

Risk-reducing regulatory strategies for protecting minors in social networks

Eva Lievens

Eva Lievens is a Senior Researcher at the Interdisciplinary Centre for Law and ICT (ICRI), KU Leuven, Leuven, Belgium.

Abstract

Purpose – *The purpose of this article is to present the preliminary results of a research project which aspires to identify requirements for risk-reducing regulatory strategies aspiring to protect children and young people in social networks. It aims to provide an insight into the changing role of law in today's networked society and the innovative regulatory solutions that will be able to deal with the paradigm shift from mass media and passive, vulnerable consumers to media for mass self-communication and active "prosumers".*

Design/methodology/approach – *First, the legal impact of social networking sites (SNS) risks for children and young people that have been identified in social science research is assessed, as well as the applicability of existing legal instruments. Second, legal trends in this field and a number of recent (alternative) regulatory initiatives and their implementation are discussed. In a final part, the use of such alternative regulatory instruments and their compliance with the broader legal (human rights) framework are analysed. To conclude, a number of elements for risk-reducing regulatory strategies for the protection of minors in online social networks are identified.*

Findings – *The first research results point towards the importance of multi-stakeholder involvement, proportionality of measures, procedural guarantees (such as transparency) and the careful combination of regulatory strategies targeted at illegal as well as harmful conduct and content risks for a balanced protection of minors in social networks.*

Originality/value – *Although social networks are very popular among young users, the risks that are associated with these networks are not at all or not appropriately addressed by existing legal or regulatory instruments. This article aims to contribute to developing innovative regulatory instruments which are effectively addressing these risks.*

Keywords *Social networks, Protection of minors, Self-regulation, Co-regulation, Alternative regulatory instruments, Youth, Regulation*

Paper type *Research paper*

1. Introduction

Participatory and collaborative online technologies, such as social network sites (SNS), transform the way in which individuals interact. In the past five years, the popularity of these SNS has expanded spectacularly, attracting an extraordinary number of users (e.g. 500 million users for Facebook) (Facebook, 2011a), particularly (but not exclusively) among the younger generations. A recent EU-wide[1] study found that 59 per cent of 9-16 year olds have a social networking profile (Livingstone *et al.*, 2011), even though most social network sites put the minimum age limit to create a profile at 13.

SNS, such as Facebook, Twitter and Netlog, can be credited with important positive features, such as innovative and sophisticated opportunities to construct one's identity and the quasi unlimited sharing of social experiences, but they also create new risks or transform risks that also exist in the offline world, in particular for vulnerable users, such as minors (Council of Europe, 2010; Livingstone and Brake, 2010).

The author's research into risk-reducing regulatory strategies for the protection of minors in online social networks is funded by the Research Fund KU Leuven (*Onderzoeksfonds KU Leuven*). This article presents the first results of this research, which will be finalised at the end of 2011. The author wishes to thank Leo Van Audenhove, Martijn Poel and Anastasia Konstantelou for their valuable comments.

It is assumed that the blurring between “public” and “private” in online social networks, the invisibility of audiences and the fact that information in such networks is persistent, replicable, searchable, and visible on a large scale (boyd, 2008) entail that risks in an SNS environment are significantly more complex compared to equivalent offline risks. Aside from providing greater access to certain (illegal or harmful) categories of content (e.g. hate speech) (Byron, 2008), and the facilitation of certain behaviour such as cyberbullying or grooming (Enisa, 2007), an added complexity can be found in the transforming role of minors, from passive consumers/victims to active contributors/perpetrators (Internet Safety Technical Task Force, 2008). This element has also been taken into consideration in the classification of a number of genuine online risks for minors, put forward by the recent renowned EU Kids Online study as shown in Table I).

It is the aim of this article to approach these social science findings from a legal perspective. Although over the past five years, online SNS have been the subject of study from diverse disciplines, such as social sciences, economics or computer sciences, research into legal risks has been significantly more limited and has in most instances focused on privacy issues (Edwards and Brown, 2009; Wong, 2009). Research into the legal impact of content and conduct risks that occur in a specific SNS context and the regulatory instruments that can be used to address these risks has been rather rare.

This article will first assess the legal impact of the SNS risks that have been identified in social science research, as well as the applicability of existing legal instruments. Second, legal trends in this field and a number of recent (alternative) regulatory initiatives and their implementation will be discussed. In a final part, the use of such alternative regulatory instruments and their compliance with the broader legal (human rights) framework will be assessed. To conclude, a number of elements for risk-reducing regulatory strategies for the protection of minors in online social networks will be identified.

2. Legal impact of SNS risks

In order to be able to assess the legal framework that surrounds SNS risks a first task is to translate the risks that have been identified by social scientists (see Table I)[2] into legal qualifications. Starting from the classification put forward by the EU Kids Online project, different legal “disciplines” come into play, such as:

- Human rights: e.g. infringement on freedom of expression, privacy/data protection (EDPS, 2011; European Commission, 2010; Council of Europe, 2010).
- Criminal law: e.g. stalking, grooming, gambling.
- Media law: e.g. defamation, (audiovisual/print) content regulation.
- Electronic communications law: e.g. spam.
- Intellectual property rights law: e.g. copyright.
- Consumer protection, e.g. advertising, etc.

Transferred to the EU Kids Online table (Table I) a preliminary assessment of the potentially applicable (broad) legal disciplines can be presented as shown in Table II.

Table I Classification of online risks

	<i>Commercial</i>	<i>Aggressive</i>	<i>Sexual</i>	<i>Values</i>
Content – child as recipient	Advertising, spam, sponsorship	Violent/hateful content	Pornographic or unwelcome sexual content	Racism, biased or misleading info/advice (e.g. drugs)
Contact – child as participant	Tracking/harvesting personal information	Being bullied, stalked or harassed	Meetings strangers, being groomed	Self-harm, unwelcome persuasion
Conduct – child as actor	Gambling, hacking, illegal downloads	Bullying or harassing another	Creating and uploading pornography	Providing advice e.g. suicide/pro-anorexic chat

Source: Hasebrink *et al.* (2009, p. 26)

Table II Legal impact of SNS risks

	<i>Commercial</i>	<i>Aggressive</i>	<i>Sexual</i>	<i>Values</i>
Content – child as recipient	Advertising, spam, sponsorship <i>Human rights, media law, consumer protection law, electronic communications law</i>	Violent/hateful content <i>Human rights, media law, criminal law</i>	Pornographic or unwelcome sexual content <i>Human rights, media law, criminal law</i>	Racism, biased or misleading info/advice (e.g. drugs) <i>Human rights, media law, criminal law, consumer protection</i>
Contact – child as participant	Tracking/harvesting personal information <i>Human rights, privacy/data protection</i>	Being bullied, stalked or harassed <i>Criminal law, media law</i>	Meetings strangers, being groomed <i>Criminal law</i>	Self-harm, unwelcome persuasion <i>Criminal law</i>
Conduct – child as actor	Gambling, hacking, illegal downloads <i>Criminal law, intellectual property rights law, consumer protection</i>	Bullying or harassing another <i>Criminal law, media law</i>	Creating and uploading pornography <i>Human rights, media law, criminal law</i>	Providing advice e.g. suicide/pro-anorexic chat <i>Criminal law</i>

On the basis of this table, taking into account the different risks, the different applicable legal disciplines and the role of the child, a number of (problematic) issues, that will have an impact on the creation of risk-reducing regulatory strategies, can be identified:

1. First, although it is possible to identify the broad legal disciplines that might be linked to SNS risks, within these disciplines, there are of course different strands of legislation that will be applicable to specific situations or acts. In practice, this will vary from country to country[3], since even in today's society in which borders are increasingly irrelevant and people are connected worldwide, for instance through social networks, legislation is still very much based on territoriality and states are usually only able to enforce legislation within their borders.
2. Second, when addressing SNS risks for minors, it is essential to differentiate between illegal acts or content and harmful acts or content. Whereas certain acts of bullying might not be serious enough to be classified as illegal (and hence fall under certain criminal provisions), this does not mean that these acts do not harm certain children. Or, whereas certain content, for instance violent or sexual content, might not be considered as illegal by the courts, it might still be considered problematic if certain categories of vulnerable users or viewers are confronted with such content. Although it remains a fact that "what is illegal offline, is also illegal online" a number of SNS risks, more specifically those that are related to harmful or inappropriate conduct and content, will not necessary entail the applicability of specific legislation. In this respect, it can be noted that the "terms and conditions" of SNS providers might provide some indications as to their policies with regard to what they consider to be "harmful behaviour/content"[4].
3. Third, in the era of traditional mass media, information and data were put in the public domain by a limited number of content providers, such as broadcast organisations or newspaper publishers. Public interest goals and fundamental rights (including freedom of expression, protection of minors, cultural diversity, privacy, etc.) have been traditionally safeguarded through a set of obligations imposed on these institutions that are professionally active in the production and dissemination of information. Whereas this limited number of institutions can be controlled with relative ease in a top-down regulatory system, this is much harder in the online social media environment where users themselves are distributing enormous amounts of information, about their personal opinions, their likes and dislikes, their professional activities, or about others.

With regard to minors, this latter trend or paradigm shift from provider/supply-oriented to user/demand-oriented media raises more specific issues:

1. First, as was mentioned in the introduction to this article, there are the changing roles that minors play in the social media eco-system: from passive "victims" to active creators,

data controllers, perpetrators (of various potentially criminal acts: bullying (Palfrey *et al.*, 2010), posting sensitive material, piracy/illegal downloading . . .), journalists, editors, or even sellers? Each of these roles may – in theory – entail different legal consequences and the applicability of specific legislation (e.g. data protection legislation or journalistic deontology). On the one hand, this leads to questions regarding liability. Can minors be held liable for certain acts they commit, or will it be possible to hold parents or educators/schools, or even the social network providers themselves, liable? On the other hand, the fact that minors commit certain criminal acts in the SNS environment has, in certain jurisdictions, such as the United States, led to the application of legislation to situations for which this legislation was not intended. The most obvious example in this context has been the application of child pornography legislation to “sexting”[5] or the distribution of nude pictures by peers[6]. This may lead (and has already led) to the conviction of minors, who took pictures of themselves or their boyfriend or girlfriend (who may be very close in age), to prison sentences and the duty to register as a sex offender for a very long period (Zhang, 2010; Sacco *et al.*, 2010). The rationale behind child pornography legislation has traditionally been to punish adults who sexually abuse and exploit children. Although it may be possible that even when intimate pictures have been taken consensually, without duress, these could later be exploited and lead to harm (for instance when those pictures are distributed on a large scale e.g. when a relationship has ended), it seems disproportionate to apply legislation with such heavy sanctions, and potentially life-ruining consequences to minors.

2. A second issue, closely linked to the roles that minors adopt in a social networking environment, is their awareness of the rights of others: e.g. right to image, privacy (Grimmelman, 2009), copyright, . . . With regard to these rights prior consent is often necessary in order to be allowed to share information about or pictures of other individuals. However, the legal validity of consent by minors is not at all obvious. Depending on the specific jurisdiction, the validity of consent might be dependent on age or in certain instances parental consent might be necessary. Linked to these questions is the question to what extent minors may carry out activities which have legal consequences (e.g. e-payment/electronic transactions), for instance when signing up to specific services which require payment.

3. Legal and regulatory trends in the online environment

From the previous section, it is possible to conclude that the application of “old-school” legislation, which has traditionally been used to protect minors, is confronted with many challenges in the SNS environment. Although the policy goal of protecting minors still remains valid in this environment (Lievens, 2010), traditional regulatory measures become less effective in a social media ecosystem, characterised by its abundance, “globalness” and massive user participation.

This fits in with the broader regulatory trend from centred to decentred forms of regulation that has been noticeable over the past decades. The former type of regulation – also dubbed “command-and-control regulation” – which entails that the state performs all regulatory tasks (creation, implementation and monitoring, and enforcement), increasingly displayed a number of shortcomings, especially in complex sectors. Such shortcomings were for instance the territoriality of traditional legislation (see above), slow legislative processes that cannot keep up with societal evolutions, and a lack of expertise and involvement of knowledgeable actors. As a result, decentred forms of regulation, which are much more flexible and open to the involvement of different actors in the regulatory process, grew in importance. It is this development which can also be credited with the growing enthusiasm for the use of alternative regulatory instruments (ARIs), such as self- and co-regulation. Self-regulation entails the creation, implementation and enforcement of rules by a group of (private) actors with no (or at least minimal) involvement of actors that do not belong to this group (such as the government). Co-regulation is a regulatory strategy that consists of elements of state regulation and elements of self-regulation. A possible co-regulatory construction, for instance, can entail that the state or government takes an initiative to set up an ARI or provides a legal basis to do so,

and that private actors are responsible for the actual implementation. In most cases of co-regulation, a government safety net in case of failure of the self-regulatory elements is established. The enthusiasm for these types of ARIs was reflected in numerous international, EU and Council of Europe (CoE) policy documents within the framework of the “Better Regulation” discourse (OECD, 1995; European Commission, 2001, 2002; European Parliament, Council, and European Commission, 2003).

Since the mid-1990s, in the media sector, pre-eminently a complex sector, and certainly with respect to the protection of minors against online risks, emphasis has been put on less legislation and more alternative regulation. One comment can be made with regard to the trends towards less legislation in this particular domain. Although it is true that, at first sight, one might assume that traditional content regulation rationales, based on the pervasiveness of mass media and large impact of programmes that are simultaneously watched by viewers, lose much of their strength with regard to digital media (characterised by a multitude of information sources and channels, individualised patterns of media consumption and a high degree of choice and control), the reality seems to be more complex. Especially with regard to minors, who have always been protected to a certain extent in all existing media, one can wonder whether the increase of control and choice warrants less regulation[7]. It has been argued that an important element with respect to children’s use of new media is that of “context”. Whereas linear media, such as television or film, offer content within a context “that tells a story or establishes a framework of expectations that is recognised by and makes sense to the consumer” (Millwood Hargrave and Livingstone, 2006), non-linear technologies permit content to be seen out of context (for instance, short clips on YouTube or Facebook, and images received via mobile phone). Other significant differences, which may have an impact on the effects of new media on children and young people, are the facilitated access to (more extreme forms of) content, the growing element of “choice” and the lowered threshold for content production (making it possible, for instance, to take pictures and disseminate them across the whole world by uploading them to a social network) (Millwood Hargrave and Livingstone, 2006). It might be premature to assume that on-demand, user-centric media do not need the same guarantees with regard to the protection of minors as traditional media. In the future, social science might provide an answer to this issue. However, it remains a fact that traditional legislation is not very effective in a social media environment.

4. (Alternative) regulatory initiatives

Policymakers have increasingly become aware of the risks concerning SNS (European Commission, 2008), especially with regard to minors, and a few regulatory initiatives (International Working Group on Data Protection in Telecommunications, 2008; Council of Europe, 2008; Facebook and Attorneys General, 2008; UK Council for Child Internet Safety, 2010; Council of Europe, 2010) have already been taken in order to address certain of these risks. Fitting in with the trends that were described above, these initiatives can mostly be categorised as ARIs in which different stakeholders are involved.

A number of SNS providers, for instance, subscribed to a self-regulatory[8] charter titled “*Safer Social Networking Principles for the EU*” (SSNPs) in February 2009, following a public consultation on online social networking by the European Commission (2008). The pan-European principles have been developed by SNS providers in cooperation with the Commission and a number of NGOs “to provide good practice recommendations for the providers of social networking and other user interactive sites, to enhance the safety of children and young people using their services” (European Social Networking Task Force, 2009). In order to achieve this one of the core elements of the SSNPs is multi-stakeholder collaboration (including SNS providers, parents, teachers and other carers, governments and public bodies, police and other law enforcement bodies, civil society and users themselves). The seven principles that are put forward are the following:

1. Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner.
2. Work toward ensuring that services are age-appropriate for the intended audience.

3. Empower users through tools and technology.
4. Provide easy-to-use mechanisms to report conduct or content that violates the terms of service.
5. Respond to notifications of illegal content or conduct.
6. Enable and encourage users to employ a safe approach to personal information and privacy.
7. Assess the means for reviewing illegal or prohibited content/conduct.

In February 2010, the results of an independent evaluation of the implementation of the SSNPs were made public (Staksrud and Lobe, 2010). This evaluation analysed the self-declaration statements of the signatories to the charter as well a number of services offered by them (Lobe and Staksrud, 2010). Overall, the report showed that there was (significant) room for improvement. As Commissioner Reding (2010) stated:

However, some important measures have not yet been implemented: Less than half of the signatories make minors' profiles visible only to their friends by default; Only half of the tested sites ensure that minors are not-searchable via search engines; Only nine out of 22 sites respond to complaints submitted by minors asking for help. I expect companies who signed up to the Safer Social Networking Principles to take rapid action to improve this situation.

In June 2011, the results of a second assessment of the SSNPs proved also to be disappointing, for instance with regard the principle of ensuring that minors' profiles are accessible only to their approved contacts by default, which only 2 SNS providers were found to comply with (Donoso, 2011; European Commission, 2011).

This raises the question of the effectiveness of this type of regulatory initiative: although the commitment of the SNS providers to take steps to make their services safer is to be applauded, the concrete implementation of such safety measures is of course crucial in order to achieve actual protection. The text of the SSNPs mentions "[t]hese Principles are aspirational and not prescriptive or legally binding, but are offered to service providers with a strong recommendation for their use". This does not provide a solid base for enforcement, nor a compelling incentive for compliance. Hence, the question whether self-regulatory instruments provide enough guarantees with regard to the prevention of certain risks and the protection of fundamental rights and values seems relevant.

5. The use of ARIs in compliance with the broader legal framework

It is very important to be aware of the fact that the use of alternative regulatory instruments does not occur in a legal vacuum. On the contrary, there are fundamental rights and other legal requirements – stemming from conventions, constitutions, laws, jurisprudence and soft law instruments – that need to be respected when creating, implementing and enforcing ARIs. Areas where concerns can arise are, for instance, the protection of fundamental rights, such as freedom of expression, privacy and the right to a fair trial and an effective remedy, internal market regulation, competition rules, and certain implementation requirements (Lievens, 2010).

Within the context of this article it is not possible to address all these different areas, but an analysis of the relevant legal provisions, conducted in a previous research project, showed that there are no legal obstacles which lead to an a priori or absolute exclusion of the use of ARIs to protect minors. However, this general conclusion should be nuanced in two ways. On the one hand, there are a number of requirements which need to be taken into account in order for ARIs to comply with the legal framework (see Table III). ARIs which aim to protect minors against harmful content could possibly restrict other fundamental rights, freedoms and principles, especially the freedom of expression, the right to privacy, internal market legislation and competition rules. Yet, the protection of minors is a goal of public interest, which can, in many cases, be considered a possible justification to restrict the above-mentioned fundamental rights and freedoms. However, measures which interfere with these rights and freedoms should not go beyond what is necessary to achieve this

Table III Legal framework for ARIs

Fundamental rights	Freedom of expression Right to privacy Right to a fair trial Right to an effective remedy	Article 10 ECHR Article 8 ECHR Article 6 ECHR Article 13 ECHR
Internal market	Free movement of goods Free movement of services	Articles 34 to 36 Treaty on the Functioning of the European Union (TFEU) (ex 28 to 30 EC Treaty) Articles 56, 57 and 52 TFEU (ex 49, 50 and 46 EC Treaty) + sector-specific provisions
Competition rules	Prohibition of anti-competitive agreements Prohibition of abuse of dominant position	Article 101 TFEU (ex 81 EC Treaty) Article 102 TFEU (ex 82 EC Treaty)
Implementation requirements	Freedom of choice of methods to implement directives	Article 288 para. 3 TFEU (ex 249 EC Treaty)

aim. Hence, in balancing the different interests at stake, proportionality will be a very important guiding principle. On the other hand, the applicability of certain provisions, typically those that are in theory addressed at states or governments, will depend on the level of government involvement in ARIs. This means that a number of provisions will be more likely to apply when there is a degree of government involvement, as is common with respect to co-regulatory systems. Conversely, self-regulatory systems may fall outside of the protection of the legal framework (except, for instance, when theories, such as the “horizontal effect” theory[9], can be applied). In our opinion, this might be dangerous in a delicate area such as the protection of minors in the online environment. Hence, to protect minors the use of co-regulatory systems, where there is an actual symbiosis between the involvement of the government and other actors, and greater guarantees are provided as to the actual realisation of the policy objective, is preferable. We can frame this finding also within the current general “*malaise*” with respect to self-regulation or regulation by the market or the sector (see for instance, the financial crisis). As a consequence, in different sectors, the calls for a renewed and more intense involvement of the government have recently grown louder.

A second conclusion from the study of the relevant legal provisions is that ARIs should be carefully structured. Attention should not only be paid to the respect for freedom of expression and privacy, but also to issues which may be more easily overlooked such as the respect for procedural guarantees (such as the right to a fair trial and the right to an effective remedy). When important rights are at stake, when decisions are made that might interfere with such rights, the least that can be expected from a decision-making body is adherence to certain procedural safeguards, such as independence, impartiality and transparency (for instance by means of reasoned decisions). Furthermore, such decisions must be disputable.

6. Identifying elements for risk-reducing regulatory strategies in SNS

To conclude this article, an attempt is made to provide a preliminary identification of a number of guidelines for the creation of efficient risk-reducing regulatory strategies for the protection of minors in online social networks:

1. A multi-stakeholder approach is essential. Only regulatory strategies in which the different stakeholders (government, SNS providers, parents, schools and minors) take up part of the responsibility will have a chance of reducing SNS risks. And although parents, schools and users must play an important role, the SNS industry must strengthen their commitment and put more effort in implementing the safety measures they are claiming to provide in a user-friendly and effective manner (Kroes, 2011). In this respect, incentives to comply are of the utmost importance. An incentive may be their social responsibility to profile themselves as providers that feel very strongly about child safety. However, commercial interests will often be considered more important, and in such cases the incentives to comply can be supplied in the form of governmental pressure. Governments do have an important role to play, in ensuring

that initiatives that have been taken by other actors are monitored and evaluated, and if needed, in insisting on a stronger enforcement of those initiatives. Their involvement will provide greater guarantees as to the actual achievement of goals of public interest, *in casu* the protection of minors.

2. In ensuring an appropriate degree of the protection of the right to freedom of expression as well as the right to privacy, two rights that are crucial with respect to the protection of minors in SNS, proportionality is of the utmost importance. This general legislative principle should be the guiding principle when risk-reducing regulatory strategies are established: the measures in question should be suitable to attain the objective that is envisaged and should not go beyond what is necessary to achieve this objective. This also entails that when attempting to protect minors their own rights to freedom of expression and privacy[10] should not be restricted too much.
3. Equally important is the fact that risk-reducing regulatory strategies should ensure a number of procedural guarantees (Council of Europe, 2010). The measures taken should be transparent, and must provide for a right to appeal. Compliance with such guarantees is not only essential for alternative regulatory instruments to be credible; it also ensures that the rights that are at stake are protected in an adequate manner.
4. In order to achieve a comprehensive protection of minors in SNS it is crucial to combine regulatory strategies targeted at illegal and harmful content and conduct. However, a different emphasis will be necessary depending on the nature of the content or conduct that is targeted:
 - With regard to illegal content and conduct, it is necessary to implement and enforce existing legislation in a pragmatic and efficient manner, and in certain instances, consider whether new legislative initiatives are required (Kroes, 2011). However, such initiatives must be creative, must take into account the fast-changing nature of SNS and must address their transborder scope. In any case, the application of legislation which has been drafted with a completely different purpose in mind should be avoided. In addition, it is necessary that awareness and training of law enforcement is increased and that cooperation between law enforcement and SNS providers is improved.
 - With regard to harmful content and conduct, given the findings that the use of technology (which has been promoted to enhance children's online safety since the mid-1990s; e.g. blocking and filtering techniques, age-verification tools) might not be as straightforward in a social media environment (Deloitte and European Commission, 2008; Innova *et al.*, 2011; Grimmelman, 2009), continued efforts are required with regard to the promotion of media literacy, education and awareness-raising. Research into user-empowering and innovative transparency enhancing tools and techniques, peer-review instruments, easy-to-use reporting mechanisms, and age-dependent accounts must continue to be undertaken.

The research that lies at the basis of this article will be continued in the context of several research projects at the Interdisciplinary Centre for Law and ICT. The ultimate goal of this research is to identify the requirements for risk-reducing regulatory strategies aspiring to offer an enhanced and balanced protection of minors in the social media ecosystem, and in this manner, to provide an insight into the changing role of law in today's networked society and innovative regulatory solutions that will be able to deal with the paradigm shift from mass media and passive, vulnerable consumers to media for mass self-communication and active "prosumers".

Notes

1. In the USA, a study found that "73 per cent of wired American teens [ages 12 to 17] now use social networking websites [...]" (Pew Research Center, 2010).
2. Of course, myriad classifications of the different risks that children are exposed to exists. For instance: Walrave (2008): content-related risks, commerce-related risks and contact-related risks;

Biegler and boyd (2011): sexual solicitation and internet-initiated sex crimes involving minors, online harassment and cyberbullying, youth access to problematic content, youth-generated problematic content.

3. For the UK, for instance, an overview is given in: UK Council for Child Internet Safety (2010).
4. E.g. Facebook's terms: "[. . .] You will not bully, intimidate, or harass any user. You will not post content that: is hateful, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence [. . .]" (Facebook, 2011b).
5. Defined as "youth writing sexually explicit messages, taking sexually explicit photos of themselves or others in their peer group, and transmitting those photos and/or messages to their peers" by the US National Center for Missing and Exploited Children: National Center for Missing and Exploited Children (2009).
6. Sacco *et al.* (2010) refer to the fact that "it is important to recognize that young people have been taking sexually provocative photographs since the Polaroid. The difference now is that such images can be produced, transmitted, reproduced, and retransmitted with ease, without the subject's approval or even knowledge, and quickly can reach a much wider audience".
7. This is an argument that has often been put forward within the context of the review of the AVMS directive, Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in member states concerning the provision of audiovisual media services (Audiovisual Media Services Directive), OJ 15.04.2010, L 95/1, recital 58.
8. Even though the label "self-regulation" is attached to this charter, it could be argued that it is a co-regulatory instrument. The Charter was fostered by the European Commission and is evaluated at regular intervals by experts appointed by the Commission: http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm (accessed 17 June 2011). However, strict categorisations of regulatory instruments are rather irrelevant and we advocate the use of the umbrella notion "alternative regulatory instruments" (Lievens, 2010).
9. The complex "horizontal effect XE "horizontal effect" theory entails that if national law accepts the direct effect of the ECHR articles, individuals or private actors can, in certain circumstances, invoke article 10 ECHR before the national courts to challenge other individuals.
10. As for instance laid down in the United Nations Convention on the Rights of the Child.

References

- Biegler, S. and boyd, d. (2011), "Risky behaviors and online safety: a 2010 literature review (draft)", available at: www.zephoria.org/files/2010SafetyLitReview.pdf (accessed 17 June 2011).
- boyd, d. (2008), "Taken out of context: American teen sociality in networked publics", PhD thesis, University of California, Berkeley, CA, available at: www.danah.org/papers/TakenOutOfContext.pdf (accessed 17 June 2011).
- Byron, T. (2008), "Safer children in a digital world: the report of the Byron review", available at: www.education.gov.uk/publications/standard/publicationdetail/page1/DCSF-00334-2008 (accessed 17 June 2011).
- Council of Europe (2008), "Human rights guidelines for internet service providers – developed by the Council of Europe in co-operation with the European Internet Service Providers Association (EuroISPA)", available at: www.coe.int/t/information_society/documents/HRguidelines_ISP_en.pdf (accessed 17 June 2011).
- Council of Europe (2010), "Draft recommendation on measures to protect and promote respect for human rights with regard to social networking services (Committee of experts on new media, 25-26 March 2010)", available at: www.coe.int/t/dghl/standardsetting/media/mc-nm/MC-NM_2010_003_en%20Draft%20Rec%20%20SNS.pdf (accessed 17 June 2011).
- Deloitte and European Commission (2008), "Safer internet: protecting our children on the net using content filtering and parental control techniques (SIP-Bench)" study commissioned by the European Union, available at http://ec.europa.eu/information_society/activities/sip/docs/project_reports/sip_bench_2008_synthesis_report_en.pdf (accessed 17 June 2011).

Donoso, V. (2011), "Assessment of the implementation of the Safer Social Networking Principles for the EU on 14 websites: summary report", study commissioned by the European Commission, available at: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report_11/part_one.pdf (accessed 22 June 2011).

EDPS (2011), "Opinion of the European Data Protection Supervisor on the 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'", available at: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf (accessed 17 June 2011).

Edwards, L. and Brown, I. (2009), "Data control and social networking: irreconcilable ideas?", in Matwyshyn, A. (Ed.), *Harboring Data: Information Security, Law and the Corporation*, Stanford University Press, Palo Alto, CA, pp. 202-27.

Enisa (2007), "Security issues and recommendations for online social networks", position paper, available at: www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks (accessed 17 June 2011).

European Commission (2001), *White Paper on European Governance*, OJ 2001/C 287/1, European Commission, Brussels.

European Commission (2002), *Communication Action Plan "Simplifying and Improving the Regulatory Environment"*, COM (2002) 278 final, European Commission, Brussels.

European Commission (2008), "Public consultation on online social networking", available at: http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating_sns/summaryreport.pdf (accessed 17 June 2011).

European Commission (2010), "A comprehensive approach on personal data protection in the European Union, Communication", COM (2010) 609 final, available at: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf (accessed 17 June 2011).

European Commission (2011), "Digital Agenda: only two social networking sites protect privacy of minors' profiles by default", press release, 21 June, available at: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/762&format=HTML&aged=0&language=EN&guiLanguage=en> (accessed 22 June 2011).

European Parliament, Council, and European Commission (2003), *Interinstitutional Agreement on Better Law-making*, OJ 2003/C 321/01, European Parliament, Council, and European Commission, Brussels.

European Social Networking Task Force (2009), "Safer social networking principles for the EU", available at: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf (accessed 17 June 2011).

Facebook (2011a), "Statistics", available at: www.facebook.com/press/info.php?statistics (accessed 17 June 2011).

Facebook (2011b), "Statement of rights and responsibilities", available at: www.facebook.com/terms.php?ref=pf (accessed 17 June 2011).

Facebook and Attorneys General (2008), "Joint statement on key principles of social networking sites safety", available at: www.state.tn.us/attorneygeneral/cases/facebook/facebookstatement.pdf (accessed 17 June 2011).

Grimmelman, J. (2009), "Saving Facebook", *Iowa Law Review*, Vol. 94 No. 4, pp. 1137-206.

Hasebrink, U., Livingstone, S., Haddon, L. and Ólafsson, K. (2009), "Comparing children's online opportunities and risks across Europe: cross-national comparisons for EU Kids Online", 2nd ed., Deliverable D3.2, LSE, London, EU Kids Online, available at: http://eprints.lse.ac.uk/24368/1/D3.2_Report-Cross_national_comparisons-2nd-edition.pdf (accessed 17 June 2011).

Innova *et al.* (2011), "SIP-BENCH 2: benchmarking of parental control tools for the online protection of children", study commissioned by the European Union, available at: http://ec.europa.eu/information_society/activities/sip/docs/sip_bench2_results/executive_summary_feb11.pdf (accessed 17 June 2011).

International Working Group on Data Protection in Telecommunications (2008), "Rome Memorandum – report and guidance on privacy in social networks", available at: www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdp/working-papers-and-common-positions-adopted-by-the-working-group (accessed 17 June 2011).

Internet Safety Technical Task Force (2008), "Enhancing child safety and online technologies: final report of the ISTTF to the Multi-state Working Group on Social Networking of State Attorney Generals of the United States", Berkman Center for Internet and Society, available at: http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf (accessed 17 June 2011).

Kroes, N. (2011), "Safer Internet Day 2011: protecting children online", speech at Child Focus, Safer Internet Centre in Belgium, 8 February, available at: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/73&format=HTML&aged=0&language=EN&guiLanguage=en> (accessed 17 June 2011).

Lievens, E. (2010), *Protecting Children in the Digital Era: The Use of Alternative Regulatory Instruments*, Martinus Nijhoff Publishers, Leiden.

Livingstone, S. and Brake, D. (2010), "On the rapid rise of social networking sites: new findings and policy implications", *Children and Society*, Vol. 24 No. 1, pp. 75-83.

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, available at: www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx (accessed 17 June 2011).

Lobe, B. and Staksrud, E. (2010), "Evaluation of the implementation of the Safe Social Networking Principles for the EU, part 2: testing of 20 providers of social networking services in Europe", study commissioned by the European Commission, available at: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/sec_part.pdf (accessed 17 June 2011).

Millwood Hargrave, A. and Livingstone, S. (2006), *Harm and Offence in Media Content: A Review of the Evidence*, Intellect, Bristol.

National Center for Missing and Exploited Children (2009), "Policy statement on sexting", available at: www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=4130 (accessed 17 June 2011).

OECD (1995), "Recommendation of the Council of the OECD on improving the quality of government regulation, OCDE/GD(95)95", available at: www.oecd.org/officialdocuments/displaydocumentpdf/?cote=OCDE/GD%2895%2995&doclanguage=en (accessed 17 June 2011).

Palfrey, J., Gasser, U. and boyd, d. (2010), "Response to FCC Notice of Inquiry 09-94 'Empowering parents and protecting children in an evolving media landscape'", on behalf of the Youth and Media Policy Working Group Initiative, Berkman Center for Internet & Society, Harvard University, available at: http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Palfrey_Gasser_boyd_response_to_FCC_NOI_09-94_Feb2010.pdf (accessed 17 June 2011).

Pew Research Center (2010), "Social media and mobile internet use among teens and young adults", available at: http://pewinternet.org/~media/Files/Reports/2010/PIP_Social_Media_and_Young_Adults_Report_Final_with_toplevels.pdf (accessed 17 June 2011).

Reding, V. (2010), "Think before you post! How to make social networking sites safer for children and teenagers?", speech at Safer Internet Day, Strasbourg, 9 February, available at: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/22> (accessed 17 June 2011).

Sacco, D.T., Argudin, R., Maguire, J. and Tallon, K. (2010), "Sexting: youth practices and legal implications", Cyberlaw Clinic, Harvard Law School, available at: http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Sacco_Argudin_Maguire_Tallon_Sexting_Jun2010.pdf (accessed 17 June 2011).

Staksrud, E. and Lobe, B. (2010), "Evaluation of the implementation of the Safer Social Networking Principles for the EU, Part 1: general report", study commissioned by the European Commission, available at: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf (accessed 17 June 2011).

UK Council for Child Internet Safety (2010), "Good practice guidance for the providers of social networking and other user-interactive services", available at: <http://media.education.gov.uk/assets/files/industry%20guidance%20%20%20social%20networking.pdf> (accessed 17 June 2011).

Walrave, M. (Ed.) (2008), "Cyberteens@risk: opportunities and risks of teens' ICT use analysed", Teens and ICT: risks and opportunities (TIRO) research project, available at: www.e-privacy.be/TIRO-summary.pdf (accessed 17 June 2011).

Wong, R. (2009), "Social networking: a conceptual analysis of a data controller", *Communications Law*, Vol. 14 No. 5, pp. 142-9.

Zhang, X. (2010), "Charging children with child pornography – using the legal system to handle the problem of sexting", *Computer Law & Security Review*, Vol. 26 No. 3, pp. 251-9.

Corresponding author

Eva Lievens can be contacted at: eva.lievens@law.kuleuven.be

To purchase reprints of this article please e-mail: reprints@emeraldinsight.com
Or visit our web site for further details: www.emeraldinsight.com/reprints