, Princeton, 2001; J. Litman, *Digital Copyright*, Prometheus, New York, 2001). See more widely in A. Murray, "The regulatory edge of the Internet", International Journal of Information Technology, 11, 2003, 87.

[37] J.P. Barlow, *Declaration of independence of Internet*, 1996, available at http://www.eff.org/barlow/library.html.

However, after the initial excitement about the Internet as a space outside the reach of governmental control has evaporated, and courts in several states have applied national laws to cyberspace, there is now a consensus among scholars and activists that the Internet is in principle subject to national regulation.[38] Moreover, we should take into account that the exclusion of governmental regulation does not exclude other forms of regulation, in which the involvement of public authorities can be reduced or limited to some specific phases of the regulatory process.

One of the alternatives to command-and-control is private regulation. This regulatory approach entails not only self-regulation and co-regulation,[39] but also voluntary decisions by single firms to self-restrain their own activity (through, for instance, codes of conduct). Private regulation of the Internet, and in particular self-regulation, is the option that has been strongly favored,[40] given the advantages it has with regards to public regulation in the online framework, namely the capacity to adapt to rapid technical progress and to the transnational development of the new communications medium. In addition to flexibility, self-regulation offers the benefits of greater efficiency, increased incentives for compliance, and reduced costs.[41]

However, recent studies have highlighted that not only pure self-regulation is a type of regulatory strategy that is unlikely to be found in real life,[42] but also that a probably better solution that could overcome the faults of self-regulation is a different strategy, namely co-regulation.[43] This category again is not a clear and precise concept,[44] rather it can take a variety of forms. For instance, it can

---

[38] See above fn. 36. See S. Stalla-Bourdillon, "Regulating the electronic marketplace through extraterritorial legislation: Google and eBay in the line of fire of French judges", International Review of Law, Computers & Technology, 2010, 39.

[39] F. Cafaggi, *Reframing self-regulation in European private law*, Kluwer Law International, 2006.

[40] See that not only the 'visionaries' such as Barlow were the advocates of a self-regulatory structure for new media during the first years of the diffusion of Internet network communication. As a matter of fact, the U.S. presidency launched a major self-regulatory initiative in particular with regard to privacy in electronic commerce, while on the other side of the Atlantic, the Council of Europe and the European Commission issued a series of reports and recommendation promoting Internet self-regulation. See for the former th White House, *A Framework for Global Electronic commerce*, 1 July 1997, available at http://www.technology.com/digeconomy/framewrk.html; and Department of Commerce, *The Emerging Digital Economy*, April 1998, available at http://www.technology.com/digeconomy/EmergingDig.pdf. While see for the latter initiatives, *Europe and the Global Information Society, Recommendations of the Bangemann Group to the European Council*, 1994; *Europe's Way to Information Society: An action Plan*, 1994, COM(94) 347 final; Commission Communication, *A European Initiative in Electronic commerce*, 1997, COM(97) 157 final.

[41] See M. E. Price and S. G. Verhulst, *Self-regulation and the Internet*, Kluwer Law International, 2005, p. 21; E.-J. Koops, M. Lips, S. Nouwt, C. Prins and M. Schellekens, "Should Self-Regulation be the Starting Point?," in, E.-J. Koops, M. Lips, J.E.J. Prins, and M. Schellekens, *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners*, T.M.C. Asser Press, 2006, p. 109.

[42] T. Prosser, "Self-regulation, Co-regulation and the Audio-Visual Media Services Directive", Journal of Consumer Policy, 31, 2008, p. 99.

[43] See Ibidem, p. 101, where the Author acknoledges that "*there is a continuum between different regulatory regimes with varying degrees of public and private input; what is apparent in practice is a cocktail of different techniques dependent on context*". See also the wider analysis on regulatory strategies in cyberspace by J. Cave, C. Marsden, and S. Simmons, *Options for and Effectiveness of Internet Self- and Co-Regulation*, report prepared for the European Commission by Rand Europe, 2008. See also the previous analysis by the PCMLP has conducted three surveys into self-regulation and co-regulation of the media for the Commission, for DG Media Culture and for DG Information Society (see in particular the latest two on Internet Codes of Conduct: An Analytic Report on Current Developments (2000) and Self-Regulation of Digital Media Converging on the Internet: Industry Codes of Conduct in Sectoral Analysis (2004)).

[44] See L. Senden, "Soft law, self-regulation and co-regulation in European law: Where do they meet?", Electronic Journal of Comparative Law, 9, 2005, available at http://www.ejcl.org/91/art91-3.PDF. See also the definition provided by European Commission, Second Evaluation Report on the application of Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity COM(2003) 776 final, 2004, available at http://europa.eu.int/comm/avpolicy/legis/reports/com2003_776final_en.pdf. The text clarifies that "[co-regulation] *should consist of cooperation between the public authorities, industry and the other interested parties, such as consumers. This is the approach laid out in the Recommendation. In order to promote national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity, the Recommendation enumerates*

provide a formal and explicit division of powers along policy area or domain lines, or a separate allocation of roles, e.g. decision-making, monitoring, reporting, and/or enforcement. Alternatively, a more flexible and adaptive arrangement can be defined where the private firms are supported in their regulatory activity when accepting and complying with certain positive conditions imposed by public bodies. These possible arrangements are obviously to be evaluated in practical terms in order to verify if the acknowledged shortcomings of self-regulation and command-and-control regulation could be overcome. For instance, in terms of legitimacy, co-regulation can be a better option where it is possible to verify empirically the respect of process values as well as efficiency and effectiveness in meeting public policy goals.

An additional point that should be highlighted in terms of Internet regulation, is the role played by technology itself in the regulation of users' behaviours. This approach is based on the so called 'code thesis', that claims that the nature of Internet is determined by the choices in software and hardware development. In this sense, code is the prime regulator or, as Larry Lessig put it,[45] 'the Code is Law'. However, such an analysis takes only into account the source of regulation, without taking into account the different regulatory functions, namely rule-making, compliance control and enforcement.[46] This more detailed analysis allows us to distinguish the different forms of regulation not only on the basis of the phases of the regulatory process allocated to private and public actors, but also including the possibility that such functions are carried out through 'architecture'.

5. Models of child online protection

In order to evaluate the level of protection of minors in relation to the risks mentioned previously, it is important to define in advance the possible regulatory approaches available. Although it is generally acknowledged that 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*",[47] for the sake of clarity the different tools will first be described individually. Then, in the case studies selected, coordinated strategies will be illustrated, emphasizing the main regulatory strategy at the core.

In the following analysis, regulatory approaches will be presented through examples from different geographical areas and addressing different risks. The objective is to identify interesting cases that could shed light on those critical issues that command-and-control regulation and private regulation practices share in terms of legitimacy, accountability and enforcement. The following sections will be devoted to command-and-control regulation in Australia and the U.S. regarding child pornography and privacy, as well as to self and co-regulation on a European level and in the UK, in the former, on general child protection in social networking sites and, in the latter, again, child pornography.

(Contd.)

different objectives to be fulfilled by (i) the Member States, (ii) the industries and parties concerned and (iii) the Commission."

45 L. Lessig, *Code version 2.0*, cit., p. 6. In another publication the Author states that "[t]*he code, or the software and hardware that make cyberspace the way it is, constitutes a set of constraints on how one can behave. The substance of these constraints varies - cyberspace is not one place. But what distinguishes the architectural constraints from other constraints is how they are experienced. […] In some places, one can elect to speak a language that only the recipient can understand (through encryption); in other places, encryption is not an option. Code sets these features; they are features selected by code writers; they constrain some behaviour (for example, electronic eavesdropping) by making other behaviour possible (encryption). They embed certain values, or they make the realization of certain values impossible. In this sense, these features of cyberspace also regulate, just as architecture in real space regulates*" (see L. Lessig, "The law of the horse: What cyberlaw might teach", in Harvard Law Review 113, 1999, 508).

46 See C. Scott and A. Murray, "Controlling the new media", cit., p. 504.

47 N. Gunningham, and D. Sinclair, "Regulatory Pluralism: Designing Policy Mixes for Environmental Protection", Law & Policy, 1999, 49-76, at p. 50.

5.1. Command & control regulation in Australia

After its victory in the latest election, the Australian Labour party started to put into reality the filtering program it sponsored during its electoral campaigning. This program would in fact replace the previous approach based mainly on voluntary filtering by ISPs and on free distribution to families of filtering software, which was deemed ineffective due to the lack of sufficient information for parents and schools and the easy circumvention of filtering software by children.

This is an exceptional case, since Australia is the first Western democracy that has almost succeeded in imposing mandatory Internet filtering upon ISPs located in its country.[48] As a matter of fact, the program is still under review by the government[49] due to the need to improve it, especially after the big debate this policy has raised at national and international levels.[50]

The plan of the government involved a two-tiered filtering system. The first level would block access to content that is illegal on the Internet under Australian law. This first level would be mandatory for all ISPs and, consequently, for all Australian Internet users. The second level would block material categorized as inappropriate for children, such as pornography and violence, and could be bypassed by users upon request. However, the governmental program did not clarify in detail what types of material would fall into this second tier of filtering.[51]

This system relies primarily on the existing legal framework that provides, under the Broadcasting Services Amendment (Online Services) Bill (1999),[52] a complaint and take-down system, in which the Australian Communication and Media Authority (ACMA) can initiate an investigation autonomously or after receiving a users' complaint concerning online content. In both cases, the results are the classification of the content under the National Classification Code,[53] and whenever such content falls into the prohibited category (such as sexually explicit activity between consenting adults, or images likely to disturb or harm minors), and it is hosted in Australia, the ACMA can send a take-down notice to the ISP, which is bound to comply with the decision.[54]

---

48 See the cases of Pakistan, Vietnam, Bahrain, Singapore, Syria, Cuba, Tunisia, Kazakhstan, UAE, Myanmar, Uzbekistan and Yemen, where the national regulation targets not only pornography, but also news, human rights and dissident websites. More in R. Deibert and N. Villeneuve, "Firewalls and Power: An Overview of Global State Censorship of the Internet", in M. Klang and A. Murray (Eds.), *Human Rights in the Digital Age*, GlassHouse, 2005, p. 121 ff.

49 See the government press release concerning the delay of 12 months in the implementation of the program which will leave the current framework up to the end of 2011, available at http://www.minister.dbcde.gov.au/media/media_releases/2010/068.

50 D. Bambauer, "Filtering in Oz: Australia's Foray Into Internet Censorship", Brooklyn Law School, Legal Studies Paper No. 125, 2008, available at http://ssrn.com/abstract=1319466.

51 See report submitted by the Electronic Frontiers Australia on *Measures to increase accountability and transparency for Refused Classification material' consultation*, available at http://www.efa.org.au/main/wp-content/uploads/2010/02/2010-EFA-DBCDE-Transparency.pdf.

52 See http://www.aph.gov.au/library/pubs/bd/1998-99/99bd179.htm.

53 See at http://www.comlaw.gov.au/ComLaw/Legislation/LegislativeInstrument1.nsf/all/search/466AAFC002CD2451CA256FD50028FBDF

54 See the Internet Industry Association's code of practice, which in art 1.6 provides that "*Under the Act ACMA has the power to investigate complaints relating to Prohibited Content or Potential Prohibited Content and to monitor compliance with the Code. Contravention of a requirement of the Code by a person covered by the Code may be the subject of a warning by ACMA or a direction by ACMA to that person to comply with the Code and, if a direction by ACMA is not complied with, enforcement action by ACMA and imposition of penalties pursuant to Part 6 of Schedule 7 of the Act.*" See the full content of the code available at http://www.iia.net.au/images/content_services_code_registration_version_1.0.pdf. If instead the content is located on a foreign server, then the ACMA notifies the website to the filtering software producers in order for them to include the site into their block lists.

After the first trial run of such a filtering system, however, many problematic issues have been raised from scholars and civil society, such as the lack of transparency and accountability of the system, as well as the technological drawbacks both on ISPs and final users.

Looking at the type of regulatory intervention that has been proposed by Australian government, it is clear that in this case the target of the regulation are the network intermediaries, i.e. the ISPs, which are not only encouraged,[55] but required to block (filter) the access to particular types of material.[56] This shift in the definition of the responsible bodies for control over users' behaviour is based on the technical construction of the information flow in the online world. As a matter of fact, ISPs serve as a link between the user and the Internet at large, not only passing information packets along the technical infrastructure, but also hosting content that is placed on their servers by others.[57] Putting legal liability on such intermediaries, thus, could overcome the practical problems that governments have in targeting the unlawful behaviour of individual actors online, due to the fact that the latter could nullify the advantage of regulatory arbitrage by moving their operations to more favourable jurisdictions.[58]

However, such a solution would have significant drawbacks, given that the filtering mechanisms could be opaque in their application by intermediaries (where it may not be clear to the end user that material is being blocked, or by whom)[59] and it would push the intermediaries to overblock content available online in order to avoid possible liability.[60] Many authors have emphasised that this approach could provide incentives to intermediaries to act as 'proxy censors', whose "*dominant incentive is to protect themselves from sanctions, rather than to protect the target from censorship*".[61] Moreover, in the analysed case the government regulation also involves practical choices that are relevant in the appraisal of some of the constituency of legitimacy, namely the already mentioned dimension of transparency of filtering choices, and the accountability issue.

Concerning transparency, the program seems to have numerous flaws, as it does not include any chance to disclose the blocked websites that can be justified under a different rationale,[62] and it does not provide a set of criteria to help understand which types of content should be blocked in addition to

---

55 See the case of the Finnish government, that has encouraged ISPs to implement a "voluntary" system that blocks access to secret list maintained by the police of IP addresses hosting websites suspected to contain child pornography. See W. Lehdonvirta, "Finnish ISPs must voluntarily block access", 2006, available at http://www.edri.org/edrigram/number3.18/censorshipFinland.

56 See the more general analysis on this approach by J. Zittrain, "Internet Points of Control", Boston College Law Review 44 (2003), p. 653

57 See that in this case the definition would be of Online service providers, which could include not only telecommunication services but also search engines, etc. See the deeper analysis provided by E. Laidlaw, "A framework for identifying Internet information gatekeepers", International Review of Law, Computers & Technology, (2010), p. 263.

58 T.J. McIntyre, "Internet Filtering: Implications of the "Cleanfeed" System", available at http://www.law.ed.ac.uk/file_download/communities/245_tj%20macintyre%20-%20internet%20filtering-%20implications%20of%20the%20cleanfeed%20system.pdf.

59 See C. Scott and T.J. McIntyre, "Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility", in R. Brownsword and K. Yeung, *Regulating Technologies – Legal futures, Regulatory Frames, and Technological Fixes*, Hart Publishing, 2008, part. at p. 118 ff.

60 See in this sense the choice adopted by the European legislator in terms of liability of Internet service providers within the E-commerce directive, where their role could be framed in terms of mere conduit, caching and/or hosting providers (artt. 12-15 dir. 2000/31/EC). On this point see L. Edwards, "The Fall and Rise of Intermediary Liability Online", in L. Edwards and C. Waelde (eds), *Law and the Internet*, Hart Publishing, 3rd ed., 2009, p. 47.

61 S. Kreimer, "Censorship by Proxy: The First Amendment, Internet Intermediaries and the Problem of the Weakest Link" (2006) 155 University of Pennsylvania Law Review, p. 28. But see also C. Scott and T.J. McIntyre, "Internet Filtering", cit.; L. Edwards, "Pornography, Censorship and the Internet", in Endwards and Waelde, Law and the Internet, cit., p. 623; I. Brown, "Internet censorship: be careful what you ask for", in S. Kirca and L. Hanson, (eds), Freedom and Prejudice: approaches to media and culture, Bahcesehir University Press, 2008, p. 74.

62 For instance, the disclosure of the list could provide a road-map for pedophiles.

child pornography. As a matter of fact, the government did not (and still does not) clarify the policy goal of this regulatory intervention, which could extend the child protection rationale to a wider censorship over any online content, for instance a pro-suicide website, online gaming, etc.

Concerning accountability, the problems appear because the government, on the one hand, proposes to expand the ACMA's block list by adding items selected and classified by foreign comparable entities (such as the Internet Watch Foundation) and, on the other hand, chooses to select the filtering software from among existing products available on the market. Both decisions could have a negative effect on accountability, as foreign entities would not be subject to Australian law but could effectively decide what Internet material is off-limits in the country. Moreover, using existing technology could confer significant power on the entities designing such software, without including in the governmental program any *ex ante* control over producers' technical choices.[63]

5.2. Command & control in the United States

The Federal Trade Commission (FTC) report concerning the risks entailed in current online marketing practices, in particular those directed towards children, which dates back to 1998, was the document that woke up U.S. policymakers in relation to the threats to minors' privacy when surfing online.[64] Evidence of concealed data collection practices presented by the report provided background for approval of the Children's Online Privacy Protection Act (hereinafter, COPPA)[65] by the U.S. Congress.[66]

COPPA works under specific age constraints, as it applies to commercial websites and online services targeting children aged 13 and under, as well as to general websites with actual knowledge that they may be collecting data from children aged under 13, though this last definition is far from being clear.

Under this regulation, collection of data from children includes data submitted directly from sources such as message boards and chat rooms as well as data received passively from devices such as online cookies.[67] The regulation imposes a general prohibition on websites to sell, release, or in any way share children's personal information with a third party, and also make such information publicly available online. Moreover, the regulation – replicating one of the so called Fair Information Principles (FIPs)[68] applicable to any data treatment – requires websites to provide effective notice as to

---

63 See D. Bambauer, "Filtering in Oz", cit., where the Author clarifies that "*If filtering is implemented based on software vendors' decisions about whether content is sexually explicit, rather than on the Classification Board's judgments, this will decrease the Australian citizens' ability to have a voice in what they can access on-line*.", at p. 28.

64 Federal Trade Commission, *Privacy Online: A Report to Congress*, Federal Trade Commisision, June 1998; and also the previous report of Center for Media Education, *The Web of Deception*, Center for Media Education, March 1996, which documented the marketing and data collection practices targeted at children on the Internet.

65 15 U.S.C. § 6501–6506 (Pub.L. 105-277, 112 Stat. 2581-728, enacted October 21, 1998). See Garber, "COPPA: Protecting children's personal information on the Internet", Journal of Law and Policy, 2001, p. 129. For a more detailed analysis of the policy making behind the enactment of COPPA, see K. Montgomery, *Going digital*, cit. p. 67 ff.

66 See that the COPPA is the statutory act that provides the delegation of authority from Congress to the administrative agency, the Federal Trade Commission. The latter enacted then the Children's Online Privacy Protection Rule which enforcement actions are brought and fines for non-compliance may be levied. As the FTC is an administrative agency, before it could implement a children's privacy protection law that carried the force and effect of law, Congress needed to pass a statute granting authority. See J. Hiller *et al.*, "Pocket Protection", 45 Am. Bus. L.J., (2008), p. 429 .

67 Examples of personal information include first and last name, home address, e-mail or any other online contact information, phone number, social security number, or the combination of a photograph of an individual coupled with the person's last name. See 16 C.F.R. § 312.2 (2009).

68 U.S. FTC, P*rivacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress*, United States (U.S.) Federal Trade Commission (FTC), May 2000, available at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

its data use and collection policies with regard to children. Parents should be informed of what the website owners intend to do with the information and whether or not they intend to disclose the personal information of their children to third parties. In order to improve the level of protection, the text of the regulation outlines specifies as to when such notice will be deemed proper.[69]

One of the important additional conditions imposed by the COPPA is the obligation for websites to create a system that could allow parents to provide their (verifiable) consent to the data treatment (opt-in system). The website must take reasonable steps to ensure that the parent receives notice of the willingness of his or her child to access a website which asks for personal data, such as name, address, city code, etc., and at that point the parent should give consent to access and, consequently, to the data treatment.[70]

However, the obligation of parental consent should be evaluated and the verification tools should be proportional to the type of data treatment (as 'sliding scale' of consent)[71], because exceptions are included in the regulation. For instance, until 2002, the FTC interpreted the verifiability of parental consent as, "*if the operator uses the information for internal purposes, a less rigorous method of consent is required. If the operator discloses the information to others, the situation presents greater dangers to children, and a more reliable method of consent is required*".[72] Accordingly, the FTC assumed that placing children under surveillance while they play and collecting their personal information in order to market products to them is inherently benign and poses only a slight risk of harm.[73]

Recent developments of the regulation focus on this point. Current public consultations, in particular, ask for opinions on additional technological methods to obtain verifiable parental consent that should be added to the COPPA Rule, on whether any of the methods currently included should be removed, and on what challenges operators face in authenticating parents.[74]

It should be added that in an effort to give websites additional incentives to comply with COPPA, the latter outlines "safe harbor" provisions, where a website operator will be in compliance with COPPA if it follows approved industry guidelines for self-regulation. Industry guidelines must be pre-approved by the FTC before receiving safe harbor protections.[75] To be approved by the FTC, participants must maintain self-regulatory guidelines including:

---

69 For example, such policies must be posted in links that are "clearly labeled" and placed in a "clear and prominent place and manner" on the home page. The policy must contain information specifically stating the contact information of website operators collecting and maintaining information, whether the information is disclosed to third parties, and how such information is used. See 16 C.F.R. § 312.4 (b). On the use and importance of privacy policies in children's websites see F. Casarosa, "Privacy policy improvements to protect children privacy", forthcoming in C. Akrivopoulou, and A. Psygkas, *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, IGI Global.

70 Several are the proposed mechanisms for obtaining such consent, in light of available technology. Some suggested methods include: providing a consent form to be signed by parents and then returned to website operators by fax; requiring a parent to use a credit card in a transaction, with the reasoning that children under the age of thirteen do not have access to credit cards; having a parent call a toll-free number staffed by personnel trained to recognize voice difference between children and adults; and using digital certificates based on available technology to verify age. See 16 C.F.R. § 312.5 (b)(2).

71 L. Matecki, "Update: COPPA is ineffective legislation! Next steps for protecting youth privacy rights in the social networking era", Northwestern Journal of Law & Social Policy, 2010, 377.

72 See the FTC Guidelines, available at http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus45.shtm.

73 See on this point I. Kerr and V. Steeves, "Virtual Playgrounds and Buddybots: a data-minefield for tinys & tweeneys", available at http://www.idtrail.org/files/Kerr_Steeves_Virtual_Playgrounds.pdf, p. 14.

74 See the Federal Register notice at http://www.ftc.gov/opa/2010/03/coppa.shtm.

75 Four organizations have been approved under this safe harbor provision: the Children's Advertising Review Unit, (Better Business Bureau); E.S.R.B. Privacy Online, (Entertainment Software Ratings Board); TRUSTe; and Privo Inc. See FTC, Safe Harbor Program Application, http:// www.ftc.gov/privacy/privacyinitiatives/childrens_shp.html.

- a requirement that participants in the safe harbor program implement substantially similar requirements that provide the same or greater protections for children as those contained in the regulation;
- an effective, mandatory mechanism for the independent assessment of safe harbor program participants' compliance with the guidelines; and
- effective incentives for safe harbor program participants' compliance with such guidelines.

In this sense, the initial heading of this paragraph should be distinguished from the former case of Australian regulation, as the regulatory strategy of the U.S. government (*rectius* of the FTC) opens the way also to ex post recognised self-regulation. This could increase the actors participating in the regulatory chain, and effectively increase the level of compliance with the public regulation, where the private regulators (i.e. the drafters on the industry guidelines) could be in charge of internal monitoring concerning the application of the approved guidelines.

In general, COPPA, as currently implemented, has been positively evaluated in its efficacy by its own enforcer, the FTC.[76] Its goals of encouraging and enhancing parental involvement in children's online activities and limiting the collection of personal information from children under 13, has been judged as reasonably achieved, although only a limited number of studies have explored the level of compliance to COPPA[77] and the figures from non-governmental research are still lower than the acceptable level. The most relevant weaknesses of the COPPA regime are the age verification tools and the ambiguity that is still present in the scope of application of the regulation, in particular with the difficulty of circumscribing the grey area of websites not primarily directed towards children. Concerning the former point, it should be noted that the mechanisms provided by the COPPA in order to grant parents' consent are clearly not foolproof, as it is possible that younger people, between 11 and 13 years of age and sufficiently tech savvy, could easily circumvent the obligation, accessing adult sites without their parents' knowledge, or consent. However, this is a fundamental technical difficulty which website operators need to face in the online environment.[78]

5.3. Self-regulation in the EU: IAP initiatives

The protection of children online has become an EU priority in the last decade and, since the ratification of the EU's Lisbon Treaty in November 2009,[79] legislators have enjoyed greater power to write laws on criminal enforcement and sanctions, which has fed into policymaking to combat child pornography on the Internet in particular.[80] However, this has been a change from the previous regulatory strategy based mostly on private regulation.

---

[76] In 2007, the Commission found that no changes were necessary to COPPA because it had been "*effective in helping to protect the privacy and safety of young children online*". FTC, *Implementing the Children's Online Privacy Protection Act: A Report to Congress*, 2007, available at http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf.

[77] X. Cai, and W. Gantz, "Online privacy issues associated with Web sites for children", Journal of Broadcasting & Electronic Media, 2000, 44, 197–214; X. Cai, W. Gantz, N. Schwartz, and X. Wang, "Children's Web site adherence to the FTC's online privacy protection rule", Journal of Applied Communication Research, 2003, 31, 346–362. See also the FTC study, *Protecting children's privacy under COPPA: A survey on compliance*, 2002, available at http://www.ftc.gov/os/2002/04/coppasurvey.pdf.

[78] However, in many cases websites, such as Facebook and MySpace, take down profiles of underage users when notified that they might be underage. See, e.g., Facebook.com Report an Underage Child, www.facebook.com/help/contact.php?show_form=underage; MySpace.com, How do you report underage MySpace users? http://faq.myspace.com/app/answers/detail/a_id/35.

[79] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJEU 2007/C 306/01, available also at http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:306:SOM:EN:HTML.

[80] Proposal for a Directive on combating the sexual abuse and sexual exploitation of children, and child pornography, repealing Framework Decision 2004/68/JHA, Brussels, 29th March 2010, COM(2010)94 final.

As a matter of fact, the milestones of EU intervention in child protection date back to 1999, when the EU adopted the first of a still running series of multi-annual action plans in order to promote safer use of the Internet for children.[81] The initial IAP actions identified areas for concrete measures where Community resources should be focused. Since 1999, the Action Plan has been extended and widened in its scope twice[82] in order to take into account "*currently unknown future developments in the on-line environment as the resulting threats will become increasingly important in the years ahead*".[83]

The IAP actions are included in 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 solutions. This option is not only due to the fact that coordinated private regulation can have a higher level of flexibility and can better fit with the needs of an ever-changing environment, but also because of 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*".[84]

The more recent IAP action defines four specific objectives: the promotion of a safer environment through a network of hotlines 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 coordination with other similar international initiatives. In particular, the public awareness-raising action is framed to encompass better 'user-empowerment' not only for parents and caregivers, but also for children and young people, and to stimulate stakeholders to take responsibility, cooperate and exchange experience and best practice at a European and international level.

Among the various initiatives, the most recent intervention is the adoption of the Safer Social Networking Principles.[85] These principles were developed by social networking sites in consultation with the European Commission (which acted as a facilitator) and a number of NGOs involved in child welfare, in order to provide good practice recommendations for the providers of social networking and other user interactive sites, so as to enhance the safety of children and young people using their services.

The signatories include different types of companies involved in the provision of social networking services online. They vary both in terms of establishment, including also US-based companies, and in

---

81 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).

82 See the European Commission, *Communication 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).

83 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.

84 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.

85 The text of the seven principles is available at http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf. See that a similar process was used in 2007 to draft and collect the participation of Mobile service providers for the "*European Framework for Safer Mobile Use by Younger Teenagers and Children*", which describes principles and measures that signatories committed to implement on the national level throughout Europe, to ensure the safety of young mobile users. See more at http://ec.europa.eu/information_society/activities/sip/self_reg/phones/index_en.htm

terms of numbers of users. Moreover, also video sharing platforms, online gaming consoles and blogging sites are signatories to the principles.[86]

The Principles cover both technical and informational issues that could limit online risks for children and young people. The measures listed in the text include, for instance, having minors' profiles visible only to their approved list of contacts by default; making minors' profiles non-searchable via common search engines; making privacy options prominent and accessible at all times, etc. All signatories to the Principles have sent the Commission a self-declaration in which they demonstrate how these Principles are implemented within their services.

In order to verify compliance with the principles, the European Commission followed all the steps of their implementation by the signatories and published a first assessment report[87] in February 2010, which not only took into account the self-declarations of the signatories vis-à-vis the principles, but also tested the sites from a user perspective, in order to measure effectively the level of compliance with the Principles.

The findings of the assessment show that most of these companies have taken action and empowered minors by making it easier to change privacy settings, block users or delete unwanted comments and content. Yet more needs to be done since only 40% of the companies make profiles of under 18 years old users visible by default only to their approved list of contacts, and only eleven service providers make minors' profiles non-searchable in common search engines. In addition, only nine service providers responded to a request for help sent by the testers. The assessment process showed that in general all social networking sites signatory to the Principles are on board in this exercise. Some of them have announced that they have implemented or are considering implementing changes on their websites following the individual results of the assessment.

In this case the importance of the European institution involvement can be perceived at a double level: on the one hand, in terms of standard setting; and on the other, in terms of enforcement.

Concerning the former, it should be noted that the involvement of the European institution was qualified as a facilitator role, providing the venue and the forum in which the social networking sites could meet and draft the rules. Although such a statement is also included in the final document of the Safer Social Networking Principles, this case cannot fall into the category of pure self-regulation as such, instead it could be framed as a peculiar form of approved self-regulation, where the standard setting activity was constantly monitored (and eventually steered) in order to achieve a result that would be in line with the public policy objectives.

Moreover, such involvement could have an effect also on the enforcement phase, as the participation of the public actor could provide additional compliance incentives, which are combined with the existing ones already available in the case of self-regulatory initiatives.[88] In particular, reputation mechanisms could have positive effect when coupled with public disclosure of non-compliance, or with threat of legal sanctions. At the moment, however, the content of the Principles does not include any provision concerning the enforcement of the rules, and consequently no sanctions are provided against parties in breach.

---

86 See the list of signatories at http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm.

87 See Staksrud, and Lobe, *Evaluation of the implementation of the Safer Social Networking Principles for the EU*, European Commission Safer Internet Programme, Luxembourg, 2010, available at http://ec.europa.eu/information_society/activities/social_networking/eu_action/implementation_princip/index_en.htm#final_report.

88 On the definition and boundaries of the self- and co-regulatory regimes see C. Marsden, 'Internet governance and law: co-regulation as a constitutional solution?', presentation given at the Third Biennial Conference of the ECPR Standing Group, Dublin, 17-19 June 2010, on file by the Author.

5.4. Co-regulation in the UK : the case of Internet Watch Foundation

During the second half of the nineties, the British government started to evaluate the opportunity to legislate on child pornography in order to limit the increased distribution of such materials in the UK. The intervention was interpreted also as a shield from the UK ISP being "abused through the posting and hosting of illegal child abuse images",[89] requiring their participation and involvement in the recognition and identification of distributors of illegal material. The debate between the government and the industry resulted in an agreement concerning the voluntary obligations that ISPs could be charged of concerning the reporting and blocking of specific types of materials made available through their services.

The so-called "R3 Safety Net agreement"[90] included the Safety Net Foundation as a member, a charitable foundation that was subsequently renamed the Internet Watch Foundation (IWF). This organization was founded by the industry to provide an online reporting mechanism for content that was alleged to be illegal. In particular, the IWF "*works in partnership with the Government to provide a 'hotline' for individuals or organizations to report potentially illegal content and then to assess and judge that material on behalf of UK law enforcement agencies. It also exists to assist service providers to avoid abuse of their systems by distributors of child abuse content and to support law enforcement officers, at home and abroad, to detect and prosecute offenders*".[91] The importance of the role of IWF is also supported by the acknowledgment that "[r]*eports made to the IWF in line with its procedures will be accepted as a report to a relevant authority*".[92]

The scope of IWF activities are limited, concerning limited types of content (essentially child pornography, obscenity and hate speech).[93] Moreover, the IWF offers services to its members aimed at facilitating ISPs in identifying illegal material. In particular, it provides:

- URL Lists of child sexual abuse content, which are reviewed and monitored;[94]
- Keyword Service, by which certain members are provided with a list of keywords often used by people who discuss illegal acts with children;
- Newsgroup Service designed to combat pedophile content in newsgroups;[95]
- Spam alert
- Best Practice Guide.[96]

Concerning enforcement, the hotline depends on individual reports of potentially illegal material being made. As soon as the IWF receives a notification, it evaluates whether a URL containing potentially

---

89 See C. Marsden, S. Simmons, I. Brown, L. Woods, A. Peake, N. Robinson, S. Hoorens, and L. Klautzer, *Options for and Effectiveness of Internet Self- and Co-Regulation Phase 2: Case Study Report*, prepared for European Commission DG Information Society & Media, 2008, available at SSRN: http://ssrn.com/abstract=1281374.

90 Internet Service Providers Association, LINX, and Safety Net Foundation, "R3 Safety Net Agreement", September 23rd 1996, available at http://www.mit.edu/activities/safe/labeling/r3.htm, where the three 'R' referred to approach taken by the agreement on rating, reporting and responsibility.

91 See the Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003, 6th October 2004, available at http://www.iwf.org.uk/documents/20041015_mou_final_oct_2004.pdf.

92 Ibidem, p. 6.

93 It does not cover issues such as pedophile conversations intended to persuade children to engage in illegal sexual acts (grooming), nor the IWW covers peer-to-peer services, online games, 'happy-slapping' and torture websites. See more at http://www.iwf.org.uk/public/page.35.htm.

94 The lists include every URL that depicts indecent images of children, advertisements for or links to such content. The list is updated twice a day to ensure all entries are live. See at http://www.iwf.org.uk/corporate/page.49.626.htm.

95 See at http://www.iwf.org.uk/corporate/page.49.231.htm.

96 See at http://www.iwf.org.uk/documents/20060911_iwf_best_practice_guide_final_110906ln.pdf.

criminal child sexual abuse content should be added or not to the aforementioned URL List. When the IWF believes a given material would be capable of sustaining a criminal prosecution if it were to be put before a jury, it can issue a notice to the ISPs in order to remove the content from their servers or disable access to it.[97] ISP members of the IWF should then comply with the notice and take down procedure, because a failure to comply with the code of practice could result in a formal warning and a report to the relevant law enforcement authorities.[98] Otherwise, ISPs should make representations to explain why a notice has not been complied with, specifically, if they believe that there has been an error in the notice.

The decision of the IWF, however, is not irrevocable, as it is possible to appeal against the accuracy of the assessment by any party with a legitimate association with the content, which includes also any user that has been prevented from accessing legal content.[99] The process then includes a re-assessment phase by the IWF and, if the IWF decision is not reversed, the final decision concerning the illegal nature of the content is then taken by the lead policy agency. The decision is final because the IWF must act in accordance with it.[100]

Despite the positive evaluation of the overall activity of the IWF, this case of co-regulation has raised criticism concerning the legitimacy of the Internet filtering system,[101] emphasized also by recent cases of questionable blocking.[102] In particular, the delegation to private parties of gate-keeping activity could entail an issue with the involvement and application, within the private sphere, of fundamental values, such as freedom of expression. As a matter of fact, art. 10 of the European Convention of Human Rights provides for restrictions on the exercise of the right to freedom of expression only in instances when such restrictions are 'prescribed by law'. Elements of this legislative basis lacking any limitation may qualify as illegitimate censorship. The IWF could face this issue as the legislation concerning child protection, the Protection of Children Act 1978[103] does not include any reference to mandatory filtering. Moreover, the role of IWF descends from the aforementioned 3R Agreement and from a subsequent memorandum of understanding with the Crown Prosecution Service and the Association of Chief Police Officers (ACPO) linked to Section 46 of the Sexual Offences Act 2003, and again none of these documents make an indirect reference to respect of freedom of expression.[104]

Recent research, however, has acknowledged the need to revise the concept of legitimacy in order to take a more pragmatic and empirical approach, where the appraisal of the legitimacy is measured

---

97 Art. 1 of the IWF Funding Council Code of Practice for Notice and Takedown of UK Hosted Content Within the IWF Remit (hereinafter IWF Code of Practice) available at http://www.iwf.org.uk/funding/page.60.htm.

98 Art. 9 of the IWF Code of Practice, cited.

99 See at http://www.iwf.org.uk/corporate/page.49.625.htm.

100 See the Content assessment appeal process at http://www.iwf.org.uk/documents/20100421_content_assessment_appeal_process.pdf.

101 L. Edwards, 'From Child Porn to China, in One Cleanfeed', Script-ed, 2006, 3 (3), available at http://www.law.ed.ac.uk/ahrc/SCRIPT-ed/vol3-3/editorial.asp; more generally on filtering techniques C. Marsden, *Net Neutrality: Towards a co-regulatory solution*, Bloomsbury Academic, 2010, at p. 118.

102 The most notable case was the one that involved a Wikipedia page containing the cover image of a music album, see more at http://en.wikipedia.org/wiki/Wikipedia:IWF.

103 See at http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1978/cukpga_19780037_en_1.

104 See that the 3R Agreement clearly excludes the involvement of free speech concerns as "*The issue addressed has nothing to do with censorship of legal material or free speech. The issue is how to deal with material or activity which society, through democratic process, has deemed to be unacceptable in law. The core issue is crime. Legal, but possibly offensive, material raises a quite separate issue. Here consumers should have the technological means to tailor the nature of their, or their family's, experience on the Internet according to their individual standards; thus supporting both individual responsibility and the Internet's traditions of diversity and free speech.*" See "R3 Safety Net Agreement", cit.

according to the differing viewpoints that government, ISPs and users have of the filtering system.[105] In particular, this reasoning takes into account the fact that the IWF and its filtering system are regarded as legitimate by many observers, and particularly by ISPs, which are voluntarily adhering to the system and complying with the blocking decisions.[106]

6. Regulatory approaches for the protection of minors online

The previous cases show different hypothesis of Internet regulation with regard to the protection of minors. However, it should be emphasised that such case studies need to take into account the different legal systems they are embedded in, as well as methods, traditions and cultural characteristics. The current level of analysis does not provide such a depth of comparative evaluation among the different experiences; nonetheless, it allows us to learn more about how the regulatory strategies are selected, and the interactions of the different regulatory tools used in each case.

A clear element is the fact that each of the previous cases has raised debates and, on some occasions, strong reactions by academia and civil society. This should not be interpreted as a failure of private and public regulation, regardless their practical effectiveness. As a matter of fact, any regulatory approach on the issues identified above can end up generating criticism due to the sensitivity of the potential victims and difficulties in balancing the conflicting interests. The previous examples show that private regulation and direct state intervention can generate similar criticism under different circumstances, such as legitimacy and enforcement.

However, most scholars acknowledge that private regulation can provide better results in terms of effectiveness, whether or not it is coupled with the guidance of governmental actors (be they at a national, supranational or international level).[107] This solution is better equipped to solve the difficulties of the other regulatory approaches, in particular the difficulties in reaching international agreement on common definitions of abuse, technical and legal enforcement by single national governments, and limitation to governmental intervention due to constitutional boundaries (such as conflicting rights, or, in the case of EU, the subsidiarity principle).

Nonetheless, the previous analysis highlights the key issues that should be taken into account when defining the regulatory strategy.

a. Objective pursued.

The different approaches described above showed that it is very difficult, if not impossible to provide a 'one size fits all' solution in order to achieve a sufficient level of protection for minors when browsing online. This is not only related to the fact that different risks can be estimated as different regulatory priorities, but also due to the fact that the underlying children's rights to be protected can conflict with other rights, such as in the case of harmful content. Thus, the type of objectives that the regulation pursues can limit the regulatory options available, and eventually hinder the effectiveness of the type of regulation chosen.

---

[105] See T.J. McIntyre, "Balancing regulatory effectiveness and legitimacy? An examination of Internet filtering in United Kingdom", presentation given at the Third Biennial Conference of the ECPR Standing Group, Dublin, 17-19 June 2010, on file by the Author.

[106] See approach relies mainly on the literature heading to J. Black, "Legitimacy and the competition for the Regulatory State", LSE Legal Studies Working Paper No. 14/2009, available at SSRN: http://ssrn.com/abstract=1424654.

[107] See F. Cafaggi, "Private Regulation in European law", EUI w.p. 2009/31, private regulation series n. 1, available at http://privateregulation.eu; see also the papers collected in F. Cafaggi, (Ed.) *Reframing self-regulation* in *European private law*, Kluwer, 2006.

b. Fairness.

Fairness should look at the subject-matter and at the results of the regulatory strategy adopted, and in particular, where private regulation is at work, equality and non-discrimination should be safeguarded. Given that protection of minors online is a complex matter where a balance of fundamental rights is crucial, an involvement of the public actor could be positively evaluated.

c. Transparency.

Though it is usually mentioned with reference to the drafting techniques of private regulation, transparency is an issue for both public and private regulation, as the Australian case showed. As a matter of fact, transparency can affect the trustworthiness of regulation in the eyes of the regulatees: given that when the rules are opaque or based on obscure criteria they would be less trusted and hence not readily followed. In case of private regulation, lack of transparency would also hinder the wider adoption of the standard, as new market actors will not be willing to comply with rules that do not provide sufficient consistency and coherence.[108]

d. Enforcement

Any regulatory intervention aims at ensuring a sufficient level of compliance through different mechanisms, and in particular, at establishing an adequate enforcement system. In case of private regulation, however, the mere creation of rules does not make the regulatees accountable for complying with such rules; thus, various additional instruments could be considered in order to improve accountability and verify compliance, such as monitoring committees and complaint-handling and dispute resolution mechanisms.[109] In self-regulatory initiatives, for instance the regulators could be responsible for the standard setting and for the enforcement process, either by imposing sanctions – mostly reputational ones – or by labelling, or also by rating mechanisms.[110] In the specific case of protection of minors online, however, the low level of effectiveness that is usually ascribed to such sanctioning systems could trigger a more active participation of public actors in this phase of the regulatory process, providing the means, power and authority to enforce the norms that private regulators do not possess.

The points raised above could provide a set of indicators and suggestions in order to define in a more effective way the regulatory approaches that could be framed in the specific case of protection of minors surfing online. However, total risk elimination through regulation alone is no more possible online than anywhere else in childhood, but efforts to provide a safer environment should continue to be pursued.

---

[108] Though this does not impose on such rules to achieve the level of legal certainty of public regulation.

[109] See that in order to improve compliance it could be also useful to increase the inclusiveness of the regulatory process, as "*the more involved all stakeholders are in drafting self-regulatory regimes, the better incentive they have to comply with the rules*". See E.-J. Koops *et al.*, 'Should self-regulation be the starting point?', cit., p. 138.

[110] In a different context see the case of rating systems within the online auction websites, F. Casarosa, "Online Auction Sites: An Example of Regulation in Electronic Communities?", European Review of Private Law, 2009, 1; more generally on the enforcement mechanisms within transnational private regulation see F. Cafaggi, "New Foundations of Trasnational Private regulation", WP RSCAS 2010/53, Private regulation series n. 4.

Author Contacts:

Federica Casarosa

Law Department - European University Institute

Via Boccaccio 121

50133 Firenze

Italy

Email: federica.casarosa@eui.eu


European
University
Institute
European University Press