Regulation of children's online privacy: current status and regulatory choices

By Milda Macenaite (*ANR 621483*)

Tilburg University, the Netherlands
Tilburg Law School
Research Master in Law
Under the supervision of prof. dr. J.E.J. Prins
Second reviewer Prof. dr. Bert-Jaap Koops

1 August 2012

Table of contents

1. Introduction

The increasing use of online services by children and the constant development of these services pose new safety and privacy risks. Such risks include, amongst others, safety risks like cyberharassment, cyberbullying, grooming, "sexting", misuse of personal data, privacy-invasive commercial practices such as online profiling, behavioural monitoring and tracking. Future technological developments are likely to aggravate these risks and related harms. Policy makers, privacy advocates and parents are scrambling to deal with these new online developments and mitigate the risks in order to protect increasingly connected, ever younger children. Recently there has been a significant increase in attention and regulation focused on child safety and privacy issues online in the European Union (EU).[1] It appears poised to step up regulatory activity on this front through the modernisation of the EU data protection directive, which intends to bring data protection law up to speed with (the threats posed by) technological development.[2] Similar developments are reflected in the policy agenda across the Atlantic. The US Children's Online Privacy Protection Act (COPPA) is under revision and special initiatives, like the Do Not Track Kids Act 2011[3] and "Eraser Button"[4], are considered in order to improve children's online privacy protection.[5] Besides legislative approach, other forms of regulation, such as self- and co-regulation, technical tools, awareness and education are more and more often included into the policy mix.

This paper examines the current regulatory framework on international and EU levels. In particular, the focus is placed on exploring whether there is a tendency to address child privacy online in a manner appropriate to the specificity and vulnerability of the individuals at risk and which regulatory instruments (law, norms, market, or technology) appear to be favoured by regulators.

1.1 Aim of the paper

The aim of this paper is to analyse the current regulatory framework. This paper does not aim to present an exhaustive overview or a full representative synthesis of the existing regulatory instruments. The selected regulatory tools are mentioned here because they give the opportunity to reflect on the trends and priorities and the variety of approaches chosen by regulators to address the problem of children protection online.

The issue of the efficiency of the current regulation and its adequacy to address current privacy, contact and commercial risks remains outside the scope. It will hopefully become a subject of a further PhD research project of the author.

---

[1] Commission Communication on a "Better Internet for Children" (2.05.2012), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:EN:PDF. Coalition to make the Internet a better place for kids, Statement of purpose, at: http://ec.europa.eu/information_society/activities/sip/docs/ceo_coalition/ceo_coalition_statement.pdf
Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[2] European Commission. 2010. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, 4 November 2010, COM (2010) 609 final

[3] Markey. E. 2011. A Bill To amend the Children's Online Privacy Protection Act of 1998. At http://markey.house.gov/docs/dntk_legislation.pdf

[4] Ibid.

[5] Thierer, A. 2011. Kids, Privacy, Free Speech & the Internet- Finding the Right Balance. Working paper. At http://mercatus.org/sites/default/files/publication/Kids_Privacy_Free_Speech_and_the_Internet_Thierer_WP32.pdf boyd d., U. Gasser,

1.2 Theoretical embedding

This paper draws upon the main internet governance and technology regulation theories.[6] In particular, it is based on Lessig's idea that human behaviour can be regulated through four constraints, i.e., four different regulatory modalities.[7] These modalities are: the law, social norms, the market, and code or architecture.[8] This paper analyses which of these four modalities are present in the current regulatory framework and how they interact. In Lessig's words, it explores how the "net regulation" in the selected area is achieved "through the sum of the regulatory effects of the four modalities together" and how policy makers trade off among the four regulatory tools.[9]

The first modality, law, in this paper is interpreted in a broad sense. It embraces both command-and-control regulation and self-regulation. The concept of 'command-and-control' regulation may be equally called legislation, centred regulation, statutory legislation.[10] It indicates that "a public authority gaining its legitimacy from the political process issues orders to companies or individuals requiring them to meet public policy goals; the implication is that these orders are obeyed".[11] Self-regulation, in contrary, is understood as an alternative way to regulation by means of legislative acts.[12] For the purpose of this paper, self-regulation is defined as "the possibility for economic operators, social partners, non-governmental organisations or associations to adopt amongst themselves and for themselves guidelines at European level (particularly codes of practise or sectoral agreements)".[13] It is constituted of self-rule-making, self-jurisdiction and bindingness of rules, as well as self-enforcement through monitoring and supervision.[14] It should be acknowledged, though, that it could be claimed that self-regulation is a distinct constrain or modality, due to its major differences from command-and-control regulation in terms of legitimacy, regulating actors, effectiveness, and sanctioning. However, as the prevalent form of self-regulation in the ICT sector is co-regulation, the role of legislator is much more important in this area and, therefore, self-regulation will be included under the first regulatory modality. In this paper co-regulation is understood as "a kind of policy making with open negotiations between interested parties about the nature, the extent, and the seriousness

---

J. Palfrey. 2010. How the COPPA, as Implemented, Is Misinterpreted by the Public: A Research Perspective. The Berkman Center for Internet & Society Research Publication Series. At http://cyber.law.harvard.edu/publications

[6] Lessig. L. 1999. The Law of the Horse: What Cyberlaw Might Teach. 113 Harvard Law Review. Lessig, L. 1999. *Code and other laws of cyberspace,* New York, Basic books. Murray. A. 2006. *The Regulation of Cyberspace: Control in the Online Environment*, Routledge-Cavendish. 1 edition; Bonnici. M. G. P. 2008. *Self-Regulation in Cyberspace* (Information Technology and Law). Asser Press. 1st Edition; Brownsword. R. 2008. *Rights, Regulation, and the Technological Revolution*. Oxford: Oxford University Press. Koops B.J. et al. (eds). 2006. *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-liners*. Information Technology & Law Series. Vol. 9. Asser Press. *Levi-Faur, David (ed.). 2012. Handbook on the Politics of Regulation*, Edward Elgar Publishing. Baldwin, R., Scott, C. and Hood, C. (eds.) 1998. *A Reader on Regulation*: *Oxford Readings in Socio-Legal Studies*, Oxford: Oxford University Press. Black, J. 2001."Decentring regulation: The role of regulation and self regulation in a "Post Regulatory" world", Current Legal Problems 54: 103-146. Morgan, Bronwen and Yeung Karen. 2007. *An Introduction to Law and Regulation: Text and Materials*, Cambridge University Press. Ayres, Ian and Braithwaite, John. 1992. *Responsive regulation: transcending the deregulation debate*, Oxford, Oxford University Press. Braitwaite, John. 2002. *Restorative justice and responsive regulation*, Oxford, Oxford University Press.

[7] Lessig. L. 1999. The Law of the Horse: What Cyberlaw Might Teach. 113 Harvard Law Review, pp. 507-514; and Lessig, L. 1999. *Code and other laws of cyberspace,* New York, Basic books, Chapter 7.

[8] Murray and Scott have elaborated on these four modalities, reclassifying them accordingly as hierarachy, community, competition, and design.[8] See Andrew Muray and Collin Scott, „Controlling the New Media: Hybrid Responses to New Forms of Power", 2002, 65 *Modern Law Review,* 491. See too Murray. A. 2007. *The Regulation of Cyberspace.* Routledge-Cavendish.

[9] Lessig. L. 1999. The Law of the Horse: What Cyberlaw Might Teach. 113 Harvard Law Review, pp. 507-514;

[10] Bert-Jaap Koops et al. (eds). 2006. Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-liners. Information Technology & Law Series. Vol. 9. Asser Press, p. 120

[11] *Tony Prosser,* Self-regulation, Co-regulation and the Audio-Visual Media Services Directive, *Journal of Consumer Policy*, 2008, vol. 31, issue 1, p. 100.

[12] Bert-Jaap Koops et al. (eds). 2006. Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-liners. Information Technology & Law Series. Vol. 9. Asser Press, p. 109.

[13] Interinstitutional agreement on better law-making, 2003/C 321/01, *OJ C 321, 31.12.2003,* Recital 22.

[14] Idid., 120.

of certain problems and the directions and options for solutions".[15] It focuses on the cooperation between the private and public sectors, and refers to a mix of self-regulatory and regulatory solutions.

The second regulatory modality, social norms, is explained by Lessig as a "constrain through the stigma that a community imposes".[16] Such stigma, for example, may be created by the government through funding of public education or awareness campaigns, netiquette online, etc.

The third modality, market, constrains human behaviour through law regulating the market, e.g. providing subsidies to private companies, to provide incentives for certain type of behaviour via reduced rates or other financial means.

The fourth modality, code or architecture, refers to regulation by technology or techno-regulation.[17] Code, e.g. hardware or software, can embed certain features or values, as well as prohibit or make certain values impossible.[18] Defined as the use of technology to shape people's behavior, techno-regulation plays an increasingly important role in the internet governance.[19] Although technology by itself may constitute regulation[20], in the area of children's protection most often it is a part of a wider regulatory strategy.[21]

Given the above-mentioned classification, the current regulatory framework on children's privacy online will be discussed as indicated in the following table.

Table 1 – Regulatory framework according to four regulatory modalities

Law		**Social norms**	**Market**	**Code**
Command-and-control	*Self-regulation*			
- International treaties - Charter of Fundamental Rights of the European Union - Directive 95/46/EC - Directive 2002/58/EC - Proposal for a General Data Protection Regulation, COM (2012) 11 final	- Safer Social Networking Principles for the EU - FEDMA code of conduct and its online marketing Annex	- Safer Internet Programme (awareness raising) - European Strategy for a Better Internet for Children (education, empowerment, digital literacy)	-	- European Strategy for a Better Internet for Children (parental controls, privacy settings, age ratings, reporting tools, hotlines) - Coalition to make a better and safer internet for children (tools to report harmful content and contact, age-appropriate privacy settings, content classification, parental controls, tools to take down of child abuse material).

[15] Bert-Jaap Koops et al. (eds). 2006. Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-liners. Information Technology & Law Series. Vol. 9. Asser Press, p. 122.
[16] Lessig, L. 1999. *Code and other laws of cyberspace,* New York, Basic books, p. 88.
[17] Roger Brownsword, Karen Yeung (eds), Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes, Oxford, Hart Publishing, 2008, p. 7.
[18] Lessig, L. 1999. *Code and other laws of cyberspace,* New York, Basic books, p. 89.
[19] Bert-Jaap Koops, The (In)Flexibility of Techno-regulation and the Case of Purpose Binding, Legisprudence, Vol. 5, No. 2, p. 174.
[20] Lessig Lawrence, The Code is the Law, The Industry Standard, 9 April 1999, at: http://www.lessig.org/content/standard/0,1902,4165,00.html.
[21] Eva Lievens, Protecting Children in the Digital Era: The Use of Alternative Regulatory Instruments, Martinus Nijhoff Publishers, Leiden/Boston, 2010, pp.231-232.

1.3 Structure of the paper

The paper is structured in the following way. Based on empirical research, Section 2 of the paper summarizes the online child safety and privacy risks, and explains the relationship between them. Section 3 discusses the right of children to privacy by examining its history, current interpretation of the right in international law and development in relevant case law of the European Court of Human rights (ECHR). Section 4 reviews regulatory developments in the EU and discusses the types of chosen regulation and how they will affect the future development of children's privacy online. Section 5 looks into the EU self-regulatory efforts, and Sections 6 and 7 accordingly explore these efforts under the remaining regulatory modalities, namely social norms, market and code (or architecture). Section 8 draws final conclusions dealing with the above-mentioned aims of the paper, i.e., the section discusses whether the current regulatory framework addresses specifically child privacy online issues and through which regulatory instruments.

2. Setting the stage: online child safety and privacy

Current youths are characterised as 'digital natives'[22] or the 'Net generation'[23] due to their immersion in ICT and extensive usage of digital tools. Digital natives are claimed to live more and more online and to be constantly connected.[24] Recent research demonstrates that internet is completely embedded in youth's daily lives: 93% of 9-16 year olds go online at least weekly and 60% almost every day. The age of internet users is becoming ever younger. On average, European children start using the internet when they are seven.[25] The range of their online activities is wide, from the use of the internet for school work (85%), to generating internet content (76%), communicating online (62%).[26]

Next to advantages of socialisation, convenience, and fun, there are also concerns about the safety and privacy, as they increase online risks and victimisation of youths in a number of ways.[27] In the framework of this paper, three groups of risks are relevant: privacy risks, contact risks and commercial risks. Most of these risks impact individuals more generally, but there are particular concerns about children as internet users. Children are often more easily misled and less proficient in seeing through (potentially) awkward and perilous situations. Moreover, particularly during adolescence, risk-taking behaviour increases and, hence, so do online risks.[28]

[22] Prenksy, M. 2001. Digital Natives, Digital Immigrants. On the Horizon, 9, 5, 1–6.
[23] Tapscott, D. 1998. Growing up digital: the rise of the Net generation. New York: McGraw-Hill.
[24] Van Kokswijk describes this constant interconnection between the online and offline worlds as "interreality", defining this concept as a "mix of the virtual and physical realities into a hybrid total experience". Cf. Van Kokswijk, J. 2007. *Digital Ego: Social and Legal Aspects of Virtual Identity*. Delft: Eburon Uitgeverij. p. 40.
[25] Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. 2011. Risks and safety on the internet: The perspective of European children. Full Findings. LSE, London: EU Kids Online.
[26] Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children. Full Findings. LSE, London: EU Kids Online.
[27] Livingstone, Sonia and Haddon, Leslie and Görzig, Anke, eds. (2012) *Children, risk and safety on the internet: research and policy challenges in comparative perspective*. Policy Press, Bristol.
[28] Livingstone. S. 2009. Children and the Internet: Great Expectations, Challenging Realities. Cambridge: Polity;

2.1 Contact risks

Recent research indicates that the main risks pertaining to children's safety as internet users are contact risks, i.e. when the child participates or creates a risky online interaction. [29] These risks can, amongst others, be identity theft, fraud, cyberharassment, cyberbullying, grooming, and "sexting". For example, EU Kids Online survey demonstrated that 30% of 9-16 year old Europeans communicated with strangers online (a phenomenon which may easily lead to cyberharassment), 6% of 9-16 year olds were victims of cyberbullying, 15% of children aged 11-16 have seen or received sexual messages online.[30] Recent research in the US showed that child identity theft is much more prevalent than adult identity theft. In 2011, children were targeted by identity thieves 35 times more often than adults.[31]

Cyberharassment seems to be the most widespread contact risk encountered by children on the internet. Accordingly, it is a growing area of concern for EU policy makers. The latest Safer Internet Programme,[32] for example, particularly focuses on harmful online conduct, such as cyberbullying and grooming.

Cyberharassment may vary from intimidation, embarrassment and humiliation to serious threat and harm. One form of harassment is cyberbullying, which in essence, means "psychologically devastating form of social cruelty among adolescents" experienced via the means of electronic media and ICT.[33] The content of cyberbullying includes aggressive harassment and threats related to physical, sexual violence or dissemination of humiliating statements to others, often based on a power imbalance between the bully and the bullied.[34] In can be a form of technological attack on a bullied person, such as hacking into his e-mail account, online profile or blog, sending of offending messages in his name, or creation of a defamatory internet website.[35] Not less frequent practise of cyber-bullying is dissemination of personal information or video clips of a bullied person without his consent. Another phenomenon of this type, ironically called as "happy slapping", refers to recording of a physical attack (most often via mobile devices) and uploading the video online.[36] Another form of cyberbullying is called "flaming", denoting an intense and aggressive dispute via e-mail or instant messages. Most of the time cyber-bullying is a form of violence inflicted on minors by

---

Hope. A. 2007. Risk-taking, boundary-performance and intentional school internet 'misuse.' Discourse: studies in the cultural politics of education, 28(1), pp. 87-99.

[29] Hasebrink, U., Livingstone, S., Haddon, L. (2008) *Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online*. London: EU Kids Online (Deliverable D3.2) available at: http://www.gobernanzainternet.es/doc/archivos/EUKidsOnlineFindings.pdf Livingstone, Sonia and Hasebrink, Uwe and Garitaonandia, Carmelo and Garmendia, Maialen (2008) Comparing online risks faced by European children: reflections on youthful Internet use in Britain, Germany and Spain. Quaderns del CAC, 31-32 . pp. 95-10

[30] Ibid.

[31] Jamie May, Chief Investigator, AllClear ID, Report 2012, Child Identity Theft Identity Thieves Target Young Children: What Parents Need to Know to Protect their Kids, at https://www.allclearid.com/assets/docs/ChildIDTheftReport2012.pdf

[32] See:
http://ec.europa.eu/information_society/activities/sip/policy/programme/current_prog/index_en.htm

[33] Shaheen Shariff and Dianne L. Hoff, "Cyber bullying: Clarifying Legal Boundaries for School Supervision in Cyberspace", International Journal of Cyber Criminology, 2007, 1 (76).

[34] Millwood Hargrave, A. 2009. "Protecting children from harmful content". Report prepared for the Council of Europe's Group of Specialists on Human Rights in the Information Society. Available at www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2009)13_en.pdf, p. 8

[35] Shaheen Shariff and Dianne L. Hoff, note 33, p. 38.

[36] Notorious recent cases of this type are: stories of an American student Tyler Clementi, 16 years old Canadian girl, and an autistic Italian boy. Clementi was secretly filmed having sex with a man by his course mates and the video was broadcasted on the internet. Due to this incident, he committed suicide. Cf. Laura Trevelyan, "Shock at student's suicide over sex video", BBC News, 4 October 2010, at http://www.bbc.co.uk/news/world-us-canada-11464617.
In 2010, a Canadian girl was allegedly drugged and raped by a group of teenagers during a party. Another participant took pictures of the incident and disseminated them on Facebook. The photos were viewed, shared and reposted numerous times. Cf. Maple Ridge, Photos of gang rape go viral on Facebook , The Globe and Mail News, 10 February, 2012, at: http://m.theglobeandmail.com/news/british-columbia/photos-of-gang-rape-go-viral-on-facebook/article1710072/?service=mobile
In 2006, an autistic boy was insulted and beaten by his classmates, who also recorded the attack via mobile phones and uploaded the footage on the Youtube. Three Google executives were convicted for a violation of privacy due to the reluctance to remove the video from the platform. Cf. Raul Mendez, Google case in Italy, *International Data Privacy Law (2011) 1 (2): 137-139.*

minors themselves, often as close as classmates.[37] Another form of cyberharassment is "cyberstalking", an extreme conduct of online chasing, through frequent and deliberate contacts and threatening. Cyberstalkers sometimes may also use real personal data of the victim, the public disclosure of which creates even higher psychological and physical suffering.[38] Cyberharassment happens through interactions by e-mails, text messages, publication of embarrassing facts or pictures online, often in an anonymous way.[39]

Cybergrooming, instead, refers to the online contact of an adult with a child to establish a relationship of mutual trust with the aim of having sexual contacts offline.[40] This behaviour is a criminal offence in several countries covered under sexual solicitation definition and criminalised in the Convention of Council of Europe on the Protection of Children against Sexual Exploitation.[41] In academic literature this risks is also named as "stranger danger", emphasising the threat of contacts with unknown adults, such as sexual predators or paedophiles.[42] Most cybergrooming cases are argued to occur in chat rooms and via instant messaging. There is no evidence that the rise of social networks would increase this phenomenon.[43]

Another example of safety risk is 'sexting' (texting of sexually-explicit messages). 15% of 11-16 year old Europeans have received peer to peer *"sexual messages or images …[meaning] talk about having sex or images of people naked or having sex".*[44] Sexting may be seen as part of exploring sexuality but can also lead to utterly embarrassing situations, even fierce bullying, when these messages are forwarded to third parties.[45]

The majority of the above-mentioned child safety risks are based on prior acquisition of personal data or on digital traces of children left online. For example, previously disclosed personal information and private facts open doors to cyberharrasment, cyberbullying, and identity theft. The traceability of children's online activities and data leads to criminal activities, such as solicitation for sexual purposes, or commercial data use.[46]

2.2 Privacy risks

Besides safety risks, children may encounter online privacy risks, such as loss of reputation, misuse of personal data, discrimination, commercial exploitation due to the increased sharing of personal data and invasive commercial practises. Personal data of children may be collected automatically, for examples via

[37] OECD. 2011. "The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them", *OECD Digital Economy Papers*, No. 179, OECD Publishing. http://dx.doi.org/10.1787/5kgcjf71pl28-en, p. 25
[38] Ibid.
[39] Dooley, J.J., Cross, D., Hearn, L. and Treyvaud, R. (2009), "Review of existing Australian and international cyber-safety research". Child Health Promotion Research Centre, Edith Cowan University, Perth. At *www.dbcde.gov.au/__data/assets/pdf_file/0004/119416/ECU_Review_of_existing_Australian_and_international_cyber-safety_research.pdf*, p. 11
[40] Van der Hof, S., Koops. B-J. 2011. "Adolescents and Cybercrime: Navigating between Freedom and Control", Policy & Internet: Vol. 3: Iss. 2, Article 4, at http://www.psocommons.org/policyandinternet/vol3/iss2/art4, p. 9
[41] Convention of Council of Europe on the Protection of Children against Sexual Exploitation (CETS 201)
[42] Byron, T. (2008), "Safer Children in a Digital World: The Report of the Byron Review". London: Department for Children, Schools and Families, and the Department for Culture, Media and Sport. Available at *www.dcsf.gov.uk/ukccis/userfiles/file/FinalReportBookmarked.pdf*, p. 53
[43] OECD. 2011. note 37. p. 25
[44] Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. 2011. Risks and safety on the internet: The perspective of European children. Full Findings. LSE, London: EU Kids Online, p. 7.
[45] Van der Hof, S., Koops, B-J. 2011. "Adolescents and Cybercrime: Navigating between Freedom and Control", Policy & Internet: Vol. 3: Iss. 2, Article 4, at http://www.psocommons.org/policyandinternet/vol3/iss2/art4
[46] Declaration of the Committee of Ministers "On securing the dignity, security and privacy of children using the Internet", adopted on 20th February 2008 at the 1018th meeting of the Ministries Deputies, at https://wcd.coe.int/ViewDoc.jsp?Ref=Decl%2820.02.2008%29&Ver=0001.

cookies, when service provider requires signing up for a service, or voluntarily filling information in online forms or platforms.[47]

One of the most important aspects of privacy risks is oversharing of personal data. Research demonstrates, that youths themselves disclose vast amounts of personal data online, e.g., on Facebook and Twitter 26% of youths share their personal information, 14% even include address and telephone number in their profiles.[48] Peers' pressure on social networks contributes to the tendency of sharing ever more data and images.[49] Additionally, the urge to explore their identities inevitably entails disclosing (potentially sensitive) personal information online. Sharing of personal data online is also partially influenced by the changing perception of traditional boundaries between private and public domains. According to several studies, children tend to consider online and offline words as the same reality and, consequently, perceive the internet a private space to socialise with their peers, reveal secrets and intrinsically share personal information.[50] As showed by Steeves et al.[51], youths do not think it is risky to share email addresses and passwords with their friends and disclosure of personal data is often seen as an expression of trust. Moreover, as Livingstone asserts, youths "work with a subtle classification of 'friends', graded in terms of intimacy, which is poorly matched by the notion of 'public' and 'private' designed into social networking sites.[52]

Often, youths are not aware of the long-term consequences of their activities.[53] On the Internet the visibility of personal information is potentially global and online content (text, pictures, video, etc.) can be effortlessly copied or searched, although not (easily) removed.[54] For example, there are many reports of online reputation problems which influence future career possibilities after a potential employer finds text, pictures and videos revealing "inappropriate" features of candidate's personality. Moreover, children often are not able to understand and manage their privacy settings properly. Although social networking sites have a minimum age of 13 or 14 for membership, an increasing number of younger children have accounts. For example, 38% of 9 -12 year olds in Europe have a social networking profile, despite of age restrictions.[55] Often these young children do not understand and therefore skip privacy policies, especially because of their difficult language and length.[56] Default privacy settings rarely set the highest level of privacy protection for children, but not all young internet users are capable to change them. In addition to the lack of digital skills, also service providers do not necessarily guarantee the adequate level of protection. Services targeting children often fail to provide effective and reliable mechanisms through which parents can give their consent

[47] YPRT (Youth Protection Roundtable) (2009), *Stiftung Digitale Chancen*. Youth Protection Toolkit. Available at *www.yprt.eu/transfer/assets/final_YPRT_Toolkit.pdf*, 2009, p. 11.
[48] Ibid.
[49] Dooley *et al.*, 2009, p. 13, 143; Marwick, A., Murgia-Diaz, D. and Palfrey, J. (2010), "Youth, Privacy and Reputation" (Literature Review), *Berkman Center Research* Publication No. 2010-5. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163 p. 5, 20f.
[50] Marwick *et al.*, 2010, p. 13; West, A., Lewis, J. & Currie, P., 2009. Students' Facebook 'friends': public and private spheres. *Journal of Youth Studies*, 12(6), 615–627.
[51] Steeves, V. & Webster, C., 2008. Closing the barn door: the effect of parental supervision on Canadian children's online privacy. *Bulletin of Science, Technology & Society*, 28(1), p. 419.
[52] Livingstone, S., 2008. Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. New Media Society, 10(3), 393-411, p. 404.
[53] Cf. Kohnstamm, R. 2009. Kleine ontwikkelingspsychologie – De puberjaren. Houten: Bohn Stafleu van Loghum.
[54] boyd, d. 2008. Taken Out of Context. American Teen Sociality in Networked Publics. At http://www.danah.org/papers/TakenOutOfContext.pdf, p. 27.
[55] Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children. Full Findings. LSE, London: EU Kids Online.
[56] Fielder, A., Gardner, W., Nairn and A., Pitt, J. (2007), "Fair game? Assessing commercial activity on children's favourite Web sites and online environments". Available at www.agnesnairn.co.uk/policy_reports/fair_game_final.pdf, p. 23; Dooley *et al.*, 2009, p. 146;

on behalf of their children to create an account online.[57] In the EU, parental consent must be sought as long as minors are not capable to make an informed choice themselves, while in the US such age threshold is 13 years old.[58] However, many online services used by European youths are US-based and, according to the EU Data Protection directive 95/46/EC, are subject to the US rather than the EU privacy rules. The basis for the applicability rule of the Directive is the place of data processing activities, i.e. it applies when the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State. Application of privacy laws across borders, questions of enforcement and jurisdiction are therefore also a challenge.[59] In addition, another complication in this respect is technical difficulties to assess the age of internet users and to obtain verifiable parental content. Parental consent requirement is ineffective as children lie about their age, a frequent practise in the online world, often happening with the approval of the parents.[60]

In addition to excessive voluntary sharing, personal information can also be spread online by others. For example, 'tagging', i.e., a way to link a person to a picture, location or event, is an increased information sharing practise, often happening without consent from the person involved.[61] Dooley et al. found that more than 40% of youths had pictures of themselves uploaded online without their permission[62], Lenhart observed that 6% of youths reported having an embarrassing photo of them uploaded online without their prior permission.[63]

Finally, there are also new possible ways to gather personal data of children, for instance through GPS or other location-based services *(e.g.* Loopt, Google Latitude, Facebook Places). [64] The use of such information may lead to privacy abuses, e.g. in the case of mobile devices this can become a real-time tracking. In chats and other online forums, the status or availability of users is displayed and can equally provide information about their location.[65]

[57] YPRT, 2009, p. 11; Marwick *et al.*, 2010, p. 4.
[58] Children's Online Privacy Protection Act of 1998, at http://www.coppa.org/coppa.htm
[59] On the applicability and jurisdiction regime of the EU Data Protection Directive see: Lokke Moerel, "Back to basics: when does EU data protection law apply?", 2011, 2 *International Data Privacy Law*, pp. 92-110
Lokke Moerel, "The long arm reach: does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?", 2011, *1 International Data Privacy Law*, pp. 23 – 41
[60] In June, 2011, Consumer Reports issued a study showing that out of the 20 million children signed up for Facebook, 7.5 million were under the age of 13, of which 5 million children were under the age of 10. *Consumer Reports*, 2011. Cf. "*CR* survey: 7.5 million Facebook users are under the age of 13, violating the site's terms," press release (10 May), at http://pressroom.consumerreports.org/pressroom/2011/05/cr-survey-75-million-facebook-users-are-under-the-age-of-13-violating-the-sites-terms-.html. Matt Richtel and Miguel Helft, 2011. "Facebook users who are under age raise concerns," *New York Times* (11 March), at http://www.nytimes.com/2011/03/12/technology/internet/12underage.html.
A later study sponsored by Microsoft Research found that 36% of parents were aware that their children under 13 signed up for Facebook and that many of those parents helped their children to lie about their age in order to access the service. Cf. danah boyd, Eszter Hargittai, Jason Schultz, and John Palfrey. (2011). "Why Parents Help Their Children Lie to Facebook: Unintended Consequences of the 'Children's Online Privacy Protection Act'." *First Monday* 16(11), November, at: http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075
[61] ENISA 2007. "Security Issues and Recommendations for Online Social Networks". ENISA Position Paper No.1. Available at *www.enisa.europa.eu/act/res/other-areas/social-networks/security-issuesand-recommendations-for-online-social-networks/at_download/fullReport,* p. 21.
[62] Dooley *et al.*, 2009, p. 141
[63] OECD. 2011. "The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them", *OECD Digital Economy Papers*, No. 179, OECD Publishing, p. 29.
[64] eNacso. 2009. "Developing a Response to a new breed of location services". At *www.enacso.eu/index.php?option=com_rokdownloads&view=file&task=download&id=8%3Aenacso-response-to-the-new-breed-of location-services&Itemid=*; YPRT, 2009, p. 30; De Haan, J. and Livingstone, S. (2009), "Policy and research recommendations". LSE, London: EU Kids Online (Deliverable D5). At *www.lse.ac.uk/collections/EUKidsOnline/Reports/D5Recommendations.pdf*, p. 11.
[65] OECD. 2011. p. 30.

2.3 Commercial risks

As many studies indicate, personal information of children is increasingly seen as online commodity, which is a valuable asset for online advertisers and marketing companies.[66] Personal information, once spread online, can be linked to individual profiles and be used by third parties with commercial intend. Children may suffer from privacy-invasive *practices* such as online profiling, behavioural monitoring and targeting, without being aware of them and having knowledge about necessary safeguards. Consumer groups warn about potential "negative impacts on children's future self-image and well-being" due to the use of psychological, behavioural and social techniques by online advertising and marketing companies.[67] In the same vein, Solove notes that due to the architectures ever more based on personal data, internet users may be harmed in the future in their dignity, monetary or physical aspects.[68]

Minors often underestimate the commercial value of their personal data and do not have knowledge about the business models and interests behind data collection. In addition, extra incentives such as surveys, quizzes, discounts and contests are used to collect personal information on children and their family members, which provide a compelling motivation for data disclosure.[69]

Moreover, children are seen as influential consumers: although their spending power is low they can influence their parents' spending. Thus, websites have a business incentive to collect children's personal information, and create dependency to particular brands or products, manipulate and exploit children's vulnerabilities for commercial purposes. [70]

2.4 Interim conclusion

This section provided an overview of the most prevalent safety and privacy risks encountered by children online. The risks were divided into three groups: contact risks, privacy risks, and commercial risks. All these three groups of risks are relevant to the debate on children's privacy protection. Privacy, understood as form of control over one's personal data,[71] may be at stake in all three cases. In case of contact risks, not only privacy but also safety of a child may become an issue, as based on the lost control over personal data a child may become a victim of cyberbullying, cybergrooming or sexting.

In the following chapters this overview will serve as a background to evaluate whether and how this empirical research on risks influences policy formulation and is reflected in policy documents. It will also be observed whether contact, privacy or commercial risks get more attention from regulators and in which type of regulatory instruments.

---

[66] Byron, 2008, p. 157.

[67] TACD (Trans Atlantic Consumer Dialogue) (2009), "Resolution on Marketing to Children Online", At http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=207&Itemid, 2009.

[68] Solove, Daniel J., A Taxonomy of Privacy. University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006; GWU Law School Public Law Research Paper No. 129, p.487.

[69] Dooley *et al.*, 2009, p. 145 f.

[70] Valerie Steeves and Ian Kerr, Virtual playgrounds and buddybots: a data-minefield for tinys & tweeneys, *Panopticon, The 15th Annual Conference on Computers, Freedom & Privacy, Keeping an Eye on the Panopticon: Workshop on Vanishing Anonymity, Seattle, April 12, 2005.*

[71] Westin, Alan. 1970. Privacy and Freedom, The Bodley Head Ltd.

3. Child right to privacy

This section looks into the development of the child's right to privacy, including the right to personal data protection. The latter right in international law, differently from the EU law, is covered under the former. As recognised by the ECHR, information privacy is a key aspect of the right to respect for private life because information about us is part of our identity.[72] Starting with a brief look into the history of child right to privacy, the section then proceeds with its current interpretation in international law and examines relevant case law of the ECHR.

3.1 Historical development

Before the UN Convention on the Rights of the Child assigned to children universal human rights, scholars debated whether children are entitled to legal and moral rights. This broader debate on the rights-versus-welfare question is outside the scope of this paper, but it is enough to stress that the idea of children as right holders has been subject to long-lasting criticism.[73] Accordingly, also the law has developed its early understanding of the child as a limited agent in law, i.e., an adult in the making. As Freeman notes, it explained childhood through adulthood.[74] Such an understanding has been supported by a number of social science domains, like psychology, social anthropology, sociology which perceived "child" as "inadequate, incomplete, dependent".[75] Therefore, protection of children had been emphasised and child as an agent in law could not have any role and perform no independent action. With a new sociology of childhood in the late1980s, a shift occurred and academics started to emphasise children as "beings", not as "becomings".[76] This evolution went hand in hand with the developments in both national and international law. In the UK, in 1986 the highest court recognised that children under 16, with sufficient understanding and intelligence, can make their own decisions (e.g., give consent to contraceptive treatment).[77] The UN Convention on the Rights of the Child in 1989 stressed the concept of the child as both a "becoming" and a "being": Article 3 requires protection and care to safeguard the well-being of the child, Article 12 stresses the opportunity of the child to participate in decision making and to be heard in any judicial and administrative proceedings. As noted by Tobin, courts followed a similar trend in construction of childhood. From late nineteenth century children were treated in three different forms by courts – first, as parental possessions, later, as objects of development (i.e., vulnerable and immature creations, lacking the capacity to defend themselves and pursue their interests), and finally, from the 1960s as right holders.[78]

The difficulty to shift to a new approach was still noticeable after the adoption of the UN Convention on the Rights of the Child. In 1998, the Committee on the Rights of the Child has expressed concern at the lack of the reflection of civil rights and freedoms in national laws of member parties: "The committee remains uncertain as to the extent to which the Member Party has undertaken measures to ensure that the traditional

[72] Pretty v United Kingdom, Appl. No. 2346/02, 29 April 2002, para. 61.
[73] For a philosophical debate on children rights, see Steiner, H., 1994, An Essay on Rights, Oxford: Blackwell; Sumner, L.W., 1987, The Moral Foundation of Rights, Oxford: Clarendon Press; MacCormick, N., 1982,'Children's Rights: A Test-Case', in *Legal Right and Social Democracy*, Oxford: Clarendon Press: 154–166; Raz, J., 1984, 'Legal Rights', *Oxford Journal of Legal Studies* 4(1): 1–21.
[74] Freeman. M. F.B.A. (ed.) 2011. *Law and Childhood Studies.* Current Legal Issues 2011. Vol. 14. Oxford University Press, p. 2.
[75] Nick Lee. 2001. Childhood and Society: Growing up in an Age of Uncertainty, Open University Press.
[76] Freeman. M. F.B.A. (ed.) 2011. *Law and Childhood Studies,* p.5.
[77] *Gillick v. West Norfolk and Wisbech Area Health Authority*, 1986, AC 112.
[78] Tobin. John. „Courts and the Construction of Childhood: A New Way of Thinking", in Freeman. M. F.B.A. (ed.) 2011. *Law and Childhood Studies.* Current Legal Issues 2011. Vol. 14. Oxford University Press, pp. 56-59.

view of children as mere objects of care has been replaced by an understanding and recognition of the child as a subject of rights. In this regard, clarification is requested as to the applicability of the provisions of the constitution guaranteeing respect for the civil rights and freedoms of children, including the right to privacy provided for in article 16 of the Convention".[79]

The ground-breaking point in the child rights area was the adoption of the UN Convention on the Rights of the Child. The Convention is now the most widely ratified treaty in history and the most comprehensive of universal human rights treaties. Since its adoption in 1989, it has been ratified by 140 states. It has brought "a qualitative transformation of the status of children as the holders of rights".[80] Cass described the effect of the Charter as "to question the public/private dichotomy" and "to disaggregate the rights of children from the rights of "families", to constitute children as independent actors with rights vis-à-vis their parents and vis-à-vis the state".[81] UN Convention is one of the few international legal documents which, among other rights, expressly refer to children's right to privacy.[82] It establishes the right to privacy as one of the fundamental rights of the child by stating that **"**no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, or to unlawful attacks on his or her honour and reputation". This article touches upon the issues of physical environment of a child, the privacy of relations and communications, control of access to personal information about the child.[83] Although the drafter the UN Human Rights Committee has not defined the concept of "privacy", the drafting Committee has referred to personal information and the collection and storage of this information on computers, data banks and other devices by both public and private entities.[84] Right to privacy require that national legislation ensure that the child: knows of the existence of the information stored about him, knows the reason of such information storage, has access to such manual or electronic records, has a possibility to object and if necessary to correct or eliminate the stored information, if necessary with the help of an independent authority.[85]

3.2 Current interpretation

In addition to the aforementioned specific child right UN Convention, the right to privacy as a universal human right is explicitly declared in a number of international instruments. The most prominent document within the Council of Europe framework is the *European Convention for Protection of Human Rights and Fundamental Freedoms.* It establishes everyone's right to his private and family life, home and correspondence and sets forth the exceptional conditions under which public authorities might interfere with the exercise of this fundamental human right (Article 8). Article 8 does not explicitly mention the protection of personal data either, but the European Court of Human Rights on various occasions acknowledged that the

[79] Federal republic of Yugoslavia IRCO, Add. 49, para 13. Recited in Rachel Hodgkin, Peter Newell, *Implementation Handbook for the Convention on the Rights of the Child*, UNICEF, 1998, p. 199.
[80] Philip Alston and John Tobin. 2005. *Laying the Foundations for Children's Rights: An Independent Study of some Key Legal and Institutional Aspects of the Impact of the Convention on the Rights of the Child*, UNICEF, at: http://www.unicef-irc.org/publications/pdf/ii_layingthefoundations.pdf, p.ix.
[81] Cass, Bettina. 1992. "The Limits of the Public/Private dichotomy: A Comment of Coady and Coady", in Alston, P. Palmer, S. Seymour, J. (eds.). Children, Rights and the Law, Clarendon Press, Oxford, p. 142.
[82] Other international documents are: Declaration of the Rights of the Child, adopted by UN General Assembly Resolution 1386 (XIV) of 10 December 1959; African Charter on the Rights and welfare of the Child,
OAU Doc. CAB/LEG/24.9/49 (1990), *entered into force* Nov. 29, 1999.
[83] Rachel Hodgkin, Peter Newell, *Implementation Handbook for the Convention on the Rights of the Child*, UNICEF, 1998, p. 197.
[84] Sharon Detrick, A commentary on the United Nations Convention on the Rights of the Child, 1999, Martinus Nijhoff Publishers, p. 273.
[85] Rachel Hodgkin, Peter Newell, *Implementation Handbook for the Convention on the Rights of the Child*, p.202.

right to data protection is covered under it.[86] Although there are no specific children's rights under the Convention, the protection guaranteed by the Convention apply equally to children. Article 1 of the Convention provides that the rights must be secured to "everyone". Moreover, Article 14 states that the rights must be secured without discrimination on the ground of age.[87] Nevertheless, some academics argue that this is not sufficient and a comprehensive children's rights convention should be adopted.[88]

In addition, Article 17 of the *UN International Covenant on Civil and Political Rights* of 1966 protects privacy, family, home and correspondence. The wording of this article is identical to the Article 16 of the UN Convention on the Rights of the Child, except ensuring that "no one" instead of "no child" shall be subjected to unlawful interference. Protection of personal data are not mentioned in the Covenant, even personal data are implicitly protected as a part of the individual's privacy.

Another important convention adopted in the framework of the Council of Europe is *the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* of 28 of January 1981. It aims to secure respect for individual right to privacy, when personal data are processed by automatic means in its signatory countries. Convention covers basic principles for data protection, special rules on trans-border data flows and mechanisms for mutual assistance and consultation between its signatory parties. The Convention is the only binding international legal instrument with a worldwide application in personal data protection field, open to any country, including non-members of the Council of Europe. However, this Convention does not add any specific value in terms of children's privacy protection. It equally applies for all data subject independently from their age and imposes uniform rules on data controller.

3.3 Case law

A number of cases in the ECHR touched upon the issues related to the child's right to privacy protected under the Article 8 of the *European Convention for Protection of Human Rights and Fundamental Freedoms*.[89] However, majority of them raise the issues of family life and separation of children from parents, medical confidentiality, children and publicity, and participation in legal proceedings. Cases directly related to personal data protection on the internet are rare.[90] Several of the most relevant cases are considered below. To a certain degree they all involve the issue of protection of children's personal information, in the form of biometric data, photographs or personal information. These cases, although not merely internet-specific, are all relevant in order to understand how the ECHR legitimates specific protection of youths' privacy by providing the knowledge on the rationale of developed protection mechanisms and main concepts in the area of child privacy protection.

S and Marper v UK[91] case has raised privacy issues of children who participate in legal proceedings

[86] Among others, in ECHR cases Leander v. Sweden, 26.03.1987, Kopp v. Switzerland, 25.03.1998, Amann v. Switzerland, 16.02.2000
[87] Explanatory Report to Protocol No. 12 to the Convention for the Protection of Human rights and Fundamental Freedoms, at 20.
[88] Philip Alston and John Tobin. 2005. *Laying the Foundations for Children's Rights: An Independent Study of some Key Legal and Institutional Aspects of the Impact of the Convention on the Rights of the Child*, UNICEF, at: http://www.unicef-irc.org/publications/pdf/ii_layingthefoundations.pdf
[89] Including, among others, ECHR cases: *S and Marper v. UK,* No. 30562/04 and 30566/04, 2009; *Reclos and Davourlis v. Greece* No. 1234/05, 2009; *KU v. Finland*, No. 2872/02, 2009; *Von Hannover v. Germany,* No. 59320/00, 2004; *Gnahoré v. France*, No. 40031/98, 2000; *Sahin v. Germany N*o. 30943/96, 2003; *Haase v. Germany*, No. 11057/02, 2004; *Elsholz v. Germany,* No. 25735/94, 2000; *Kutzner v. Germany*, No. 46544/99, 2002; *Gineitiene v. Lithuania*, *No. 20739/05, 2010; Wagner and J.M.W.L. v. Luxembourg*, *No. 76240/01, 2007.*
[90] For the discussion of the available case law see De Hert & Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action', in Gutwirth, S., Poullet, Y., De Hert, P., Nouwt, S., De Terwangne, C. (eds.), Reinventing Data Protection?, Berlin, Springer, 2009, 330 p.
[91] App. No. 30562/04 and 30566/04, 2009, 48 EHRR 50.

as suspects. The applicant S (11 years old) was suspected with a robbery and his fingerprints and DNA samples were stored in the UK DNA database. After he was acquitted, he required the police to destroy his biometric data. The police refused to do so and the applicant started the procedure first before the national courts and subsequently before the ECHR. Before the ECHR he claimed that the retention of his biometric data violated Article 8 of the European Convention for Protection of Human Rights and Fundamental Freedoms and underlined the "social stigma and psychological implications" of the database. The ECHR stated that indiscriminate retention constituted disproportionate interference with Article 8 of the Convention. This was one of the few cases when the Court referred to the status of the applicant who was child and emphasised his vulnerability:

> *the retention of the unconvicted persons' data may be especially harmful in the case of minors, given their special situation and the importance of their development and integration in society.*[92]

Thus, in this case the ECHR took child-specific interests into account and referred to the harmful and detrimental impact of data retention upon the development of the child.[93]

Several ECHR cases involved child privacy issues in relation to dissemination of photographs taken in public places.

In *Reklos and Davourlis v Greece*[94] a professional photographer working in a hospital took pictures of a new-born baby and offered to sell them to the parents. The pictures were taken without parent's consent or knowledge after the baby's birth in a sterile unit. The parents objected to the photographs having been taken and required to give the negatives to them, but the photographer refused to do so. The parents brought a claim arguing that the personality rights of the child had been infringed, but the claim was dismissed by the highest court in Greece as being too vague. Consequently, the parents lodged an application with the ECHR on the basis of Article 8 of the European Convention for Protection of Human Rights and Fundamental Freedoms. The respondent, the Greek government, argued that there was no infringement of the Article 8, because photographs had not been disseminated, i.e. there was no commercial exploitation of the image, and the baby was not mature enough to suffer any infringement of his personality rights. The ECHR refused to analyse the latter argument of the respondent and did not deal with the question whether the infringement of the right to privacy depends on the individual being aware of that infringement. As noted by Hughes, if the ECHR had done so, this would curtain the rights of young children.[95] As regards the first argument, the ECHR agreed to consider an alleged interference with the child's right to respect for his private life although the images had not been published. The ECHR held that private life was a broad concept and it encompassed one's right to identity. It emphasised that an image reveals person's unique characteristics and forms one of the main attributes of his personality. Therefore, it is essential for an individual to control his image, including giving consent to one's image being taken, reproduced, conserved, published. Since the person concerned was a minor, his right to protection of his image had been in the

[92] Ibid., 124.
[93] Cf. K. Hughes, "The Child's Right to Privacy and Article 8 European Convention on Human Rights", Freeman. M. F.B.A. (ed.) 2011. Law and Childhood Studies. Current Legal Issues 2011. Vol. 14. Oxford University Press. Also see Chapter IV „Technology as a Regulatory Tool: DNA Profiling and Marper", in Brownsword, Roger & Goodwin, Morag. 2012. *Law and the Technologies of the Twenty-First Century*, Cambridge University Press.
[94] *Reclos and Davourlis v. Greece* No. 1234/05, 2009, EMLR 16.
[95] K. Hughes, "The Child's Right to Privacy and Article 8 European Convention on Human Rights", Freeman. M. F.B.A. (ed.) 2011. Law and Childhood Studies. Current Legal Issues 2011. Vol. 14. Oxford University Press, p. 478.

hands of his parents, whose prior consent was indispensable:

> *the key issue in the present case is not the nature, harmless or otherwise, of the applicants' son's representation on the offending photographs, but the fact that the photographer kept them without the applicants' consent. The baby's image was thus retained in the hands of the photographer in an identifiable form with the possibility of subsequent use against the wishes of the person concerned and/or his parents.*[96]

As a result, the ECHR held that the act of taking the photographs and their retention constituted a violation of the child's right to privacy under Article 8 of the Convention.

Similarly, *Von Hannover v Germany case*[97] concerned interference by sensational press with the right to the private life of Princess Caroline of Monaco. The subject of the application was the photographs of the applicant. In some cases applicant was photographed together with her children. The latter type of photographs were excluded from the subject of the application in its admissibility stage, because on a national level the Federal Constitutional Court of Germany had earlier recognised that photographs featuring the applicant with her children had infringed her right to the protection of her personality rights guaranteed by German law. The national court granted an injunction restraining the publication of these photographs.[98] It held that minors are entitled to special protection as not only their 'existing personality' but also their 'still-developing personality' should not suffer undue interference. Therefore, the collection and disclosure of data related to minors must be justified more than data related to adults, whose personality is already-developed. As regards the rest of the photographs, the ECHR held that there was a necessity to balance protection of the applicant's private life against freedom of expression, as guaranteed by Article 10 of the Convention.

The only case directly related to the informational privacy on the internet is the case of *KU v Finland.*[99] KU, a 12-year old applicant, lodged a complaint because an unknown person placed an advertisement on a dating site on the internet in his name, without his knowledge. The advertisement included KU's personal data, such as age and year of birth, gave a detailed description of his physical characteristics and provided a link to his web page with his picture. In the advertisement, it was claimed that KU was looking for an intimate relationship with a boy of his age or older. The applicant's father requested the police to identify the person who had placed the advertisement in order to bring charges against him. The service provider refused to disclose the identity of the person in question due to the confidentiality of telecommunications protected by law. The Finnish Court equally refused to oblige the service provider to disclose requested data because there was no legal provision authorising such an obligation. The ECHR held that Article 8 of the Convention has been violated. It emphasised the vulnerability of children and potential threat to the applicant's physical and mental welfare. The Court stressed that the applicant was a minor and that due to the advertisement he became target of paedophiles. This decision is the most prominent example when the ECHR considered seriously that the victim of privacy violation was a child and took his specific interests into account.

[96] *Reclos and Davourlis v. Greece, para. 42.*
[97] Von Hannover v Germany, App. no. 59320/00, 2004, 40 EHRR 1.
[98] BVerfG, 1 BvR 1353/99 of 31.3.2000.
[99] App no. 2872/02, 2009, 48 EHRR 52.

3.4 Interim conclusion

This section looked into the development of the child's right to privacy, including the right to personal data protection. The analysis showed that international treaties, except the UN Convention on the Rights of the Child, pay limited attention to children as right to privacy holders. Although being explicit, the UN Convention on the Rights of the Child does not seem to benefit children online in practise from a data protection perspective either. The only more relevant Convention in data protection respect is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 of January 1981, but it applies for all data subject independently from their age and imposes uniform rules on data controller. Therefore, it could be stated that in international law children are treated equally to adults and protection of their privacy is not tailored to their needs in any particular way.

A more promising, even if still limited, tendency can be noticed in the jurisprudence of the ECHR as regards Article 8 of the European Convention for Protection of Human Rights and Fundamental Freedoms. From eleven cases under study[100], which to a certain degree involved the issue of protection of children's personal information, in several cases the ECHR paid special attention to children as applicants and gave a reasoning to justify special, more rigorous, protection of their interests. In Reklos and Davourlis v Greece, the ECHR afforded a high degree of protection to minor's photographs, as protection from publicity deserves high protection also in adult cases. In two cases KU v Finland and S and Marper v UK, the ECHR afforded to children a higher degree of protection than to adults. The reason for such reinforced protection may be the evident harm that the data misuse may have caused to children in these cases (retention of DNA data and misuse online data by paedophiles).[101]

The following section will shift from the international to the regional level and look into the EU initiatives in this area. It will analyse online privacy protection through various EU regulatory instruments.

4. Online privacy protection for children in the EU

4.1 Charter of Fundamental Rights of the European Union

On 1 December 2009 *the Charter of Fundamental Rights of the European Union*[102] came into force. Besides a right to private life declared in the Article 7, the Charter also explicitly recognised the protection of personal data as a new, autonomous human right under its Article 8:

"Article 7
Respect for private and family life
Everyone has the right to respect for his or her private and family life, home and communications.

[100] ECHR cases: *S and Marper v. UK,* No. 30562/04 and 30566/04, 2009; *Reclos and Davourlis v. Greece* No. 1234/05, 2009; *KU v. Finland*, No. 2872/02, 2009; *Von Hannover v. Germany,* No. 59320/00, 2004; *Gnahoré v. France*, No. 40031/98, 2000; *Sahin v. Germany N*o. 30943/96, 2003; *Haase v. Germany*, No. 11057/02, 2004; *Elsholz v. Germany,* No. 25735/94, 2000; *Kutzner v. Germany*, No. 46544/99, 2002; *Gineitiene v. Lithuania*, *No. 20739/05, 2010; Wagner and J.M.W.L. v. Luxembourg*, *No. 76240/01, 2007.*
[101] K. Hughes, "The Child's Right to Privacy and Article 8 European Convention on Human Rights", Freeman. M. F.B.A. (ed.) 2011. Law and Childhood Studies. Current Legal Issues 2011. Vol. 14. Oxford University Press, p. 483.
[102] Charter of Fundamental Rights of the European Union [2000] OJ C364/01 (18.12.2000).

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

The right to data protection as a right for every individual is also enshrined in Article 16 of the Treaty on the Function of the European Union.

The distinction between privacy and personal data protection in the Charter not only highlights the final step in a long evolution, separating privacy from data protection, but also the difference between the two rights and the need of their coexistence. In practice, there may be cases when the right to privacy applies without involving data protection and vice versa.[103] Moreover, these two rights reflect different aspects of the required protection. The right to privacy refers to a static, negative protection and requires not to interfere with one's private and family life. Conversely, the right to personal data protection reflects a dynamic protection though the settlement of rules how to process and safeguard the data.[104]

Likewise the *European Convention for Protection of Human Rights and Fundamental Freedoms,* the Charter uses universal language and does not specifically refer to children. In other words, it guarantees the right to privacy and data protection to "everyone". Up until now, however, there have been no cases in the Court of Justice of the European Union in which this right was applied in the context of minors. However, the Charter should be seen in a dynamic interplay with the European Convention for Protection of Human Rights and Fundamental Freedoms. Article 52(3) of the Charter requires interpreting the Charter rights in the same meaning and scope as those laid down in the Convention. Therefore, the practice of the ECHR discussed in the previous section is relevant also in the context of the Charter.

4.2. Directive 95/46/EC and Directive 2002/58/EC

Information privacy issues for children online fall under the general EU data protection rules. Some security risks, such as sexual solicitation or identity theft, are considered to constitute a criminal offence.

Data Protection Directive 95/46/EC regulates the processing of personal data at European level.[105] Personal data are defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity". The Directive sets up a regulatory framework which aims to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal

[103] See De Hert, P. & Gutwirth, S., *"Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location-based services and virtual residence",* in IPTS, Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview. Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, IPTS Technical Report Series, EUR 20823 EN, 111-162 .

[104] Stefano Rodota, Data Protection as a Fundamental Right, in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds.), *Reinventing Data Protection?* , Springer, 2009, pp. 77-82.

[105] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 - 0050

data within the European Union. It is applicable to data processing by automated means, including the processing on the internet.

The text of the Directive makes no reference to children as data subjects and does not take into account particularity of their situation. For example, the Directive establishes the main principles of fair, lawful and transparent data processing. Transparency implies that data controllers (e.g. online service providers) must adopt and publish their privacy policies. This obligation does not receive any further specification in case of children, although the ability of children to understand such policies and foresee possible consequences differs from adults' abilities.[106] In addition, the Directive establishes rights of data subjects to access, correct, update their data or to object to their data processing. Again, the Directive makes no distinction how such rights may be executed by adults and by children. Therefore, according to the current legal framework the processing of children's personal data has to be authorized by law or parental consent and to conform to data processing principles. Parental consent is necessary until the child has developed the capacity to fully understand the processing and his data subject rights. This leaves ambiguities as regards the legitimation of the processing of children's data, as the exact age limit from which the child can consent to his data processing vary from child to child and across various situations. In addition, age verification mechanisms are problematic as in practise no easy-to-implement, effective and reliable tools to verify parental consent are currently available.

It should be noted, that the lack of specific attention to children to a certain extent has been compensated by the Article 29 Data Protection Working Party, a body established by the Directive and composed of representatives from supervisory authorities of each Member State. It issued several opinions explaining how the Directive should apply to children. Although the opinions of the Article 29 Working Party are usually influential, they have no legally binding effect.

In 2007, the Article 29 Working Party issued an *Opinion on the concept of personal data*[107] in which the four elements of the definition of personal data are elaborately discussed. These four elements are as follows: "any information", "relating to", "identified or identifiable", "natural person". As regards the last element, the Working Party stated that the Directive 95/46/EC is applicable to personal data of natural persons. This is a broad concept, which makes the protection independent of nationality or residence of the individual at stake. The concept of personality of human beings is commonly understood as "the capacity to be the subject of legal relations, starting with the birth of the individual and ending with his death."[108] Thus, in principle, the Working Party clarified that personal data relating to identified or identifiable living individuals, including children, fall under protection of the Directive 95/46/EC.

In 2009, the Working Party adopted *Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools).*[109] The purpose of the opinion was to analyse the general data protection principles relevant to the protection of children, and to explain their relevance and offer guidance for those working in a specific area, at school. In the Opinion, the Working Party clarified the concept of the child. According to the Working Party, a child as "a human being in the complete sense of the word" is entitled to the right to the protection of his or her personal data. Although children have the same rights, the specificity of the child as a data subject must be taken into account:

[106] Van Eecke, Patrick and Truyens, Maarten. 2010. Privacy and Social Networks, Computer Law &Security Review, 26, p. 542.
[107] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136.
[108] Ibid., p. 22.

…the child is in a special situation, which should be seen from two perspectives: the static, and the dynamic. From the static point of view, the child is a person who has not yet achieved physical and psychological maturity. From the dynamic point of view, the child is in the process of developing physically and mentally to become an adult. The rights of the child, and the exercise of those rights – including that of data protection - , should be expressed in a way which recognises both of these perspectives.[110]

It also emphasized other principles applicable to children as data subjects: best interest of the child, protection and care necessary for the wellbeing of children, representation, adaptation to the degree of maturity of the child, participation in decision making.

The Working Party noted that the Directive due to its limited personal and material scope, does not touch upon a number of important questions related to the protection of children's privacy. For example, problems arise with regard to the degree of individual maturity of a child, i.e. determination when children can start dealing with their own personal data without parental involvement. Second, uncertainty remains as regards the extent to which representatives can represent minors if the disclosure of minor's personal data prejudices his or her best interests.

Another key issue which was also clarified by the Article 29 Data Protection Working Party is consent of minors. It took a flexible approach and did not set a precise age limit at which parental consent is required. Instead, it underlined the importance of maturity of a child and complexity of the data processing at hand.[111] For instance, Article 29 Data Protection Working Party believed that data collection from an 8-year-old child for the purpose of sending a free magazine or newsletter does not require parental consent, while such consent would be necessary for the girl to take part in a live TV show. The same complex question was brought up by the Article 29 Data Protection Working Party in its latest *Opinion on consent*, where it acknowledged that the lack of general rules and harmonisation of the age threshold and the way children's consent is obtained, causes legal uncertainty.[112] Article 29 Data Protection Working Party encouraged the European Commission to take initiative to regulate this matter. In the Opinion 15/2011 it advocated age verification use and advised to include into the revised Directive 95/46/EC specific provisions on age verification. As an example it proposed to establish age verification based on "sliding scale approach" which would mean that age verification depends on the evaluation of specific circumstances (age, capacities, complexity of data processing) in each and individual case.[113] However, this suggestion is not reflected in the Proposal for a General Data protection Regulation.

The Directive 95/46/EC in the online context should be applied in conjunction with another sectorial

[109] Article 29 Data Protection Working Party, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), WP 160, 11 February 2009
[110] Ibid., p. 3.
[111] Article 29 Data Protection Working Party, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), WP 160, 11 February 2009
[112] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 01197/11/EN WP 187, 13 July 2011.
[113] Article 29 Data Protection Working Party has repeatedly stesssed the importance to find solution for regulating consent. It its opinion depending on the maturity of the child, obligation to obtain consent could follow sliding-scale approach: from mere consultation of the child, to a parallel consent of the child and the legal representative, to the sole consent of the child. Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), WP 160, 11 February 2009

Directive 2002/58/EC (e-Privacy Directive).[114] This Directive contains provisions aiming to ensure that users can trust the services and technologies they use for communicating electronically and deals with spam, the user's prior consent ("opt-in"), and the installation of cookies. However, in terms of children's privacy protection online, this Directive does not address children, as internet users, either. It applies to all users independently from their age and imposes identical obligations on service providers regarding, for instance, the placement of cookies in the computer of the child.

4.3. Proposal for a General Data Protection Regulation

On 25 January 2012 European Commission announced a Proposal for a General Data Protection Regulation[115] (the Proposal), which in several years is expected to replace the current Directive 95/46/EC. According to the legislative process of the EU, the Proposal will require approval from the Council of the European Union and the European Parliament and, therefore, will most probably be notably changed. Nevertheless, the Proposal clearly shows the ground-breaking intentions of the EU as a policy maker and seems "to remake the data protection landscape in Europe by introducing far-reaching changes"[116]. One of the main objectives of the Proposal is to enhance the effective control of individuals, including children, over their personal data.

Recital 29 explicitly recognises that children deserve specific protection of their personal data, as "they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data." Among many other new definitions, the Proposal also introduces a definition of child, which is taken from the UN Convention on the Rights of the Child: a child is defined as any person below 18 years (Article 4 Part 18 of the Proposal).

Article 8 of the Proposal addresses the issue of consent given by a child in the online environment. The Proposal establishes that when information society services are offered directly to a child below the age of 13, online service providers are obliged to obtain consent or authorisation from his parents or custodians. The Proposal is silent about the obligation to obtain parental consent from children of the age between 14 and 18.[117] The proposal seems to follow the legislative approach of the US, which is present in the Children's Online Privacy Protection Act (COPPA). COPPA places certain obligations on internet service providers, which target children under 13 or which knowingly collect children's data on websites oriented towards general audience. Parental consent in the EU should, in principle, become verifiable in the future as the Proposal states: "the controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology". The Commission will adopt delegated acts which further specify the criteria and requirements for concrete methods to obtain verifiable consent. In order to take account of the

[114] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal L 201 , 31/07/2002 P. 0037 - 0047*

[115] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[116] C. Kuner, 2012. The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Privacy & Security Law Report, 11 PVLR 06, 02/06/2012, p.2.

[117] Article 29 Data Protection Working Party has repeatedly stesssed the importance to find solution for regulating consent. It its opinion depending on the maturity of the child, also children from 14 to 18 may need parental representation. Obligation to obtain consent, according to the Working Party, could follow sliding-scale approach: from mere consultation of the child, to a parallel consent of the child and the legal representative, to the sole consent of the child. Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), WP 160, 11 February 2009

specific needs of micro, small and medium-sized enterprises, the Commission will consider specific measures for them.

As regards other legal basis for data processing, the legitimate interest of a controller under the Proposal becomes a limited ground, as it needs careful assessment where the data subject is a child.

The Proposal emphasizes the obligation of transparency through easily accessible privacy policies, information to data subjects provided in an intelligible form, clear and plain language, adapted to specific needs of data subjects. In particular, this obligation applies for any information addressed to children (Article 11).

The data subject's right to be forgotten and to erasure, foreseen in the Article 17 of the Proposal, provides another effort to strengthen the control over one's personal data. Both rights should signify respectively practical instruments to have online personal data deleted. The right to be forgotten should apply ''especially in relation to personal data which are made available by the data subject while he or she was a child'' when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet (Article 17(1)). However, there are practical difficulties in implementing these tools or enforcing such rights in the online environment. This has been noticed by many stakeholders in their reactions to the Proposal, which will be discussed below.

Article 18 of the Proposal creates a new data subject's right to data portability allowing to obtain a copy of personal data undergoing processing in an electronic format and to transmit it from one electronic service provider or processing system to another. As a precondition it provides the possibility to obtain from data controllers data in a structured and standard electronic format, which will be specified by the Commission in implementing acts.

Article 33 introduces a new obligation for data controllers or processors to conduct an impact assessment, where processing operations present specific risks to the rights and freedoms of data subjects due to their nature, scope or purposes. This obligation, among others, applies to the processing of personal data in large scale filing systems on children.

Another safeguard of children's privacy introduced by the Proposal relates to prohibition of profiling. Profiling by means of automated processing is subjected to suitable safeguards and according to the Proposal cannot concern a child.

Protection of children's personal data receives some attention also in the framework of awareness raising. According to the Article 52, one of the new duties of supervisory authorities is to promote the awareness of the public on risks, rules, and rights in relation to the processing of personal data. Proposal explicitly states that activities addressing specifically children shall receive specific attention.

Taking the above-described provisions into account, it is obvious that the European Commission made an important step to explicitly address children as data subjects in data protection law. However, it may be questioned how effective and sufficient such regulation will be. In the present Proposal uncertainty remains, regarding the consent of children between the ages of 14 and 18, the age group which is the most risk-taking and less dependent on their parents. It is not clear whether children of this age can consent without parental engagement always or just in certain cases. The regulation of consent applies only in digital environment and many other offline situations are left unregulated. Moreover, the methods to obtain verifiable consent may remain in stagnation phase, as service providers are not clearly obliged to implement them, but only to make a reasonable effort towards doing so. The need to take into account existing age-

verification technology, and no clear imposed commitment to develop new or improve existing technologies, may lead to no more than sound words on paper. Also, the lack of definition of "services offered directly to a child" does not provide a clear answer how to deal with mixed online communities or websites where children are present in substantial numbers together with adults. In reality, few service providers guarantee clear delineation of their services between the communities of children and adults.[118]

Such a limited attention to children in the new Proposal would not be welcomed by many stakeholders, who in their responses to the Public Consultation of 15 January 2011[119] emphasised the necessity to target specific issues around the protection of children. For example, the European consumers' Organisation (BEUC) considered necessary to include specific provisions across the new regulation, such as the obligation for data controllers to implement mechanisms for age verification, prohibition to collect sensitive information from children and other information unless it is relevant, necessary and lawful.[120] Also according to Privacy International, more consideration should be given to privacy-related interests of children.[121]

After the Proposal has been adopted, several stakeholders and institutions expressed their reaction and evaluated the provisions dedicated to the protection of children. In general, the majority welcomed the effort of the Commission to address the long-standing and complex issues related to children's privacy online. Several Committees of the European Parliament welcomed and endorsed the special provisions on children's consent and the right to be forgotten, at the same time asking to clarify them and ensure their effectiveness.[122]

Article 29 Working Party reacted to the child specific provisions in a concise manner. In the Opinion on the data protection reform proposals the representatives of the member states underlined the importance of pure national discretion to set the age limits in contract law and to apply progressive protection in accordance with maturity level, thus without setting precise age limits, in EU data protection law.[123] It welcomed the minimum rule that the processing of personal data of a child below the age of 13 is only lawful if consent is given by a child's parent or custodian. The Working Party also suggested broadening the scope of this rule beyond information society service area and foreseeing more situations in which specific rules for children apply.

As regards the right to be forgotten and to erasure, the Working Party equally welcomed the introduction of these rights as means to strengthen the control over one's personal data. However, given the formulation of these rights in the Proposal and characteristics of the online word, it noted that these rights may be of a very limited effectiveness. In particular, problems may arise when data or its replications and

[118] This question is solved in COPPA in the following way: in order to determine whether a service is directed at children, the Federal Trade Commission takes into account criteria, such as the subject matter; the audio or visual content; the age of any models; the language used; the presence of advertising on the specific site. Other empirical evidence are also important to decide upon the age of the actual or intended audience, such as the use of animated characters or other child-oriented features.

[119] European Commission, Communication on the "Comprehensive Approach on Personal Data Protection in the European Union", (COM(2010)609).

[120] BEUC, Response to the European Commission's Communication on the „Comprehensive Approach on Personal Data Protection in the European Union", at: http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/beuc_en.pdf

[121] Privacy International, Response to the European Commission's Communication on the „Comprehensive Approach on Personal Data Protection in the European Union", January 2011, p. 6, at: http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/pi_en.pdf

[122] Draft Report on the protection of minors in the digital world, Committee on Culture and Education, Rapporteur: Silvia Costa, at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-486.198+01+DOC+PDF+V0//EN&language=EN. Draft Opinion of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on Culture and Education on protecting children in the digital world (2012/2068(INI)), Rapporteur: Anna Hedh, 2012/2068(INI), 11 June 2012, at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-491.241%2b01%2bDOC%2bPDF%2bV0%2f%2fEN

copies which have to be erased are processed beyond the control and knowledge of the data controller (e.g. by third parties which are not obliged to comply with erasure requests or by controllers which are no longer in existence). Moreover, the Working Party emphasised the need to balance privacy rights and the right to freedom of expression.

In reaction to the Proposal also the European Data Protection Supervisor (EDPS) issued an opinion, which similarly to the Working Party, does not pay extensive attention to the issue of minors.[124] The EDPS merely stated that the requirement of parental consent or authorization only for children below the age of 13 is a reasonable approach.[125] In addition, the EDPS proposed to expand the rules on legal representation to all individuals lacking sufficient capacity, thus not only children, including the rules on the way of exercising of rights on behalf of legally incapable individuals and covering the possible conflict of interests between such individuals and their representatives.[126] The EDPS also commented on the right to be forgotten and to erasure. In this respect, the EDPS welcomed a right to be forgotten, which he sees as an effort to strengthen the right to erasure in the digital environment. However, as many other stakeholders, the EDPS emphasized that this right must be effective in reality and needs to be more developed in the Regulation. Also the right to data portability, needs more clarification. According to the EDPS, current text suggests that it applies only to data provided by data subject on the basis of consent and a contract excluding other grounds. Moreover, it is not clear whether the invocation of the right means that the data controller has to erase the data or may continue processing them.

4.4. Interim conclusion

Even though the EU has been a frontrunner in regulating the matters of children protection online,[127] the binding regulatory framework which has been and still is in force does not specifically tackle the problems related to children's privacy on the internet. However, there is a recent effort to address child privacy issues online. This effort of the European Commission is evident through the revision of command-and-control regulation in the area of data protection. In the Proposal for a General Data Protection Regulation children are granted specific recognition. The Proposal foresees several special requirements to ensure the realisation of a more adequate data protection regime for children, such as requirements related to transparency, specific conditions for the processing of children's data, a 'right to be forgotten' online, and protection from profiling. Although concrete rules of the Proposal regarding children may be criticized as being too limited, incomplete or ineffective, on a more fundamental level, they demonstrate a long-awaited recognition of the specific needs of children as a group of data subjects. Despite the loopholes mentioned by stakeholders, these rules provide protection tailored to children's level of maturity and comprehension.

---

[123] Opinion 01/2012 on the data protection reform proposals, 00530/12/EN WP 191, 23 March 2012.
[124] Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012, at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf
[125] Ibid, para. 128
[126] Para 130.
[127] The first regulatory effort in the area is found in 1996, Green Paper on the protection of minors and human dignity in audiovisual and information services, COM (1996) 483 final, 16 October 1996.

5. Self-regulation

From the mid-1990s onwards at the EU level it is recognised that legislation may be not the best way to achieve the policy goal of protecting minors (including their privacy) on the internet.[128] Gradually a preference for self-regulation as a supplement to existing legislation became apparent. Self-regulation, in which private sector plays a greater role, was suggested as the solution to the deficit of legislation in force. The advantages of quick adaptation to the rapid technological developments and flexibility were the main justification of the self-regulatory instruments to protect minors and human dignity online.[129] With time an increased attention was drawn to co-regulation. The Commission noted that "co-regulation may be "more flexible, adaptable and effective than straightforward regulation and legislation" and "with regard to the protection of minors, where many sensibilities have to be taken into account, co-regulation can often better achieve the given aims".[130]

5.1. Safer Social Networking Principles for the EU

Also in practise self-regulation became a viable option for protecting online safety of minors. One of the most recent soft-law interventions is the *Safer Social Networking Principles for the EU*,[131] a self-regulatory initiative, signed by 21 social networking companies in 2009. Although entitled as self-regulatory initiative rather than co-regulation, the Principles were developed in close cooperation with the European Commission. The Principles encourage a safe approach towards personal information and privacy by having adequate safety tools and policies implemented in online services. Examples of concrete measures taken by the participating social networks are the introduction of reporting mechanisms such as an easy-to-use and accessible "report abuse" buttons, the improvement of default privacy settings and controls for profiles of users under 18, and preventing users below the age the service is targeting, from registering. In particular, Principle No. 6 "Encourage safe use approach to privacy" foresees that social networking sites should:

> "*Enable and encourage users to employ a safe approach to personal information and privacy: Providers should provide a range of privacy setting options with supporting information that encourages users to make informed decisions about the information they post online. These options should be prominent in the user experience and accessible at all times. Providers should consider the implications of automatically mapping information provided during registration onto profiles, make users aware when this happens, and should consider allowing them to edit and make public/private that information where appropriate. Users should be able to view their privacy status or settings at any given time. Where possible, the user's privacy settings should be visible at all times.*"

[128] Commission of the European Communities, Green Paper on the protection of minors and human dignity in audiovisual and information services, COM (1996) 483 final, 16 October 1996.
[129] Recommendation 98/560/EC of 24 September 1998 on the development of the 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
[130] Commission of the European Communities, Second Evaluation Report from the Commission to the Council and the European Parliament on the application of Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity, COM/2003/0776 final, 12 December 2003.
[131] European Commission. 2009. Safer Social Networking Principles for the EU. 10 February 2009. At http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf.

The European Commission periodically assesses the compliance with the Principles based on self-declarations submitted by the participating social networks. According to the latest independent assessment, the majority of service providers complied with the principles in a rather satisfactory manner.[132] For example, implementation of the Principle 6 was assessed as very satisfactory in 7 out of 9 tested services. The best assessed services were those that effectively offered accessible and always available privacy settings on their sites allowing users to have full control over the visibility of personal data and communication of such data. The compliance with other Principles varies by service provider with two social networks being evaluated very satisfactory and the majority demonstrating good or fair compliance.

5.2 European Code of Conduct of FEDMA and its online marketing Annex

Another example of a rather successful self-regulatory initiative in action is the *European Code of Conduct of FEDMA and its online marketing Annex*.[133] The Code and the Annex were approved by the Article 29 Data Protection Working Party in 2010 as fulfilling the requirements for codes of conduct set forth in the Directive 95/46/EC and offering solutions for the problems in the online marketing sector.[134] Section 6 of the Code deals with the protection of children and, among others, establishes the responsibility of the data controller for setting up the procedures to guarantee verification of the age of the minor and the authenticity of the parental consent. However, it acknowledges that there is no easily accessible, universally accepted age verification system available on the internet.

The Code also obliges data controllers to provide child-appropriate information about data processing, prohibits family data collection from children, limits collection of sensitive data, and forbids incentives to provide personal data for marketing purposes or in exchange for a reward, including games of chance, tombola or lotteries.

5.3 Future self-regulatory initiatives

More self-regulatory initiatives may be expected in the future. Recently the EU Commissioner N. Kroes increased pressure on the industry to come up with self-regulatory and technical solutions in the area of child safety online.[135] Moreover, a new Proposal for a General Data Protection Regulation clearly opted for self-regulation to ensure child protection. As a general rule, it obliges the Member States, the supervisory authorities and the Commission to encourage self-regulation through codes of conduct, certification, data protection seals and marks. More specifically, article 78 of the Proposal takes into account specific features of the various data processing sectors. The sector of information and protection of children is mentioned as one of the areas in which codes of conduct could in particular contribute to the proper application of the provisions of the Proposal. Unfortunately, the control and enforcement of the codes of conduct is left to the total discretion of the associations or bodies themselves. The Proposal does not establish any obligatory

[132] Assessment of the Implementation of the Safer Social Networking Principles for the EU on 9 services: Summary Report, 2011, at: http://ec.europa.eu/information_society/activities/social_networking/docs/final_reports_sept_11/report_phase_b_1.pdf
[133] FEDMA, European Code of Practise for the use of personal data in direct marketing electronic communications Annex, 2010, at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp174_annex_en.pdf
[134] Article 29 Data Protection Working Party, Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing, WP 174, 13 July 2010, at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp174_en.pdf
[135] Kroes, N. 2011. My visit to Silicon Valley – where the nerds meet the hippies. At <http:// blogs.ec.europa.eu/neelie-kroes/my-visit-to-silicon-valley-where-the-nerds-meet-the-hippies/>.

compliance control process. The authors of the codes may only submit the texts of new or existing amended or extended codes to the supervisory authority of a Member State for an opinion. Associations or other bodies acting in the name of data controllers in several Member States may submit such codes to the European Commission for the recognition of their general validity throughout the territory of the whole EU and publicity. Equally to the codes of conduct, the Member States and the Commission are required by the Proposal to encourage the establishment of certification mechanisms, seals and marks, which could help data subjects to rapidly evaluate the level of data protection offered by data controllers or processors in various sectors. The only clear indication of control from the side of the European Commission is the fact that the Commission retains the power to specify the criteria, conditions of granting or withdrawing for certification mechanisms as well as to foresee standards for promotion and recognition of technical standards, seals and marks. The efficiency of such self-regulatory model will become clearer once the Proposal is adopted and comes into force.

5.4. Interim conclusion

Self-regulatory initiatives take into account special issues and risks related to the child's right to privacy and demonstrate a clear tendency to address child privacy online in a specific manner. However, the incentives of voluntary codes are fragmented depending on industries or membership of a representative umbrella organisation. As a result, the two examples of codes of conduct in social networking and advertising areas are focused on that particular areas. They mainly address privacy and commercial risks. Contact risks are not subject to their provisions.

In the context of online privacy, there are no comprehensive, sector-crossing self-regulatory codes drafted to protect children online. The new Proposal has already called for the implementation of data protection rules in the area of children protection through the adoption of codes of conduct of a more general nature. Such codes or a single European Code could create a uniform system of online child privacy protection across Europe. It is questionable, however, why the EC did not opt for a more rigorous co-regulatory process in this case and did not introduce any mandatory compliance control instead of limiting its role to advisory function. Greater involvement of the EC into the drafting of the codes of conduct to protect children online could lead to more effective and binding self-regulatory commitments.

6. Market and social norms

Market as a modality of regulation in the area of children's online privacy protection is the weakest from all the four regulatory modalities. From the current regulatory framework it does not seem that the EU uses this incentive in any respect.

As regards the social norms the situation is quite different. In recent years, EU has devoted an increasing attention to the development of digital literacy, education and awareness campaigns.[136] Such campaigns can be seen as a way to introduce or improve the existing social norms in the area of online child

[136] European Commission, Communication "A European approach to media literacy in the digital environment", Brussels, 20.12.2007, COM(2007) 833 final, at http://ec.europa.eu/culture/media/literacy/docs/com/en.pdf. Recitals 8, 37 and Article 8 of the Directive 2010/13/EU of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member

safety and privacy. Although at the beginning the emphasis was placed on illegal internet content and online safety risks, recently more and more references to data protection were included in education campaigns. For example, events of the Safer Internet Programme focused on sharing of personal data online in 2010, and on social networking sites and control over the personal data in 2011.[137]

6.1 Safer Internet Programme

The objective of the programme is to draw the society's attention to illegal and harmful internet content and online safety issues. The Safer Internet programme finances and implements various activities in EU member states and on European level. For example, the programme finances national awareness raising nodes, which intend to help children, parents and educators to avoid the dangers associated with digital communication and educate them about safer internet, and hotlines, i.e., facilities which process reports from the public about the illegal and harmful internet content. The programme of 2009-2013 in particular focusses on contact risks, grooming and bullying.[138] The aims of this latest programme are: to increase public awareness; provide contact points for reporting illegal and harmful content and conduct (child sexual abuse material, grooming and cyber bullying); promote self-regulatory initiatives in this area; establish an empirical knowledge base on online activities and their consequences for children.[139]

6.2 European Strategy for a Better Internet for Children

Recently the European Commission has adopted a Communication which developed a far-reaching European strategy for child protection on the internet.[140] The Communication builds upon the EU Agenda for the Rights of the Child,[141] the Digital Agenda for Europe,[142] and the Council Conclusions on the Protection of Children in the Digital World.[143] The Communication states that children have specific needs and vulnerabilities and their difference has to be recognised. In particular, the Communication recognises that data protection is a key element for the protection of children online and empowerment to enjoy online benefits and safety.

The Commission acknowledges that a combination of policies is required to deliver a Better Internet for Children. It expresses the preference for alternative regulatory tools by stating: "regulation remains an option, but, where appropriate, it should preferably be avoided, in favour of more adaptable self-regulatory tools, and of education and empowerment".[144]

Awareness is one of the key ingredients of the European Strategy for a Better Internet for

---

States concerning the provision of audiovisual media services; Recital 13 and Annex 2 of the European Parliament and Council Recommendation 2006/952/EC on the protection of minors and human dignity.

[137] Safer Internet Day 2010 : "What you post online remains online. Think before you post!", Safer Internet Day 2009: "Empowering and protecting young people on social networks", at http://ec.europa.eu/information_society/activities/sip/events/day/si_day_previous/index_en.htm

[138] Safer Internet Programme 2009 -2013, at http://ec.europa.eu/information_society/activities/sip/policy/programme/index_en.htm

[139] Ibid.

[140] Commission Communication on a "Better Internet for Children" (2.05.2012), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:EN:PDF

[141] Digital Agenda for Europe, COM(2010) 245 final.

[142] EU Agenda for the Rights of the Child, COM(2011) 60 final.

[143] Council Conclusions on the Protection of Children in the Digital World, 3128th EDUCATION, YOUTH, CULTURE and SPORT Council meeting Brussels, 28 and 29 November 2011.

[144] Ibid.

Children.[145] As one of the aims of the Strategy is "stepping up awareness and empowerment", it focuses on awareness and empowerment of children online and enhancement of their self-protection and self-responsibility. The Strategy, amongst others, requires member states to include digital and media literacy in their school curricula by 2013 and support related public-private partnerships to develop educational and awareness materials for teachers and children. The Strategy also aims to scale up awareness activities and youth participation to reach children, parents, and teachers across the EU. Particular attention should be paid to the youngest and most vulnerable children. To reach this goal, the EC from 2014 undertakes to create an EU-wide interoperable service infrastructure with online safety information and public awareness tools, and guarantee platforms for youth participation. Industry is asked to promote the scaling up of awareness activities by supporting education providers and NGOs as well as disseminating awareness raising materials to their customers.

7. Code or architecture

Technological tools are increasingly seen by scholars as useful measures that regulators can use to reach certain policy objectives in digital environment.[146] The emerging child safety and privacy area is not an exception. Technology is more and more used as a regulatory tool, often as a part of regulatory strategy in this area.[147] As becomes evident from two recent initiative described below, parental controls, privacy settings, age ratings, age-verification, reporting tools, have been hailed by the EC as the answer to concerns regarding children protection online, but their implementation in practise is still in an early stage.

7.1 European Strategy for a Better Internet for Children

Besides awareness and empowerment mentioned above, one of the main aims of the Strategy is to create a safe online environment. In the area of online privacy this is achieved through techno-regulation, as the main proposed actions include default privacy settings, parental controls, age-rating and content classification mechanisms.

As regards privacy settings, the actions proposed in the Strategy are based on the presumption that it is not possible to find a one-size-fit-all solution for children of all ages. Therefore, age-appropriate default privacy settings are recognised as a necessity. Privacy settings under the Strategy fall under the responsibility of industry which is expected to "implement transparent default age-appropriate privacy settings, with clear information and warnings to minors of the potential consequences of any changes they make in their default privacy settings and contextual information on the privacy level of every piece of information required or suggested to set up an online profile".[148] In order to employ age-appropriate settings, industry also has to implement technical means for electronic identification and authentication. The task of the Commission in this respect is to propose in 2012 a pan-European framework for electronic authentication. The framework should enable the use of personal attributes (age in particular) to ensure

[145] Commission Communication on a "Better Internet for Children" (2.05.2012), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:EN:PDF

[146] Cf. Chark, Charles, The Answer to the machine is in the machine", in Hugenholtz. P. Bernt (ed.). 1996. *The future of copyright in a digital environment*, The Hague, Kluwer Law International, p. 139.

[147] For example, see the European Strategy for a Better Internet for Children, COM(2012) 196 final; Digital Agenda for Europe, COM(2010) 245 final

compliance with the age provisions of the proposed data protection regulation. The Commission also undertakes to support research and development of technical means for electronic identification and authentication across the EU. Finally, member states are asked to encourage the adoption of self-regulatory measures by industry and follow their implementation at national level as well as to support awareness raising activities.

Moreover, the Strategy recognises the necessity to ensure the wider availability and use of parental control tools in several languages to allow parents to make an informed choice about the use of these tools. Therefore, industry should ensure the availability of parental controls that are simple to configure, user friendly and accessible for all on all internet-enabled devices available in Europe. According to the Strategy, the Commission will support benchmarking and testing of parental control tools and research into how age-rating and content classification systems could be made interpretable by effective parental controls that can deal with a wider range of languages. It will also consider legislative measures if industry self-regulation fails to deliver the required results. Member states are invited to support industry's efforts in this field and to follow up their implementation on devices sold on their territory, perform tests and certification cycles for parental control tools as well as promote their availability.

The European Data Protection Supervisor in its recent Opinion on the Communication "European Strategy for a Better Internet for Children"[149] expressed the support for the online safety initiatives and welcomed the acknowledgment of the importance of data protection in this context. It called for appropriate consideration of data protection risks and requirements by industry, member states and the Commission when implementing the Strategy. In this respect, the EDPS believes that references to data protection should be included in education campaigns about online safety. Industry should respect data protection law, obtain parental consent, provide more protective default privacy settings for children than for adults, implement warning mechanisms to alert children when they change default privacy settings. Moreover, industry should work to implement appropriate age-verification mechanisms, which are not intrusive from a data protection perspective.

As regards advertising to children, the EDPS refers to the Article 29 Working Party opinion on behavioural advertising and states that there should be no direct marketing aimed at minors and that children should not be subjected to behavioural advertising.[150] According to the EDPS the Commission should encourage industry to develop privacy friendly self-regulatory measures with respect to online advertising to children at EU level. Besides self-regulation, the Commission is encouraged to explore the possibility to use command-and-control regulation and legislate at EU level to ensure the appropriate consideration of children's rights to privacy and data protection in the context of advertising.

7.2 Coalition to make a better and safer internet for children

Children's safety online is one of the key commitments reflected in the Digital Agenda for Europe.[151] As a flagship initiative under the Europe 2020 strategy for smart, sustainable and inclusive growth, among

---

[148] Commission Communication on a "Better Internet for Children" (2.05.2012), para. 2.3.1.
[149] EDPS Opinion on the Communication from the Commission - "European Strategy for a Better Internet for Children" (17.07.2012).
[150] Article 29 Working Party Opinion 2/2010 on online behavioural advertising, 22 June 2010, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf.
[151] Digital Agenda for Europe: key initiatives, Memo/10/200, 19 May 2010, at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/200&format=HTML&aged=0&language=EN&guiLanguage=en.

other priorities, such as creation of digital single market, interoperability, faster internet access, research and development, the Digital Agenda emphasises internet trust and security. In this respect, the Agenda aims to address online threats, such as identity theft and cyber-attacks, by developing responsive mechanisms and effectively enforce the right to privacy and to the protection of personal data. In order to reach this objective the Vice-President of the European Commission N. Kroes has initiated a coalition from 28 private companies working in various sectors of ICT industry (operating system providers, handset manufacturers, Internet Service Providers, broadcasters, social networks and mobile operators).[152] The underlying idea of the Commission is that the Coalition proposes and develops, first of all technical, solutions and measures to make the internet a "safer place for children" which later can be embraced also by other market players. The areas in which the companies agreed to take action and develop solutions include: tools for users to report harmful content and contact, age-appropriate privacy settings, content classification, parental controls, effective take down of child abuse material. The Coalition has adopted the Statement of Purpose, which sets forth the deadlines for the performance of concrete tasks and outlines the work plan.[153] Recently, the Coalition has evaluated its work in progress. Overall, it was recognised that progress has been made in all 5 action areas, but more effort is needed to achieve the agreed goals, in particular in the areas of content classification and effective takedown of child abuse content.[154] Also, a need for independent monitoring and review of the coalition's work was emphasised.[155] In the context of age appropriate privacy settings, the results achieved by the Coalition are quite disappointing. The Coalition members shared their own current practises on the protocols through which they give information and warning to users about changes in default privacy settings, and analysed the question whether a single standard for online privacy settings is possible. After a dissemination of a questionnaire among Coalition members, it became clear that to find a common definition of various age groups and accordingly to implement age-dependent privacy settings is a big challenge. A single standard for such settings is not possible across sectors.[156] Concerning the wider availability and use of parental controls, the results of the Coalition's specific working group are equally disappointing. Due to diversity of Coalition members and differences in cultures and approaches, no single solution for a "parental control", and agreement on what would be the best way to guarantee parental controls to consumers could be reached.[157]

Some stakeholders, like European Digital Rights (EDRi), an association of 32 privacy and digital rights organisations, have expressed criticism of this initiative. EDRi noted that this self-regulatory process is being used for purposes of big businesses in Europe: to promote their own products or to get a competitive advantage over others. It stressed that companies with a worrying reputation in concrete technological measures, such as Facebook in privacy settings and Microsoft in "notice and takedown" practice, became

---

Digital Agenda for Europe: what would it do for me?, Memo/10/199, 19 May 2010, at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/199&format=HTML&aged=0&language=EN&guiLanguage=en

[152] Neelie Kroes Vice-President of the European Commission responsible for the Digital Agenda, Making internet a better place for children – a shared responsibility, Safer Internet Forum 20 October 2011, Luxembourg, SPEECH/11/703, 20 October 2011, at: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/703&format=HTML&aged=0&language=EN&guiLanguage=en

[153] Coalition to make the Internet a better place for kids, Statement of purpose, at: http://ec.europa.eu/information_society/activities/sip/docs/ceo_coalition/ceo_coalition_statement.pdf

[154] Report of Mid-term review meeting of the CEO Coalition to make the internet a better place for kids, July 2012, at: http://ec.europa.eu/information_society/activities/sip/docs/ceo_coalition/report_11_july.pdf

[155] Ibid.

[156] WG2: Age appropriate privacy settings progress report, at http://ec.europa.eu/information_society/activities/sip/docs/ceo_coalition/privacy_progress_report.pdf

[157] Progress Report for WG 4: Wider availability and use of Parental controls, http://ec.europa.eu/information_society/activities/sip/docs/ceo_coalition/parental_controls_progress_report.pdf

responsible for the development of the same measures on European level.[158] Moreover, EDRi noted that the Coalition experiences strong political pressure from the Commission to deliver quick solutions for complex problems. This leads to strange proposal which may infringe freedom of speech and net neutrality principle, such as a proposal to scan all computers using through automatic Windows updates for child abuse material or to whitelist all webpages of Europe.[159] Finally, the Coalition did not collect the experiences from different EU countries on the identified problems, including various options already available on the market, and therefore the productivity of the discussions which start from scratch may be questioned.

In summary, it could be stated that the EC still sees command-and-control regulation as a valid option, but prefers to avoid it in favour of more adaptable self-regulatory technical tools. A strong push towards the development of new solutions to protect children's privacy and safety online by the industry is felt in both initiatives - the European Strategy for a Better Internet for Children and Coalition to make a better and safer internet for children**.** However, up to date none of them proposed concrete improvements and empowerment of children though technology online. Moreover, both initiates are questionable from a co-regulatory perspective. The role of the EC is not clearly defined and there are no yet any binding commitments or enforcement mechanisms set.

8. Conclusions

Having reviewed a number of regulatory initiatives it is time to draw the threads together. The regulation of child online privacy and safety has been analysed from the perspectives of law (command-and-control and self-regulation), social norms, market and code.

In each of these areas the extent to which child-specific interests are taken into account is different. In command-and-control legislation on the international level, children are not considered as a specific category of individuals which deserve a reinforced protection. Although the UN Convention on the Rights of the Child grants specific rights to children, including the right to privacy, this Convention does not seem to benefit much children online in practise from a data protection perspective. On the contrary, the Article 8 of the European Convention for Protection of Human Rights and Fundamental Freedoms, although being a universal, non-child-specific provision, may be seen as providing greater and more adequate privacy protection to children on the internet. In some cases, like *KU v Finland* and *S and Marper v UK,* based on Article 8 of the Convention, the ECHR has given serious consideration to the child's right to privacy and afforded a higher degree of protection for minors than for adults.

In the EU law, there is currently no specific regime for children to protect their online privacy. Children are subject to general protection guaranteed in the data protection Directive 95/46/EC and E-privacy Directive 2002/58/EC. Nevertheless, in the EU there has been an increasing recognition of the specific needs of children as a group and the necessity for protection tailored to their level of maturity and comprehension.[160] Especially the Proposal for a General Data Protection Regulation may be seen as a

[158] Edri notes: "Microsoft's history in "notice and takedown" is hardly exemplary. Recent cases showing that Microsoft, using Google's global application of US copyright law, has repeatedly demanded that Google removes links from its search results – links which remain available on Microsoft's own search engine. Microsoft, on the other hand, has also developed a product called "photoDNA," used by Facebook UK as an upload filter to prevent known child abuse material being added to their site." Edri-gram, *The rise of the European upload filter,* 20 June, 2012, at http://edri.org/edrigram/number10.12/the-rise-of-the-european-upload-filter

[159] EDRi-gram newsletter - Number 10.5, 14 March 2012, CEO Coalition to make the Internet a better place for kids 14 March, 2012, at http://www.edri.org/edrigram/number10.5/ceo-coalition-freedom-of-speech

[160] See Article 29 Working Party Opinion 2/2009 on the protection of children's personal data (General

ground-braking point in this respect. It grants to children specific, although limited, recognition. The Proposal foresees several specific requirements to ensure the realisation of more adequate data protection regime for children, such as requirements related to transparency and accountability, specific conditions for the processing of children's data, a 'right to be forgotten' online, and protection from profiling.

On the contrary, self-regulation in the area is adapted to the specific child-related needs and interests, but is fragmented depending on industries or membership of a representative umbrella organisation. In the area of children protection there are no codes of conduct of a more general nature. The new Proposal for General Data Protection Regulation has already called for the adoption of such codes which hopefully can create a uniform system of online child privacy protection across Europe in the future.

Other modalities (social norms and code) take into account special issues and risks related to the child's right to privacy and demonstrate a clear tendency to address child privacy online in a manner appropriate to the specificity and vulnerability of the individuals at risk.

As regards the choice of the preferred regulatory instruments, at least in the EU, there seems to be a trend to rely on law, especially self-regulation, and code. These two modalities are seen as viable in the battle against online privacy and safety risks. Not only the new Proposal for a General Data Protection Regulation but also the European Strategy for a Better Internet for Children and the Coalition to Make a Better and Safer Internet for Children entail a strong shift towards self-regulation and technological tools. However, the role of the European Commission is not clearly defined in these initiatives and there are no yet any binding commitments or enforcement mechanisms which could give hope for their effective functioning in the near future.

Finally, the EU tends to use various regulatory modalities which differ according to risk categories. Legislation is used partially to regulate privacy and commercial risks. Those groups of risks are also subject to self- and co- regulatory initiatives. Contact risks, if not criminalised by national laws, are mainly subject to social norms and are often mitigated through education and awareness raising measures.

In summary, it could be stated that there is a growing tendency to address child privacy online in a specific manner tailored to the specificity and vulnerability of children as Internet users, especially on EU level. Such tendency is particularly evident in two types of regulatory instruments, law (including self-regulation) as well as technology. Social norms are also increasingly attracting the attention of EU policy makers, but law and technology as regulatory modalities currently appear to be favoured by the EU as a regulator.

Guidelines and the special case of schools), 11 February 2009, WP 160, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_en.pdf. Recital 29 of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Bibliography:

- Alston, Philip and Tobin, John. 2005. *Laying the Foundations for Children's Rights: An Independent Study of some Key Legal and Institutional Aspects of the Impact of the Convention on the Rights of the Child*, UNICEF, at: http://www.unicef-irc.org/publications/pdf/ii_layingthefoundations.pdf
- Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 01197/11/EN WP 187, 13 July 2011.
- Article 29 Data Protection Working Party, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), WP 160, 11 February 2009
- Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136.
- Article 29 Data Protection Working Party, Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing, WP 174, 13 July 2010, at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp174_en.pdf
- Article 29 Working Party Opinion 2/2010 on online behavioural advertising, 22 June 2010, at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf.
- Ayres, Ian and Braithwaite, John. 1992. *Responsive regulation: transcending the deregulation debate*, Oxford, Oxford University Press.
- Baldwin, R., Scott, C. and Hood, C. (eds.) 1998. *A Reader on Regulation*: *Oxford Readings in Socio-Legal Studies*, Oxford: Oxford University Press.
- Black, J. 2001."Decentring regulation: The role of regulation and self regulation in a "Post Regulatory" world", Current Legal Problems 54: 103-146.
- Bonnici. M. G. P. 2008. *Self-Regulation in Cyberspace* (Information Technology and Law). Asser Press. 1st Edition
- boyd d., U. Gasser, J. Palfrey. 2010. How the COPPA, as Implemented, Is Misinterpreted by the Public: A Research Perspective. The Berkman Center for Internet & Society Research Publication Series. At http://cyber.law.harvard.edu/publications
- boyd, d. 2008. Taken Out of Context. American Teen Sociality in Networked Publics. At http://www.danah.org/papers/TakenOutOfContext.pdf
- Braitwaite, John. 2002. *Restorative justice and responsive regulation*, Oxford, Oxford University Press.
- Brownsword, Roger and Goodwin, Morag. 2012. *Law and the Technologies of the Twenty-First Century*. Cambridge University Press.
- Brownsword. R. 2008. *Rights, Regulation, and the Technological Revolution*. Oxford: Oxford University Press.
- Byron, T. 2008. "Safer Children in a Digital World: The Report of the Byron Review". London: Department for Children, Schools and Families, and the Department for Culture, Media and Sport. Available at *www.dcsf.gov.uk/ukccis/userfiles/file/FinalReportBookmarked.pdf*
- Cass, Bettina. "The Limits of the Public/Private dichotomy: A Comment of Coady and Coady", in Alston, P. Palmer, S. Seymour, J. (eds.). 1992. *Children, Rights and the Law*, Clarendon Press, Oxford.
- Chark, Charles.1996. The Answer to the machine is in the machine", in Hugenholtz. P. Bernt (ed.), The future of copyright in a digital environment, The Hague, Kluwer Law International.
- Coalition to make the Internet a better place for kids, Statement of purpose, at: http://ec.europa.eu/information_society/activities/sip/docs/ceo_coalition/ceo_coalition_statement.pdf
- Coalition to make the Internet a better place for kids. Statement of purpose, at: http://ec.europa.eu/information_society/activities/sip/docs/ceo_coalition/ceo_coalition_statement.pdf
- CoE, Declaration of the Committee of Ministers "On securing the dignity, security and privacy of children using the Internet", adopted on 20th February 2008 at the 1018th meeting of the Ministries Deputies, at https://wcd.coe.int/ViewDoc.jsp?Ref=Decl%2820.02.2008%29&Ver=0001.7
- Commission of the European Communities, Second Evaluation Report from the Commission to the Council and the European Parliament on the application of Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity, COM/2003/0776 final, 12 December 2003.
- De Haan, J. and Livingstone, S. 2009. "Policy and research recommendations". LSE, London: EU Kids Online (Deliverable D5). At *www.lse.ac.uk/collections/EUKidsOnline/Reports/D5Recommendations.pdf*, p. 11.
- De Hert & Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action', in Gutwirth, S., Poullet, Y., De Hert, P., Nouwt, S., De Terwangne, C. (eds.), 2009. *Reinventing Data Protection?,* Berlin, Springer.

- De Hert, P. & Gutwirth , S., *"Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location-based services and virtual residence",* in IPTS, Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview. Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, IPTS Technical Report Series, EUR 20823 EN.
- Detrick, Sharon. 1999. *A commentary on the United Nations Convention on the Rights of the Child*, Martinus Nijhoff Publishers.
- Dooley, J.J., Cross, D., Hearn, L. and Treyvaud, R. 2009. "Review of existing Australian and international cyber-safety research". Child Health Promotion Research Centre, Edith Cowan University, Perth. Available at *www.dbcde.gov.au/__data/assets/pdf_file/0004/119416/ECU_Review_of_existing_Australian_and_international_cyber-safety_research.pdf*
- EDPS, Opinion of the on the data protection reform package, 7 March 2012, at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03 07_EDPS_Reform_package_EN.pdf
- EDPS, Opinion on the Communication from the Commission - "European Strategy for a Better Internet for Children" (17.07.2012) http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-07-17_Better_Iternet_Children_EN.pdf
- eNacso. 2009. "Developing a Response to a new breed of location services". Available at*www.enacso.eu/index.php?option=com_rokdownloads&view=file&task=download&id=8%3Aenacso-response-to-the-new-breed-of-location-services&Itemid=*;
- ENISA. 2007. "Security Issues and Recommendations for Online Social Networks". ENISA Position Paper No.1. At *www.enisa.europa.eu/act/res/other-areas/social-networks/security-issuesand-recommendations-for-online-social-networks/at_download/fullReport*.
- European Commission. 2002. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal L 201 , 31/07/2002 P. 0037 – 0047*
- European Commission. 2007. Communication "A European approach to media literacy in the digital environment", Brussels, 20.12.2007, COM(2007) 833 final, at http://ec.europa.eu/culture/media/literacy/docs/com/en.pdf.
- European Commission. 2009. Safer Social Networking Principles for the EU. 10 February 2009. At http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf.
- European Commission. 2010. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, 4 November 2010, COM (2010) 609 final
- European Commission. 2011. EU Agenda for the Rights of the Child, COM(2011) 60 final.
- European Commission. 2012. Communication on a "Better Internet for Children" (2.05.2012), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:EN:PDF.
- European Commission. 2012. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
- European Commission. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 - 0050
- European Commission. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
- European Commission.2010. Digital Agenda for Europe, COM(2010) 245 final.
- FEDMA. 2010. European Code of Practise for the use of personal data in direct marketing electronic communications Annex, at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp174_annex_en.pdf
- Fielder, A., Gardner, W., Nairn and A., Pitt, J. 2007. "Fair game? Assessing commercial activity on children's favourite Web sites and online environments". At *www.agnesnairn.co.uk/policy_reports/fair_game_final.pdf*
- Freeman. M. F.B.A. (ed.) 2011. *Law and Childhood Studies.* Current Legal Issues 2011. Vol. 14. Oxford University Press.

- Hasebrink, U., Livingstone, S., Haddon, L. 2008. *Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online*. London: EU Kids Online (Deliverable D3.2) available at: http://www.gobernanzainternet.es/doc/archivos/EUKidsOnlineFindings.pdf
- Hodgkin, Rachel and Peter Newell. 1998. *Implementation Handbook for the Convention on the Rights of the Child*, UNICEF.
- Hope. A. 2007. Risk-taking, boundary-performance and intentional school internet 'misuse.' Discourse: studies in the cultural politics of education, 28(1)
- Jamie May, AllClear ID, Report 2012, Child Identity Theft Identity Thieves Target Young Children: What Parents Need to Know to Protect their Kids, at https://www.allclearid.com/assets/docs/ChildIDTheftReport2012.pdf
- Kohnstamm, R. 2009. Kleine ontwikkelingspsychologie – De puberjaren. Houten: Bohn Stafleu van Loghum.
- Koops B.J. et al. (eds). 2006. *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-liners*. Information Technology & Law Series. Vol. 9. Asser Press.
- Koops, Bert-Jaap. 2011. The (In)Flexibility of Techno-regulation and the Case of Purpose Binding, Legisprudence, Vol. 5, No. 2.
- Kuner. C. 2012. The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Privacy & Security Law Report, 11 PVLR 06, 02/06/2012
- Lee, Nick. 2001. Childhood and Society: Growing up in an Age of Uncertainty, Open University Press.
- Lessig, L. 1999. *Code and other laws of cyberspace,* New York, Basic books
- Lessig. L. 1999. The Law of the Horse: What Cyberlaw Might Teach. 113 Harvard Law Review
- Levi-Faur, David (ed.). 2012. *Handbook on the Politics of Regulation*, Edward Elgar Publishing.
- Lievens, Eva. 2010. Protecting Children in the Digital Era: The Use of Alternative Regulatory Instruments, Martinus Nijhoff Publishers, Leiden/Boston.
- Livingstone, S., 2008. Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. New Media Society, 10(3), 393-411.
- Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. 2011. Risks and safety on the internet: The perspective of European children. Full Findings. LSE, London: EU Kids Online.
- Livingstone, Sonia and Hasebrink, Uwe and Garitaonandia, Carmelo and Garmendia, Maialen. 2008. Comparing online risks faced by European children: reflections on youthful Internet use in Britain, Germany and Spain. Quaderns del CAC.
- Livingstone, Sonia, Haddon, Leslie and Görzig, Anke (eds.). 2012. *Children, risk and safety on the internet: research and policy challenges in comparative perspective.* Policy Press, Bristol.
- Livingstone. S. 2009. Children and the Internet: Great Expectations, Challenging Realities. Cambridge: Polity
- Markey. E. 2011. A Bill To amend the Children's Online Privacy Protection Act of 1998. At http://markey.house.gov/docs/dntk_legislation.pdf
- Marwick, A., Murgia-Diaz, D. and Palfrey, J. 2010. "Youth, Privacy and Reputation" (Literature Review), *Berkman Center Research* Publication No. 2010-5. Available at *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163*.
- Millwood Hargrave. A. 2009. "Protecting children from harmful content". Report prepared for the Council of Europe's Group of Specialists on Human Rights in the Information Society. Available at www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2009)13_en.pdf,
- Moerel, Lokke. 2011. "Back to basics: when does EU data protection law apply?", 2 *International Data Privacy Law*, pp. 92-110
- Moerel, Lokke. 2011. "The long arm reach: does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?", *1 International Data Privacy Law*, pp. 23 – 41
- Morgan, Bronwen and Yeung Karen. 2007. *An Introduction to Law and Regulation: Text and Materials*, Cambridge University Press.
- Muray, Andrew and Scott, Collin. 2002. „Controlling the New Media: Hybrid Responses to New Forms of Power", 65 *Modern Law Review.*
- Murray. A. 2006. *The Regulation of Cyberspace: Control in the Online Environment*, Routledge-Cavendish. 1 edition
- OECD. 2011. "The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them", *OECD Digital Economy Papers*, No. 179, OECD Publishing. http://dx.doi.org/10.1787/5kgcjf71pl28-en.
- Prenksy, M. 2001. Digital Natives, Digital Immigrants. On the Horizon, 9, 5, 1–6.
- Prosser, Tony. 2008. Self-regulation, Co-regulation and the Audio-Visual Media Services Directive, *Journal of Consumer Policy*, vol. 31, issue 1.

- Rodota, Stefano. Data Protection as a Fundamental Right, in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds.). 2009. *Reinventing Data Protection? ,* Springer.
- Shariff, Shaheen and Hoff, Dianne. 2007. L."Cyber bullying: Clarifying Legal Boundaries for School Supervision in Cyberspace", International Journal of Cyber Criminology, 1 (76).
- Solove, Daniel J., 2006. A Taxonomy of Privacy. University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006; GWU Law School Public Law Research Paper No. 129.
- Steeves Valerie and Kerr, Ian. 2005. Virtual playgrounds and buddybots: a data-minefield for tinys & tweeneys, *Panopticon, The 15th Annual Conference on Computers, Freedom & Privacy, Keeping an Eye on the Panopticon: Workshop on Vanishing Anonymity, Seattle.*
- Steeves, V. & Webster, C., 2008. Closing the barn door: the effect of parental supervision on Canadian children's online privacy. *Bulletin of Science, Technology & Society*, 28(1).
- TACD (Trans Atlantic Consumer Dialogue). 2009. "Resolution on Marketing to Children Online", At *http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=207&Itemid*, 2009.
- Tapscott, D. 1998. Growing up digital: the rise of the Net generation. New York: McGraw-Hill.
- Thierer, A. 2011. Kids, Privacy, Free Speech & the Internet- Finding the Right Balance. Working paper. At http://mercatus.org/sites/default/files/publication/Kids_Privacy_Free_Speech_and_the_Internet_Thierer_WP32.pdf
- UNICEF, 2002. *Implementation Handbook for the Convention on the Rights of the Child*
- Van der Hof, S., Koops. B.J. 2011. "Adolescents and Cybercrime: Navigating between Freedom and Control", Policy & Internet: Vol. 3: Iss. 2, Article 4, at http://www.psocommons.org/policyandinternet/vol3/iss2/art4
- Van Eecke, Patrick and Truyens, Maarten. 2010. Privacy and Social Networks, *Computer Law &Security Review*, 26, pp. 535-546.
- Van Kokswijk, J. 2007. *Digital Ego: Social and Legal Aspects of Virtual Identity*. Delft: Eburon Uitgeverij.
- West, A., Lewis, J. & Currie, P., 2009. Students' Facebook 'friends': public and private spheres. *Journal of Youth Studies*, 12(6), 615–627.
- Westin, Alan. 1970. *Privacy and Freedom*, The Bodley Head Ltd.
- YPRT (Youth Protection Roundtable). 2009. *Stiftung Digitale Chancen*. Youth Protection Toolkit. Available at *www.yprt.eu/transfer/assets/final_YPRT_Toolkit.pdf*, 2009.