Lievens, Eva

Conference Paper

Risks for young users on social network sites and the legal framework: Match or mismach?

23rd European Regional Conference of the International Telecommunications Society (ITS), Vienna, Austria, 1st-4th July, 2012

Provided in Cooperation with:
International Telecommunications Society (ITS)

Suggested Citation: Lievens, Eva (2012) : Risks for young users on social network sites and the legal framework: Match or mismach?, 23rd European Regional Conference of the International Telecommunications Society (ITS), Vienna, Austria, 1st-4th July, 2012, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/60357

Risks for young users on social network sites and the legal framework: match or mismatch?

dr. Eva Lievens[1]

eva.lievens@law.kuleuven.be

Abstract

The availability and use of social networking sites creates both opportunities and risks for their young users. This paper evaluates the applicability of the current legal framework to (cyber)bullying and sexting, two types of behaviour that are increasingly occurring between peers in the social networking environment. The analysis includes a mapping of applicable provisions at the European and national level, an analysis of the Terms of Service of two social networking providers and an overview and assessment of self-regulatory initiatives that have been taken by the industry in this area. The ultimate goal is to identify a number of elements for a comprehensive strategy to ensure that risks of cyberbullying and sexting are dealt with in a manner that empowers young users.

Keywords

Social network sites – protection of minors – bullying – sexting – legislation – self-regulation – empowerment

1. Introduction

Over the past five years, the popularity of Social Network Sites (SNS) has increased spectacularly, attracting an extraordinary number of users, of which a significant proportion are teenagers. The recent EU Kids Online study showed that in Europe 77% of 13-16 year olds have a profile on a social networking site (Livingstone et al., 2012). Even though most social network sites put the minimum age required to create a profile at 13,[2] the study also found that 38% of 9-12 year olds are already active on SNS. According to a US study which examined the social media use of 12-17 year olds 80% of American teenagers are active on social network sites, of which 93% are present on Facebook (Lenhart et al., 2011). Recent social science research also shows that smart phones with social networking capabilities are increasingly popular among young people "*suggesting they would 'die' without their*

[1]Dr. Eva Lievens is a Senior Research Fellow of the Research Fund Flanders at the Interdisciplinary Centre for Law & ICT – KU Leuven – IBBT. The research findings presented in this paper are the result of two research projects in which the author is involved at the Interdisciplinary Centre for Law & ICT (www.icri.be): 1/ Risk-reducing regulatory strategies for illegal and harmful conduct and content in online social network sites (Postdoctoral research project funded by Research Fund Flanders; www.fwo.be) and 2/ EMSOC – User empowerment in a social media culture (SBO project funded by Agency for Innovation by Science and Technology; www.iwt.be; www.emsoc.be).

[2] The Statement of rights and responsibilities of Facebook stipulates that "*[y]ou will not use Facebook if you are under 13*". The Terms and Conditions of Netlog state that *"[m]inors should have the permission of one of their parents or legal guardian before registering. In any case, you should be 13 or older to register on Netlog*".

phones, that phones and social networks play a 'massive part' in their relationships, and are shaping most aspects of everyday lives" (Ringrose et al, 2012: 53).

The availability and use of SNS brings both opportunities and risks to their young users. As the Council of Europe put it recently in their *Recommendation on the protection of human rights with regard to social networking services*, SNS have "*a great potential to promote the exercise and enjoyment of human rights and fundamental freedoms, in particular the freedom to express, to create and to exchange content and ideas, and the freedom of assembly*" (Council of Europe, 2012). However, the fact that SNS allow users to communicate through status updates, through messages on 'walls' or through instant messaging, to share photo or video fragments, and to connect with old or new 'friends', also entails a number of risks.

Whereas over the past ten years discourse related to child safety in the online environment often focused on grooming or inappropriate contact between adults and minors, social scientists increasingly argue that "*the success of e-safety campaigns is evident in teenagers' awareness of practices to reduce online risk from strangers, and it is time to shift the focus towards reducing risk from known peers*" (Ringrose et al., 2012: 7). *Bullying* and *sexting* are two examples of (conduct)[3] risks originating from peers that may occur in SNS.

Although sometimes it is mistakenly assumed that the Internet in general, and social networks in particular, function within a legal vacuum, in reality a spectrum of different legal disciplines are applicable to SNS risks (Lievens, 2011). However, at the moment there is a lack of clarity about this as well as a lack of understanding by young people, parents, teachers (de Zwart, 2011) as well as policymakers. This paper will analyse and assess the applicability of the current legal framework to bullying and sexting, taking into account existing legislation and case law, both at the EU and national level. In addition the Terms of Use of two SNS (Facebook and Netlog) related to these specific risks, as well as the commitment of SNS providers to address these issues, for instance through self-regulatory initiatives such as the EU's Safer *Social Networking Principles*, will be examined.

2. Setting the scene

Avoiding moral panic, but acknowledging the (potential impact of the) risks

Bullying has always been part of reality, happening on the playground or around the corner from the school gates, just as teenagers used to take analogue pictures of their boyfriend or girlfriend, which sometimes ended up being seen by others who were not meant to see such intimate images. However, whereas any moral panic surrounding (cyber)bullying or sexting must thus be avoided by all means, the transfer of these offline long existing risks to the online environment, and more specifically the SNS environment, does change their nature, complexity and potential impact (boyd, 2008). The possibility to act anonymously, the 24/7 availability, the lack of non-verbal elements of communication, the lack of an immediate, visible reaction (the so-called 'cockpit effect'), the lack of supervision and the public character of the online environment have been argued to lead to more psychological, emotional and social damage in case of bullying (Walrave et al., 2009). In addition, the technical features of SNS allow comments or images to be "*produced, transmitted, reproduced, and retransmitted with ease, without the subject's approval or even knowledge, and quickly [...] reach a*

[3] For a classification of online risks (content – contact – conduct), cf. Hasebrink et al., 2009.

much wider audience" (Sacco et al., 2010). Before, going to a store, physically handing over a film of intimate pictures to be developed and picking them up ensured a much higher threshold to do so. Of course, the emergence of Polaroid (Sacco et al., 2010) and then digital cameras already drastically lowered this threshold. However, SNS, often accessed by means of a smart phone, do make it significantly easier to share these images with often large groups of individuals, and consequently very quickly control is lost over who may see or further share them. In certain instances the wide sharing of intimate pictures by a previous love interest has already led teenagers to commit suicide (Schmitz and Siry, 2011). Whereas these are of course extreme cases which –fortunately – do not often occur, it reveals the urgency of thinking about bullying and sexting and the legal impact of these phenomena.

Statistics[4]

According to the EU Kids Online study (Livingstone et al., 2011) 6% of 9-16 year olds have been sent nasty or hurtful messages on the Internet. Four in five of those who received such messages were fairly or very upset. 3% of 9-16 year olds admit to having bullied others. Comparing with other risks, it appeared that while bullying is among the least common risks, it is the risk that upsets children most. With regard to sexting the study found that 15% of 11-16 year olds have received sexual messages on the Internet. One quarter of 11-16 year olds who received sexual messages online were bothered or upset. 3% of 11-16 year olds say that they have posted or sent sexual messages online in the past 12 months.

A US study carried out by the Pew Research Center (Lenhart et al. 2011) found similar trends. 8% of teens (12-17 year olds) say they have experienced some form of online bullying, for instance through email, a social network site or instant messaging. Two-thirds of respondents who have witnessed online cruelty have also witnessed others joining in – and 21% say they have also joined in the harassment. Only 2% of respondents state that they have sent sexually suggestive images or videos, but 1 in 6 say they have received them.

Yet, a recent UK study concluded that sexting is far more prevalent than previous studies have demonstrated (Ringrose et al., 2012).

Defining (cyber)bullying and sexting

In order to map the applicability of the existing legal framework, it is necessary to clearly understand what the notions (cyber)bullying and sexting mean.

Bullying has been defined as negative, aggressive behaviour that is intentional, involves an imbalance of power, and is, most often, repeated over time (Olweus, 2011). *Cyberbullying* has been characterised as "*being cruel to others by sending or posting harmful material or engaging in other forms of social cruelty using the Internet or other digital technologies*" (Willard, 2007: 1). Social networks are one environment in which this can happen. Very interesting recent research by Alice Marwick and danah boyd draws attention to the fact that adults and teenagers may have a very different conception of bullying than adults, and may use different notions (for instance 'drama' instead of 'bullying') to refer

[4] Not all statistics relate to sexting or bullying solely on SNS, as research that focuses specifically on these services is currently lacking.

to the same (type of) behaviour (Marwick and boyd, 2011).[5] This may, of course, have a significant impact on research into the occurrence or frequency of such behaviour.

Sexting has been 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*" (National Center for Missing & Exploited Children, 2009) or the "*creating, sharing and forwarding of sexually suggestive nude or nearly nude images*" (Lenhart, 2009: 3) through mobile phones and/or the Internet (Ringrose et al., 2012). Sexting thus refers to "*sexually explicit content communicated via text messages, smart phones, or visual and web 2.0. activities such as social networking sites*" (Ringrose et al., 2012: 9). A number of remarks can be made with regard to this phenomenon. First, the practice of sending sexually suggestive images is of course not limited to young people; adults as well engage in this type of behaviour. However, in the context of this paper we look at sexting by minors. Second, it is important not to lose sight of the fact that for teenagers sexting may be a (legitimate) part of exploring their sexuality. Third, notwithstanding the previous point, research has shown that sexting is often coercive and that it is not easy to draw a line between sexting and bullying (Ringrose et al., 2012). Fourth, a distinction may be made between primary and secondary sexting (Schmitz and Siry, 2011); the first meaning that minors take pictures of themselves and share these pictures with peers themselves, the second meaning that someone forwards or further shares a picture that was sent to him by a person that took a picture of him or herself. Whereas primary sexting can be consensual (unless of course it is the result of coercion), secondary sexting is likely not to be consensual, but rather part of a revenge action (for instance by a previous love interest) or bullying behaviour, and may have a grave impact on the person in the image.

Minors: targets and offenders

A common issue regarding bullying and sexting on SNS is the fact that minors may be, from a legal perspective, both the target[6] as well as the (alleged) offender of the actions. Each of these roles may – in theory – entail different legal consequences. The question arises whether these acts fall under the existing legal framework (for instance criminal law provisions). In addition, this leads to issues regarding liability. Can minors be held liable for certain acts they commit, or will it be possible to hold parents or educators liable? These questions will be addressed in the next section.

3. Application of the legal framework

In this section, we first examine the current legal framework with regard to sexting (3.1.) and bullying (3.2.) both at the European level and the national level (Belgium)[7]. In a second part, we address the potential criminal and civil liability of minors, parents and teachers.

[5] They found that teens (mostly girls) use the notion 'drama' to describe "*a host of activities and practices ranging from gossip, flirting, arguing, and joking to more serious issues of jealousy, ostracization, and name calling*". Using this notion allows them "*to distinguish their actions from adult-defined practices like bullying", letting them frame the social dynamics and emotional impact as inconsequential, allowing them to 'save face' rather than taking on the mantle of bully or victim*" (Marwick and boyd, 2011: 2).

[6] We try to avoid the use of the notion 'victim' to point to minors who are being bullied or who are harmed by sexting.

[7] Please note that it is outside of the scope of this paper to provide an exhaustive and detailed study of the various applicable legal provisions (especially at the national level). Rather, it is the objective of this section to provide an overview of possible types of provisions that may be applied to bullying and sexting.

3.1. Sexting

In several countries sexting has already been addressed by the courts. In the United States, for instance, sexting has led to the application of child pornography, resulting in 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; Haynes, 2012). In Australia as well courts have convicted minors based on child pornography legislation (de Zwart et al., 2011). The rationale behind child pornography legislation has traditionally been to punish adults who sexually abuse and exploit children. It seems disproportionate to apply legislation with such heavy sanctions, and potentially life-ruining consequences, to minors. This has been questioned by various scholars (Schmitz and Siry, 2011), arguing for instance that sexted images should be protected by the right to freedom of expression (and hence would fall within the protection of the First Amendment in the United States) (Haynes, 2012), that child pornography may be re-defined to exclude sexted images or that legislation may be adapted to include an affirmative defense in child pornography statutes for minors who voluntarily self-produce and transmit such images to other minors (Sacco et al., 2010). In Europe, the debate on the legal consequences of sexting is much less active, perhaps because no high-profile cases have yet been brought before a court. It is therefore interesting to examine whether existing provisions, both at the European and national level, could entail similar consequences as in the United States and Australia.

3.1.1. European level

Council of Europe

Two conventions adopted by the Council of Europe contain provisions related to child pornography: the *Budapest Convention on Cybercrime* (Article 9) (Council of Europe, 2001) and the *Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (Article 20) (Council of Europe, 2007). The focus of article 9 of the Cybercrime Convention is the criminalisation of child pornography offences (producing, distributing, offering, making available, procuring or possessing) 'through a computer system'. In the Cybercrime Convention, 'child pornography' is defined as "*pornographic material that visually depicts: a minor engaged in sexually explicit conduct, a person appearing to be a minor engaged in sexually explicit conduct, realistic images representing a minor engaged in sexually explicit conduct*". The term 'minor' includes "*all persons under 18 year of age*". However, a Party may require a lower age-limit, provided that it is not less than 16 years. The explanatory report to the Cybercrime Convention clarifies exactly what is understood by the notion 'child pornography':

> *99. The term 'pornographic material' in paragraph 2 is governed by national standards pertaining to the classification of materials as obscene, inconsistent with public morals or similarly corrupt. Therefore, material having an artistic, medical, scientific or similar merit may be considered not to be pornographic. The visual depiction includes data stored on computer diskette or on other electronic means of storage, which are capable of conversion into a visual image.*
> *100. A 'sexually explicit conduct' covers at least real or simulated: a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal,* ***between minors****, or between an adult and a minor, of the same or opposite sex; b) bestiality; c)* ***masturbation****; d) sadistic or masochistic abuse in a*

> *sexual context; or e)* ***lascivious exhibition of the genitals or the pubic area of a minor****. It is not relevant whether the conduct depicted is real or simulated.*
> *101. The three types of material defined in paragraph 2 for the purposes of committing the offences contained in paragraph 1 cover depictions of sexual abuse of a real child (2a), pornographic images which depict a person appearing to be a minor engaged in sexually explicit conduct (2b), and finally images, which, although 'realistic', do not in fact involve a real child engaged in sexually explicit conduct (2c). This latter scenario includes pictures which are altered, such as morphed images of natural persons, or even generated entirely by the computer.*[8]

It can be concluded from the definition of 'child pornography' and the explanation thereof, that sexting could be interpreted as falling within the scope of application of this Convention. Sexting images may picture "*sexual intercourse between minors*", "*masturbation*" or "*lascivious exhibition of the genitals or the pubic area of a minor".* Whether this will be considered 'pornographic material' will ultimately be a decision of the courts who will take into consideration the national standards at that time.

Article 20 of the Lanzarote Convention also deals with the criminalisation of producing, offering, making available, distributing, transmitting, procuring, possessing and, knowingly obtaining access (through information and communication technologies) to child pornography (para. 1), which is defined as "*any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes*" (para.2). However, the third paragraph states that "*[e]ach Party may reserve the right not to apply, in whole or in part, paragraph 1.a and e to the production and possession of pornographic material: [...] involving children who have reached the age set in application of Article 18, paragraph 2, where these images are produced and possessed by them with their consent and solely for their own private use*". This means that Member States can decide that sexting between minors that have reached the age of sexual consent,[9] at least as far as producing and possessing it is concerned ('primary sexting'), should be excluded from child pornography legislation. However, it also implies that this is not the case for sexting between minors that have not reached this age nor for offering, making available, distributing, transmitting, procuring or knowingly obtaining access to this type of material.

European Union

In December 2011, the European Union adopted the *Directive on combating the sexual abuse and sexual exploitation of children and child pornography*.[10] The approach of this Directive to offences concerning child pornography is similar to the approach of the Lanzarote Convention. Article 5 contains the (range of) punishments that should be applied to the acquisition, possession, knowingly obtaining access to, distribution, dissemination, transmission, offering, supplying or making available

[8] Emphasis added by the author.
[9] Note that article 18 para. 3 also excludes consensual sexual activities between minors from the scope of article 18 para. 1 which states that "*[e]ach Party shall take the necessary legislative or other measures to ensure that the following intentional conduct is criminalised: a engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities*".
[10] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:EN:PDF.

of child pornography (para. 2-6). In addition article 8 specifically allows Member States to decide whether article 5(2) and (6) apply to the production, acquisition or possession of material involving children who have reached the age of sexual consent where that material is produced and possessed with the consent of those children and only for the private use of the persons involved, in so far as the acts did not involve any abuse. As recital 20 put it:

> *This Directive does not govern Member States' policies with regard to **consensual sexual activities** in which children may be involved and which can be regarded as the normal discovery of sexuality in the course of human development, taking account of the different cultural and legal traditions and of new forms of establishing and maintaining relations among children and adolescents, **including through information and communication technologies**.[11] These issues fall outside of the scope of this Directive. Member States which avail themselves of the possibilities referred to in this Directive do so in the exercise of their competences.*

This can be interpreted as a clear signal that Member States may exclude 'unproblematic' sexting, i.e. types of consensual primary sexting, from child pornography legislation.

Another relevant legislative document is the Data Protection Directive,[12] which asserts that personal data, such as photos, may only be processed if the data subject has unambiguously given his consent (article7). In its *Opinion on online social networking*, the Article 29 Working Party recommended that "*users should only upload pictures or information about other individuals, with the individual's consent*".[13]

3.1.2. National level: Belgium

Criminal provisions

In Belgium, a number of articles of the Criminal Code may be relevant with regard to sexting. Article 383 criminalises the display, sale or distribution of writings or images that are indecent. If this is done in the presence of minors below the age of 16 more severe sentences are imposed according to article 386. In addition, article 384 stipulates that the production of indecent writings or images is also a criminal offence. Child pornography is addressed in article 383bis of the Criminal Code. This article criminalises the display, sale, rental, distribution, transmission, delivery, possession or (knowing) obtainment of access of or to images that depict poses or sexual acts with a pornographic character which involve or depict minors. All articles are formulated in a technology-neutral and broad manner, so in theory they could be applied to social networking and sexting.

Right to image / privacy

Article 10 of the Copyright Act prohibits the author or owner of a portrait from reproducing or communicating it to the public without the consent of the person that is portrayed. In addition, posting or sharing a picture of someone else can also be qualified as the processing of personal data (supra). This entails the application of the Data Protection Act which also requires the consent of the person involved (Article 5). In cases of secondary sexting these Acts could thus be violated.

---

[11] Emphasis added by the author.

[12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 concerning the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[13] Cf. also Van Alsenoy et al., 2009; European Data Protection Supervisor, 2010.

3.1.3. Interim conclusion

At the European level, the more recent legislative documents clarify that the rationale of child pornography legislation is not to criminalise consensual sexual conduct between minors that have reached the age of sexual consent. This is both in the Lanzarote Convention and Directive 2011/92/EU limited to the production and possession of sexual images. Distribution or transmission of such images may still fall within their scope of application. Although the further transmission of images (secondary sexting) may certainly cause harm, the question remains whether this type of 'offenses' should be dealt with on the basis of the provisions that are aimed fighting child pornography. A new, carefully tailored legal provision to address this may be more appropriate. A relevant consideration is whether this should be a criminal provision or not (van der Hof and Koops, 2011). In any case, if harm does occur, it will be possible to rely on the provisions related to civil liability (infra).

Two issues may be mentioned. First, difficulties may arise when the age of sexual consent and the age used in provisions that are applied to sexting diverge.[14] This can lead to situations where minors can legally engage in sexual conduct but may not take pictures that are sexually suggestive. Although from certain perspectives this may be desirable since harm may follow if the images are used involuntarily at a later date, one may wonder whether every type of conduct that can potentially lead to harm should be regulated. At the very least, this situation may be confusing to teenagers, who may not be aware of this divergence. Second, on the basis of the image itself it may be very difficult to assess whether the image was taken voluntarily or not, as consensual sexted images may look exactly the same as images that can be classified as child pornography (Sacco et al., 2010). It will thus be very important to judge each case on an individual basis, taking into account the intention of the minors involved and the particular circumstances.

3.2. Bullying

3.2.1. European level

Council of Europe

The Council of Europe has pointed to the importance of addressing cyberbullying in several documents, such as the Recommendation on empowering children in the new information and communications environment (Council of Europe, 2006), the Declaration on protecting the dignity, security and privacy of children on the Internet (Council of Europe, 2008), the Recommendation on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment (Council of Europe, 2009) and the Recommendation on the protection of human rights in social networks (Council of Europe, 2012). Aside from these recommendations and declarations there are no binding legislative provisions at Council of Europe that might be specifically applied to cyberbullying on social networks.

[14] This is the case in Belgium: the age of sexual consent is 16, the age used in the criminal code for instance with regard to article 383bis related to child pornography is 18.

European Union

The European Union as well has repeatedly pointed out that cyberbullying is an important issue that needs to be tackled, for instance in the framework of the Safer Internet Programme,[15] or in the European Strategy for a better internet for children (European Commission, 2012).

With regard to legislation, the most relevant and applicable provisions are included in the Data Protection Directive (supra). As the European Data Protection Supervisor has stated:

> *When individuals put information about third parties, for example, comments on their appearances or behaviors, independently of whether this constitutes legally cyber-harassment, they disclose personal information of their victims. For example, their real name, their address, school, etc. The principles and obligations embodied in the EU data protection legislation are fully applicable to the disclosure of this information, which under EU legislation qualifies as personal data, for example, in forums or social networks. For example, data protection legislation requires informing and in many cases obtaining the consent of individuals before publishing information that relates to them. Obviously, those engaged in cyber harassment do not inform, much less ask for the consent of their victims to publish their personal data, thus, automatically breaching data protection legislation.* (European Data Protection Supervisor, 2010: 4)

It is possible to file a complaint with the national Data Protection Authority or go to court in case of a violation of the Data Protection Directive.

3.2.2. National level: Belgium

Given that cyberbullying in social networks may encompass a wide range of behaviour or acts, different legal provisions may applicable.[16]

Criminal provisions

A first provision that may be applicable is article 145 §3bis of the Act of 13 June 2005 on electronic communications[17] which criminalises 'harassment by electronic communication means'. Different elements must be present in order for this article to be applicable. First, the harassment must be done by electronic means, this includes the Internet and SNS. Second, the perpetrator must have the intention to harass, and third, the harassment must be done vis-à-vis a 'correspondent'. This implies that there must be some form of interaction between the perpetrator and the target (Walrave, 2009).

The Criminal Code also contains a number of provisions that may applicable to bullying in social networks. In addition to article 383, 384, 386 and 383bis which have been discussed with regard to sexting (supra), article 422bis of the Criminal Code may be applied to bullying. This article punishes persons who menace an individual, while they knew or should have known that through their behaviour they would seriously disturb the peace of that individual. Moreover, the article specifies that if the targeted individual is particularly vulnerable because of a.o. age the punishment is doubled.

[15] Decision No 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 establishing a multiannual Community programme on protecting children using the Internet and other communication technologies.

[16] Note that some of the provisions that are discussed in this section may also be applicable to cases of 'sexting' when sexting is part of a bullying situation.

[17] http://www.bipt.be/ShowDoc.aspx?objectID=951&lang=en.

Four conditions must be fulfilled to be able to apply the article: menacing or harassing behaviour, a serious disturbance of the peace of the targeted individual, a causal link between the first two elements and the fact that the perpetrator knew or should have known that this behaviour would cause the disturbance. The crime can only be prosecuted if a complaint has been lodged.

It is also possible that cyberbullying in the SNS environment is classified as libel or defamation. Article 443 of the Criminal Code considers that a person who maliciously charges someone of a certain fact, which may offend his honour or may expose him to public contempt, and which is not legally proven, is guilty of libel if the charge is not proven, or defamation when the law does not allow this proof. Article 444 Criminal Code determines the punishment (imprisonment and fine) that will be applied when the charges occur

- in public meetings or places; or
- in the presence of several individuals in a place which is not public, but nevertheless accessible to a number of individuals which have the right to meet or visit; or
- wherever, in the presence of the offended individual and witnesses; or
- by means of writings, printed or not, by means of pictures or symbols, which are posted, distributed or sold, being offered for sale or publicly exhibited; or
- by means of writings which have not been made public, but which have been sent or communicated to several individuals.

It has been argued that defamation and libel on the Internet may fall within the scope of article 443 and 444 of the Criminal Code (Uyttendaele, 2002). In addition, article 448 of the Criminal Code punishes persons who offend or insult someone by means of writings or images. The perpetrator must have a malicious intent and the insult must be public (according to article 444, supra) (Walrave et al., 2009).[18] These articles could also be applicable in the SNS environment.

Finally, in certain cases it may be possible that cyberbullying involves acts of hacking (article 550bis Criminal Code), sending of viruses (article 550ter Criminal Code) or forgery by means of informatics (article 210bis, para. 2 Criminal Code) (Walrave et al., 2009).

The right to image / privacy

If a certain cyberbullying situation involves the use of images, the same provisions of the Copyright Act and the Data Protection Act that were discussed in the section about sexting (supra) may apply.

3.2.3. Interim conclusion

A number of existing legislative provisions can be applicable to cases of cyberbullying on SNS. In Belgium, most of these provisions are formulated in a technology-neutral manner, which implies that they may be applied in a SNS environment. There is thus no need for new legislation to address this issue. However, this does not mean that the application of the articles may not be confronted with obstacles. Problems that may arise for instance are the potential anonymity of perpetrators and the fact that the majority of popular SNS providers are located abroad, hindering effective enforcement of the national legislative provisions (infra).

[18] This article could also be applicable in instances of sexting.

3.3. Liability of minors

Given that (in the framework of this research) acts of sexting or cyberbullying are being committed by minors, the question arises whether they can be held liable for these acts. In this section, we look at the situation in Belgium. The Youth Protection Act of 1965 states that minors cannot be put on a par with adults with regard to the degree of liability and the consequences of their actions (Preamble, para. 4). However, if a minor commits an 'act that is described as a crime' they should be made aware of the consequences of that offence. As a result, the Youth Protection Act does impose, instead of the punishments of the Criminal Code, other measures, including supervision, education, disciplinary measures, guidance, advice or support. Measures can be imposed on parents or on the minors themselves. The age of the minor in question is taken into account; different measures will be imposed before and after the age of 12 years (article 37). If possible, the judge may give preference to victim-offender mediation (article 37bis).

In addition, from the moment that they are able to discern the scope of their actions, minors may be held civilly liable. This will be assessed on a case-by-case basis but judges have held that this may be as early as the age of seven (Walrave et al., 2009). On the basis of article 1382 and 1383 of the Civil Code, to be held liable the victim must prove the offence and the causal link with the damage that this offence has caused. This entails that the offender has not acted as a normal, reasonable and careful person, that he or she acted freely and consciously and that he or she must have been able to foresee that his or her behaviour would cause damage to the victim (Walrave et al., 2009). One may wonder whether, for instance in the case of sexting, minors can reasonably foresee the consequences of their actions. This is something that the judge will need to evaluate in each specific case.

It can be added that parents and teachers may in certain circumstances be held liable for the acts of their children or pupils. For parents as well as teachers an assumption of liability has been included in article 1384 of the Civil Code. This means that, in order not to be held liable, the parents and teachers in question must prove that they did not commit a mistake in raising or supervising the child (Walrave et al., 2009). Walrave et al. argue that supervision with regard to a child's activities online is very difficult and advocate evolving towards a liability system without fault that would require an obligatory insurance (Walrave et al., 2009).

4. Terms of services of SNS

In addition to existing legislative provisions, the Terms of Service (ToS) of SNS providers may also contain stipulations with regard to sexting, cyberbullying and the consequences that may be attached to such behaviour. In this section we list the relevant clauses of the ToS of Facebook and Netlog.

Facebook

The *Statement of Rights and Responsibilities* of Facebook stipulates that:

> *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.*
>
> *We respect other people's rights, and expect you to do the same.*

> *You will not post content or take any action on Facebook that infringes or violates someone else's rights or otherwise violates the law.*

Elaborating on these principles, the Facebook *Community Standards* state that:

> *Facebook does not tolerate bullying or harassment. We allow users to speak freely on matters and people of public interest, but take action on all reports of abusive behavior directed at private individuals. Repeatedly targeting other users with unwanted friend requests or messages is a form of harassment.*
>
> *Facebook does not permit hate speech. While we encourage you to challenge ideas, institutions, events, and practices, it is a serious violation to attack a person based on their race, ethnicity, national origin, religion, sex, gender, sexual orientation, disability or medical condition.*
>
> *Facebook has a strict policy against the sharing of pornographic content and imposes limitations on the display of nudity. At the same time, we aspire to respect people's right to share content of personal importance, whether those are photos of a sculpture like Michelangelo's David or family photos of a child breastfeeding.*
>
> *Before sharing content on Facebook, please be sure you have the right to do so. We ask that you respect copyrights, trademarks, and other legal rights.*

Netlog

The *Terms & Conditions* of Netlog include the following clauses:

> *All public data cannot be in violation of any law or statute. You explicitly accept this statement and you are responsible (according to civil and criminal law) for the data, text and pictures that you publish.*
>
> *All data you upload or post cannot violate or infringe upon the rights of authors, patents, trademarks or trade secrets, or the property, intellectual, privacy, personality or publicity rights of a third party.*
>
> *All data you upload or post cannot be misleading, threatening, defamatory or tormenting.*
>
> *You cannot use this Website in an irregular manner, for any unlawful purpose or any purpose contrary to the conditions and warnings in this text or in any other text. You have to use the entire Website as a normal, careful and reasonable human being.*

Netlog's *Code of conduct* states that

> *In order for everyone to be able to enjoy Netlog, you need to follow a few rules. The following acts are prohibited by law and, thus, subject to punishment:*
>
> *Racism, xenophobia, negationism, and discrimination (prison sentences). Racist remarks, propagating discrimination of sexual preferences, publishing racist pictures or insulting foreigners are forbidden on Netlog.*
>
> *Public offences, publishing sexually suggestive pictures, pedophilia, offering prostitution or escort services and implicit or explicit invitations for sexual activities. Uploading pornographic, sexually suggestive or overtly erotic pictures/text is forbidden. Invitations for sexual activities in public or by private messages are also prohibited. Humorous or caricatural pictures can be an exception, as long as the humorous character is predominant.*
>
> *Slander, defamation, stalking, abusing someone's name or picture, abuse of confidence, etc. are prohibited by law and subject to punishment. Therefore, using abusive language, insults, abusing someone's name or picture, slander and defamation are forbidden on Netlog as well.*
>
> *It is strictly forbidden to publish messages or pictures with damaging, threatening, misleading, defamatory, rancorous, aggressive, racist, vulgar, denigrating, indecent, insulting, violent, obscene or pornographic content.*

> *On Netlog you can only publish content (pictures, text, music, films, etc.) for which you hold the necessary copyrights. You are solely responsible for obtaining these rights.*

Issues and implications

It is clear from both Facebook and Netlog's ToS that sexting nor bullying are tolerated on their respective networks. However, four issues can be identified.

First, the ToS indicate that Facebook is subject to US law,[19] and that Netlog is subject to Belgian law.[20] This leads to significant conflict of law issues, entailing that in many cases the enforcement of the national legislative provisions will be problematic. However, in a recent case in France, a judge declared himself competent in a dispute concerning Facebook.[21] It remains to be seen whether this will be upheld in the future.

Second, the question arises to what extent agreements such as the ToS are binding on minors and whether they are capable of agreeing to these ToS. In Belgium, for instance, article 1124 of the Civil Code declares minors incapable of entering into a contract. However, in certain instances, including if they have an adequate 'discerning capability' the agreement in question may be found valid and violations may hence be enforced. However, a relevant question is whether, when agreeing to the ToS, the minor knows and understands the content of the ToS. The ToS are often very extensive, drawn up in complex language, and easy to agree to without having read the full text. Awareness of minors with regard to these ToS should be improved.[22]

Third, if the ToS are violated the SNS providers may apply various sanctions, such as removing content, suspending or deleting accounts.[23] However, according to national legislation certain clauses of contracts may be considered invalid if they are too one-sided or if there is a manifest imbalance of rights and responsibilities. Of course, again, jurisdictional issues may arise with regard to disputes concerning the validity of ToS. In any case, it is very important to note that SNS providers have a crucial role in addressing issues of cyberbullying and sexting on their networks. It is important that if they receive complaints about such behaviour they promptly act upon them, warn offenders that this type of behaviour is not tolerated and apply sanctions if necessary.

Four, the ToS of SNS include clauses which deny any liability for content or behaviour of users on their networks. It is possible that under certain national legislation and in particular circumstances such clauses will be considered invalid. In this context, we can also refer to the e-Commerce

[19] "*The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions. You agree to submit to the personal jurisdiction of the courts located in Santa Clara County, California for the purpose of litigating all such claims*".
[20] "*The use of this Website shall be governed by the Belgian laws. In case of dispute concerning the use of the Website or services of this Website the courts located within Brussels have jurisdiction*."
[21] Court of Appeal of Pau, First Chamber, Judgement of 23 March 2012, http://www.legalis.net/spip.php?page=breves-article&id_article=3382 ([in French].
[22] Industry has committed to this in the framework of various self-regulatory initiatives, cf. infra.
[23] E.g. the ToS of Netlog stipulate that "*Massive Media may cease to provide the service, as well as block or delete a membership at any time and without warning*".

Directive[24] which includes a number of provisions related to the exemption of liability of intermediaries, for instance for hosting providers, such as social networks.[25] Article 14 stipulates that

> *"where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider is* ***not liable*** *for the information stored at the request of a recipient of the service, on condition that:*
>
> *(a) the provider* ***does not have actual knowledge of illegal activity or information*** *and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or*
>
> - *(b)* ***the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information*** *and if he acts according to the following procedure: when the provider obtains actual knowledge of the illegal activity or information, he immediately reports it to the public prosecutor who takes action according to article 39bis of the Code of Criminal Procedure*
> - *as long as the public prosecutor has not made any decision with regard to the copying, disabling access and removing of stored data, the provider can only take measures as to prevent access to the information.*
>
> *The exemption does not apply when the recipient of the service is acting under the authority or the control of the provider".*[26,27]

Whereas this provision may be relevant in the context of cyberbullying or sexting in order to assess whether the SNS provider may be held liable for certain acts, again potential conflicts of law may arise.

5. Self-regulation: the role of social networking providers

During the past 3 years SNS providers and other companies have taken initiatives to ensure a safer internet for children.

Safer Social Networking Principles for the EU

In February 2009, a number of SNS providers subscribed to a self-regulatory[28] charter titled '*Safer Social Networking Principles for the EU*' (SSNPs) following a public consultation on online social networking by the European Commission (European Commission, 2008).[29] The pan-European

[24] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:En:HTML.
[25] Cf. European Court of Justice, SABAM v. Netlog, 16 February 2012.
[26] Emphasis added by the author.
[27] It can also be noted that article 15 e-Commerce Directive states that providers do not have a general obligation to monitor their services. The European Court of Justice confirmed that this article is also applicable to SNS providers, and that, for instance, the installation of a general filter system cannot be imposed on them: European Court of Justice, SABAM v. Netlog, 16 February 2012.
[28] 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. However, we have argued that strict categorisations of regulatory instruments are rather irrelevant (Lievens, 2010).
[29] In the United States in 2008 the *Joint statement on key principles of social networking safety* was adopted (Facebook & Attorneys General, 2008).
.

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 goal 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 were put forward are the following:

> *Principle 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*
>
> *Principle 2: Work toward ensuring that services are age-appropriate for the intended audience*
>
> *Principle 3: Empower users through tools and technology*
>
> *Principle 4: Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service*
>
> *Principle 5: Respond to notifications of illegal content or conduct*
>
> *Principle 6: Enable and encourage users to employ a safe approach to personal information and privacy*
>
> *Principle 7: Assess the means for reviewing illegal or prohibited content/conduct*

Especially important in the context of cyberbullying and sexting are the availability of reporting mechanisms and the response from the SNS providers to complaints or reports (Livingstone, 2012; Ringrose et al., 2012; European Commission, 2012).

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 and evaluated a number of services offered by them (Lobe and Staksrud, 2010). Overall, the report showed that there was (significant) room for improvement. With regard to reporting mechanisms the evaluation showed that only 9 out of 22 sites responded to complaints submitted by minors asking for help (Staksrud and Lobe, 2010).

In June and September 2011, the results of a second assessment of the SSNPs proved also disappointing, for instance with regard the principle of ensuring that minors' profiles are accessible only to their approved contacts by default, which only four SNS providers were found to comply with (Donoso, 2011a and 2011b; European Commission, 2011a). Whereas this evaluation found that almost all services offer age-appropriate, user-friendly, easily accessible and always available reporting mechanisms, still only 17 out of 23 services responded to complaints or reports,[30] sometimes taking up to 10 days to do so (Donoso, 2011a and 2011b). According to the report these responses ranged from "*personalised e-mails explaining to minors how to delete the offending content themselves and giving minors concrete tips on how to deal with this type of situation to replies mentioning that the offending content had been/would be reviewed and eventually removed from the site*" (Donoso, 2011a: 10-11).

The results of these evaluations raise 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

[30] The reporting mechanisms were tested by "*creating a realistic bullying situation on the SNS where a fake 'bullied child' contacted the provider asking for help to remove offending content posted on her profile*" (Donoso, 2011a: 10).

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. Yearly evaluations must thus continue to be undertaken, the results thereof must be publicised widely and, if necessary, the European Commission should consider taking appropriate measures.

CEO Coalition

In December 2011, 28 companies voluntarily formed the *Coalition to make the Internet a better place for kids* and published a Statement of purpose (Coalition to make the Internet a better place for kids, 2011). This self-regulatory initiative is an answer to a call for action from the European Commission and has been endorsed by Commissioner Kroes (European Commission, 2011b). Social network providers such as Facebook and Netlog have also joined this coalition. In order to achieve their goal the coalition has drafted a work plan which runs from December 2011 until December 2012, and focuses on 5 concrete action points:

- *Simple and robust reporting tools for users*
- *Age appropriate privacy settings*
- *Wider use of content classification*
- *Wider availability and use of parental controls*
- *Effective takedown of child abuse material*

ICT Coalition for a Safer Internet for Children and Young People

In January 2012 another industry initiative was launched. 25 companies, including Facebook and Google, formed the ICT Coalition for a Safer Internet for Children and Young People, and issued the *Principles for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU* (ICT Coalition for a Safer Internet for Children and Young People). Their focus is on

- *Content*
- *Parental controls*
- *Dealing with abuse/misuse*
- *Child sexual abuse content or illegal contact*
- *Privacy and control*
- *Education and awareness*

Towards an actual implementation of self-regulation

Industry seems to be very active and committed to make Internet and SNS use safer for minors. Over the past decade calls have grown louder for industry to take up their responsibility in this area, and it must be welcomed that they take initiatives to do so. With regard to cyberbullying and sexting the importance of raising awareness and providing young users with the mechanisms to report harmful behaviour cannot be overestimated. However, the implementation of these initiatives must be evaluated on a regular basis and policymakers and civil society must call on industry to ensure that the work programmes are actually carried out. The three 'coalitions' that are currently active consist of different constellations of companies (some companies, such as Facebook, are a member of the three coalitions) and put forward largely similar principles, with different emphases. The European

Commission could play a role in observing and guiding the different initiatives in order to avoid fragmentation, discrepancies or contradictions.

6. Conclusion

Answering the question in the title of this paper is not straightforward. Although we may conclude that with regard to cyberbullying the existing legislative provisions might be a sufficient match to the problem, we have also tried to illustrate that in concrete cases practical difficulties may arise which hamper the enforcement of the existing legislation, such as conflicts of law or anonymity of offenders. In the case of sexting, the answer leans more to a mismatch between the issue and the current legislative framework, as in our view, sexting should not be criminalised on the basis of child pornography legislation. If policymakers decide that new legislation needs to be drafted, such legislation will need to be carefully considered, addressing questions such as how to define sexting in a future-proof manner, how to distinguish between primary and secondary sexting, and which age (range) to protect (what about near-age-peers?). In our view, in any case, only secondary sexting could be the subject of new (criminal) legislation. Whereas the harm that can result from secondary sexting is evident, with regard to primary sexting this is far less the case. In this context, we may wonder whether the rights to freedom of expression and privacy that have been attributed to minors by the United Nations Convention on the Rights of the Child do not preclude the creation of legislation to address primary sexting that happens on a consensual basis.

Recent research emphasises that "*[w]hile recognising that measures to reduce specific risks have their place, it is also important to develop strategies to build children's resilience and to provide resources which help children to cope with or recover from the effects of harm*" (Livingstone et al. 2012). Hence, in addition to the appropriate enforcement of legislative provisions in cases where this is called for, a comprehensive strategy to ensure that risks of cyberbullying and sexting are dealt with in a manner that empowers young users should also aim to:

- increase awareness of young users of the fact that certain behaviour may have serious consequences (such as the applicability of criminal law);
- provide young users with tools that enable them to report harmful behaviour;
- educate parents, teachers as well as other actors, such as law enforcement and judges, on cyberbullying and sexting practices and their possible legal impact;
- require SNS providers to take these issues seriously, invest in safety and respond to reports of cyberbullying and sexting in a suitable manner without delay; and
- evaluate all measures that are taken regularly and critically, on the basis of up-to-date sociological, technical and legal research.

References

boyd, danah (2008), *Taken out of context: American teen sociality in networked publics*, Ph.D. Thesis, University of California, Berkeley, http://www.danah.org/papers/TakenOutOfContext.pdf.

Coalition to make the Internet a better place for kids (2011), Statement of purpose and work plan, http://ec.europa.eu/information_society/activities/sip/docs/ceo_coalition_statement.pdf.

Council of Europe (2001), Convention on Cybercrime, ETS No. 185, 23 November 2001, Budapest, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

Council of Europe (2006), Recommendation Rec(2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment, https://wcd.coe.int/ViewDoc.jsp?Ref=Rec(2006)12&Sector=secCM&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

Council of Europe (2007), Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No. 201, 25 October 2007, Lanzarote, http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm.

Council of Europe (2008), Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet, https://wcd.coe.int/ViewDoc.jsp?Ref=Decl(20.02.2008)&Language=lanEnglish&Ver=0001&Site=COE&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

Council of Europe (2009), Recommendation CM/Rec(2009)5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment, https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2009)5&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

Council of Europe (2012), Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services, https://wcd.coe.int/ViewDoc.jsp?id=1929453&Site=CM.

de Zwart, Melissa, Lindsay, David, Henderson, Michael and Philips, Michael (2011), *Teenagers, legal risks & social networking sites*, http://newmediaresearch.educ.monash.edu.au/moodle/pluginfile.php/2117/mod_label/intro/SNSandRisks_REPORT.pdf.

Donoso, Veronica (2011a), "Assessment of the implementation of the Safer Social Networking Principles for the EU on 14 websites: Summary Report" (Study commissioned by the European Commission), http://ec.europa.eu/information_society/activities/social_networking/docs/final_report_11/part_one.pdf.

Donoso, Veronica (2011b), "Assessment of the implementation of the Safer Social Networking Principles for the EU on 9 services: Summary Report" (Study commissioned by the European Commission), http://ec.europa.eu/information_society/activities/social_networking/docs/final_reports_sept_11/report_phase_b_1.pdf.

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

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

European Commission (2011b), "Digital Agenda: Coalition of top tech & media companies to make internet better place for our kids [sic]", Press release 1 December 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1485.

European Commission (2012), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Strategy for a Better Internet for Children, COM(2012) 196 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:EN:PDF.

European Data Protection Supervisor (2010), Data protection legislation in Europe, preventing cyber-harassment by protecting personal data and privacy, http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-06-07_Speech_Cyber-harassment_EN.pdf.

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

Facebook & Attorneys General (2008), "Joint statement on key principles of social networking sites safety", http://www.state.tn.us/attorneygeneral/cases/facebook/facebookstatement.pdf.

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, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf.

Hasebrink, Uwe, Livingstone, Sonia, Haddon, Leslie and Ólafsson, Kjartan (2009), "Comparing children's online opportunities and risks across Europe: cross-national comparisons for EU Kids Online, 2nd edition, Deliverable D3.2.", LSE, London, EU Kids Online, http://eprints.lse.ac.uk/24368/1/D3.2_Report-Cross_national_comparisons-2nd-edition.pdf.

Haynes, Antonio M. (2012), "The age of consent: when is sexting no longer 'speech integral to criminal conduct'", *Cornell Law Review*, Vol. 97, 369-404.

ICT Coalition for a Safer Internet for Children and Young People (2012), Principles for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU, http://www.gsma-documents.com/safer_mobile/ICT_Principles.pdf.

Lenhart, Amanda (2009), Teens and sexting: how and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging?, Pew Research Center Report, http://www.pewinternet.org/~/media//Files/Reports/2009/PIP_Teens_and_Sexting.pdf.

Lenhart, Amanda, Madden, Mary, Smith, Aaron, Purcell, Kristen, Zickurh, Kathryn and Rainie, Lee (2011), Teens, kindness and cruelty on social network sites, Pew Research Center Report, http://pewinternet.org/Reports/2011/Teens-and-social-media.aspx.

Lievens, Eva (2010), *Protecting children in the digital era: the use of alternative regulatory instruments*, Martinus Nijhoff Publishers, Leiden.

Lievens, Eva (2011), "Risk-reducing regulatory strategies for protecting minors in social networks", *Info - The journal of policy, regulation and strategy for telecommunications, information and media*, Vol. 13, No. 6, 43-54.

Livingstone, Sonia, Haddon, Leslie, Görzig, Anke and Ólafsson, Kjartan (2011), EU Kids Online Final Report, http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/Final%20report.pdf.

Livingstone, Sonia, Ólafsson, Kjartan, O'Neill, Brian and Donoso, Verónica (2012), Towards a better internet for children, EU Kids Online, http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/EUKidsOnlinereportforthe CEOCoalition.pdf.

Lobe, Bojana and Staksrud, Elisabeth (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)", http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/sec_part.pdf.

Marwick, Alice and boyd, danah (2011), "The drama! Teen conflict, gossip and bullying in networked publics", A decade in Internet time: Symposium on the dynamics of the Internet and society, September, Oxford Internet Institute, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926349.

National Center for Missing & Exploited Children (2009), "Policy statement on sexting", http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=4130.

Olweus (2011), Bullying Prevention Program, Bullying, http://www.violencepreventionworks.org/public/bullying.page.

Phippen, Andy (2009), Sharing personal images and videos among young people, http://www.swgfl.org.uk/Staying-Safe/Sexting-Survey.

Ringrose, Jessica, Gill, Rosalind, Livingstone, Sonia and Harvey, Laura (2012), A qualitative study of children, young people and 'sexting' - A report prepared for the NSPCC, 2012, http://www.nspcc.org.uk/Inform/resourcesforprofessionals/sexualabuse/sexting-research-report_wdf89269.pdf.

Sacco, Dena T., Argudin, Rebecca, Maguire, James and Tallon, Kelly (2010), "Sexting: youth practices and legal implications", Cyberlaw Clinic, Harvard Law School, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Sacco_Argudin_Maguire_Tallon_Sexting_Jun2010.pdf.

Schmitz, Sandra and Siry, Lawrence (2011), "Teenage folly or child abuse? State responses to "sexting" by minors in the U.S. and Germany", Policy & Internet, Vol. 3, Iss. 2, Article 3.

Staksrud, Elisabeth and Lobe, Bojana (2010), "Evaluation of the implementation of the Safer Social Networking Principles for the EU, Part 1: General report (Study commissioned by the European Commission)", http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf.

Uyttendaele, Caroline (2002) *Openbare informatie – Het juridisch statuut in een convergerende mediaomgeving*, Antwerpen, Maklu, 400 p.

Van Alsenoy, Brendan, Ballet, Joris, Kuczerawy, Aleksandra and Dumortier, Jos (2009), "Social networks and web 2.0: are users also bound by data protection regulations?", *Identity in the information society*, Vol. 2, No. 1, 65-79.

van der Hof, Simone and Koops, Bert-Jaap (2011), "Adolescents and cybercrime: navigating between freedom and control", *Policy & Internet*, Vol. 3, Iss. 2, article 4.

Walrave, Michel, Demoulin, Marie, Heirman, Wannes and Van der Perre, Aurélie (2009), Onderzoeksrapport Cyberpesten, http://www.internet-observatory.be/internet_observatory/pdf/brochures/Boek_cyberpesten_nl.pdf.

Willard, Nancy (2007), Educator's guide to cyberbullying and cyberthreats, http://csriu.org/cyberbully/docs/cbcteducator.pdf.

Wolak, Janis and Finkelhor, David (2011), Sexting: A typology, *Crimes against Children Research Center,* http://www.unh.edu/ccrc/pdf/CV231_Sexting%20Typology%20Bulletin_4-6-11_revised.pdf.