Formulating adequate legislation to address cyber-bullying: Has the law kept pace with advancing technology?

F CASSIM*

ABSTRACT
The development of new accessible technologies and the expansion of the Internet have revolutionised communication across the world. Online users rely on the safety and security of the Internet and digital media in their daily lives. However, these new technologies have exposed them to a variety of new threats and risks, such as cyber-bullying. The study reveals that cyber-bullying or online bullying has become prevalent among adolescents, and it is considered to be more harmful than typical schoolyard bullying. Cyber-bullying has a significant impact on the lives of victims, their families and friends. It is submitted that acts of cyber-bullying endanger online digital safety and erode confidence in the network technologies that are used. It is recommended that appropriate mechanisms should be put in place to ensure the safety and security of online users and address the devastating impact of cyber-bullying. However, the introduction of any anti-bullying legislation should consider the competing interests of the online user and the victim in an equitable manner. A collaborative effort by all role-players is also necessary to address the rise in cyber-bullying.

1. Introduction
The advent of modern technology has revolutionised communication across the world and introduced new platforms for social interaction. The use of digital technology has simplified one’s modern lifestyle and improved methods of communication by granting immediate access to information. Trust is said to be an important facet for online users who rely on the safety and security of the Internet and digital media in their daily lives. However, the development of new accessible technologies and the expansion of the Internet have resulted in new criminal

* BA (Law) (University Durban-Westville) LLB (University of Natal – Durban) LLM LLD (University of South Africa), Associate Professor in the Department of Criminal and Procedural Law, University of South Africa (UNISA), admitted attorney and conveyancer of the High Court of South Africa.
behaviours such as cyber-bullying. The Internet was originally designed for adults and not for children. However, the increasing use of the Internet by children has raised issues of concern regarding digital safety and the welfare of young children for policymakers. Cyber-bullying involves the use of digital technology or technological devices such as the Internet, mobile phones or online games by a person or group of persons (including adolescents) to threaten, harass or humiliate another person. These digital devices are used to send or post text messages or images which are aimed at hurting or embarrassing another person. Thus, there has been migration of traditional bullying to the digital world where the anonymity and accessibility of digital technology makes it easier for bullies to harass their victims.

The aim of cyber-bullies is to victimise the other person and the impact is said to be different for everyone. Some victims may react positively by blocking communication with the bully, deleting messages without reading them or reporting the problem to friends.

---


2 This concern has been raised by the European Commission. See B O’Neill ‘Trust in the information society’ 28 (2012) 28 Comp. Law & Sec. Rev. 551-559 at 551.

3 See ‘Cyber bullying’ Childline, available at http://www.childline.org.uk/explore/bullying/pages/cyberbullying.aspx, accessed on 17 February 2013; T Anderson and B Sturm ‘Cyberbullying: From playground to computer’ (2007) Young Adult Lib. Serv. 24-27 at 24; I Moodley ‘Cyber bullying: A legal framework for South African educators’ (2012) 27 SAPL 540 and Nuth op cit (n1) 438. It should be stated at the outset that the term ‘adolescents’ also incorporates reference to ‘children’, ‘teenagers’ and ‘minors’. Therefore, unless otherwise indicated, these terms are ‘all inclusive’ and are used interchangeably. It is also noteworthy that a child is defined in the South African Constitution 1996 as it person under the age of 18 years. The age of 18 also conforms with the United Nations Convention of the Rights of the Child, 1989.

4 Anderson and Sturm op cit (n3) 2.

family or teachers, whilst other victims may suffer depression, anxiety, experience academic problems, resort to drugs and alcohol abuse or withdraw into themselves.\(^6\) Cyber-bullying is said to be prevalent amongst adolescents today. Tech-savvy teenagers are using technology all the time to interact with their friends and family. Most teenagers have high-speed Internet access which they use to \textit{inter alia} send instant messages to their friends and families, create blogs and online videos and communicate with their friends on social networking websites such as Facebook and Twitter.\(^7\) The prevalence of social media in the lives of teenagers has created an environment that can be easily accessed and exploited by sexual predators, criminals and cyber-bullies.\(^8\) Cyber-bullying has thus become a problematic issue as adolescents begin increasingly using modern technology and the Internet at a young age. The global reach of the social media also compounds the problem of seeking adequate redress for victims.\(^9\) This also enables offenders to continue with their activities unhindered and without any fear of retribution. However, attempts to legislate cyber-bullying may impact on the freedom of expression of individuals and the right to privacy of online users. The role of the media in exaggerating the harm of cyber-bullying has also been criticised by some academic writers.\(^10\)

The dearth of adequate legislation to address cyber-bullying has raised concerns for many policymakers. The article will examine the emergence of cyber-bullying in the United States of America, the United Kingdom and South Africa and the suitability of existing legislative frameworks to address cyber-bullying and provide adequate redress for victims of cyber-bullying.\(^11\) The article will also examine whether specific legislation or policies have been introduced to address cyber-bullying in such countries and their impact on core constitutional values such as the rights to freedom of speech, human dignity and

\(^6\) For a detailed discussion about the effects of cyber-bullying see, Manuel op cit (n5) 224-228.

\(^7\) These social networking sites are said to provide teenagers with shared spaces for interaction and communication with known and unknown groups of people. See D Agosto, A Forte and R Magee ‘Cyberbullying and teens: What YA librarians can do to help’ (2012) 10 \textit{Young Adult Lib. Serv.} 38-45 at 38.

\(^8\) Ibid. Also see Cannizzaro op cit (n1) 64. Also see S Kierkegaard ‘Cybering, online grooming and ageplay’ (2008) 24 \textit{Comp. Law & Sec. Rev.} 41-55 at 41.

\(^9\) It is problematic if the victim and the offender live in different locations or jurisdictions but meet via the Internet. Problems arise regarding enforcement and jurisdiction. See further, Manuel op cit (n5) 224.

\(^10\) It has been advocated that the focus of adolescent cyber-bullying should rather be on the responsibility of parents to educate their children. See Hayward op cit (n5) 90.

\(^11\) It should be noted that this discussion will focus more on cyber-bullying by adolescents or teenagers and the resultant impact on adolescent or teenage victims.
privacy. The study reveals that the increased use of social networking sites such as Facebook and Twitter has resulted in an increase in the number of cases of cyber-bullying.\textsuperscript{12} The inability of the police and the prosecution authorities to keep pace with advancing technology and the lacuna in current laws to address the spectre of cyber-bullying, have circumvented a call for the introduction of specialised legislation to provide adequate relief for victims of cyber-bullying. It is advocated that countries should consider the competing interests of online users and victims when enacting new laws or amending existing laws to address the rise in cyber-bullying. An equitable balance between competing interests has to be struck which recognises new technologies “as positive tools to be embraced rather than feared”.\textsuperscript{13}

2. Defining cyber-bullying

Traditional bullying involves repeated intimidation by a stronger person or powerful group of persons over a weaker person.\textsuperscript{14} This can involve physical, verbal or social aggression. Cyber-bullying on the other hand, involves the use of digital technology or electronic media to intentionally upset, anger or intimidate someone else.\textsuperscript{15} Cyber-bullying is regarded as a form of bullying or harassment by electronic means. It has been defined as being particularly aggressive, intentional and comprising repeated harmful acts through electronic means of contact with a particular individual.\textsuperscript{16} However, the fact that it happens online or on mobile phones means that it can happen frequently and daily with devastating consequences.\textsuperscript{17} Cyber-bullying can be distinguished from other types of bullying because of its online content, its anonymity, its accessibility, its ability to involve or reach more people and its ability to invade the privacy of one’s home.\textsuperscript{18}

\textsuperscript{12} It has been reported that these cyber-bullies are even targeting families of dead children, soccer stars and television contestants. See V Allen ‘Rise of the sick internet trolls’ \textit{Daily Mail} 8 June 2012, available at http://www.dailymail.co.uk/news/article, accessed on 5 March 2013.
\textsuperscript{13} O’Neill op cit (n2) 558.
\textsuperscript{14} This can encompass intimidation of a physical, verbal and psychological nature. See Hayward op cit (n5) 86-87.
\textsuperscript{15} See BBC ‘Understanding cyber bullying’, available at http://www.bbc.co.uk/schools/parents/cyber_bullying/, accessed on 17 February 2013. Also see Cannizzaro op cit (n1) 64.
\textsuperscript{16} The bullying may involve several youths victimising another youth. Also see Manuel op cit (n5) 220.
\textsuperscript{17} See ‘Cyber bullying’ op cit (n3). Also see Manuel op cit (n5) 222.
\textsuperscript{18} Also see BBC ‘Understanding cyber-bullying’ op cit (n15) . For a detailed discussion about cyber-bullying and face-to-face bullying, see Anderson and Sturm op cit (n3) 26.
Thus, electronic media provides an avenue for people to easily violate or infringe the rights of others.

3. **Types of cyber-bullying**

Cyber-bullying can take place by sending nasty or threatening e-mails or by posting intimidating messages on social networking sites. Therefore, it may include writing posts, comments, tweets, posting images or sending texts.\(^{19}\) There are thus several types of cyber-bullying and the choice of a particular medium depends on the available technology such as instant messaging services (AOL instant messaging or Yahoo), text messaging by cell phones, e-mail bullying, websites, message boards and blogs.\(^{20}\) These forms of social media present dangers to adolescents. According to Nancy Willard, there are eight categories of specific cyber-bullying behaviours, namely, ‘flaming’ which involves engaging in the use of angry and offensive language, ‘harassment’ which involves sending repeated offensive communications, ‘denigration’ which entails the posting of false information to defame a person or damage one’s relationships, ‘impersonation’ which involves pretending to be someone else online, ‘outing’ which entails revealing another person’s secrets online, ‘trickery’ which involves tricking someone into revealing private information online, ‘exclusion’ which means the deliberate exclusion of a person from an online group, and ‘cyber stalking’ which entails the use of online media to stalk or frighten someone.\(^{21}\)

Cyber-bullying may involve adults, adolescents or teenagers. A parent or adult may participate in the cyber-bullying with devastating

---

19 See N Willard ‘Educator’s guide to cyber bullying and cyberthreats’ *Centre for Safe and Responsible Use of the Internet* (April 2007) 4, available at [http://www.accem.org/pdf/cbcteachers.pdf](http://www.accem.org/pdf/cbcteachers.pdf), accessed on 18 March 2013. Also see Manuel op cit (n5) 221, for further examples of social media used by cyber-bullies to harass their victims. Also see Hayward op cit (n5) 88-89.

20 For more information on these different media, see Anderson and Sturm op cit (n3) 25.

21 All these categories involve the use of posting harmful material or engaging in harmful aggression via digital technologies. See Agosto et al op cit (n7) 39; N Willard op cit (n19) 1-2 and C Badenhorst ‘Legal responses to cyber bullying and sexting in South Africa’ (August 2011) *Centre for Justice and Crime Prevention* 1-20 at 2, regarding the various types of cyber-bullying which includes *inter alia*, harassment, outing and denigration.
consequences. This is known as ‘bullying by proxy’.22 In the United States, it has been reported that most teenagers have experienced cyber-bullying in their school years and half of these incidents were committed by their classmates.23 This type of cyber-bullying is an extension of bullying that takes place at schools. Threats and taunts posted online are easily accessible and this can be emotionally destructive. Cyber-bullying or online aggression has become quite widespread, and it represents an imminent threat to a teenager’s online security.24 Teenage victims can experience a variety of emotions when they are cyber-bullied. These emotions can range from experiencing feelings of anger, hurt, embarrassment and fear. These emotions can cause teenagers to seek revenge on the bully, to withdraw into themselves or even commit suicide.25 However, the lack of specific legislation to address the control of contents published or distributed through the Internet and digital technologies, has made it difficult for victims of cyber-bullying to obtain adequate redress. Many incidents also go unreported as many victims believe that if they report the abuse to the police, they will not be taken seriously.26

4. The impact of cyber-bullying on human rights: Balancing competing rights?

Cyber-bullying may well infringe some basic human rights. The South African Constitution of 1996 (hereinafter, ‘the Constitution’) imposes a duty on the state and all its organs not to perform any act that infringes the entrenched rights such the right to life, human dignity, and freedom and security of the person.27 Section 16 of the Constitution provides that everyone has the right to freedom of expression, which includes inter alia, freedom to receive or impart information and

22 The most notorious example of cyber-bullying by proxy involved the case of Megan Meier, a thirteen year old girl from Missouri who committed suicide in 2007. The creator of the fictional character ‘Josh’, who was the cause of Megan’s suicide, was found to be the mother of one of Megan’s friends, Lori Drew. Mrs Drew wanted to find out what Megan and other peers thought about her daughter. She used the services of an eighteen-year-old employee, Ashley Grills, to participate in the cruel hoax. See Cannizzaro op cit (n1) 65.

23 Manuel op cit (n5) 222.

24 Agosto et al op cit (n7) 39.

25 This may also lead to reduced academic performance and negative self-esteem. Ibid.

26 It is also difficult to report the frequency of cyber-bullying incidents. See V Allen ‘Victory over cyber-bullies: Legal first as High Court orders Facebook to reveal trolls who tormented mother for defending X factor star’, Mail Online 8 June 2012, available at http://www/dailymail.co.uk/news/article-215635/Nicola-Brookes-victim-internet-troll, accessed on 5 March 2013.

27 See Carmichele v Minister of Safety and Security 2001(10) BCLR 995 (CC) para 44.
freedom of artistic creativity. However, this right does not extend to incitement of imminent violence or advocacy of hatred based on race, ethnicity, gender, religion and any action that constitutes incitement to cause harm. This means that the right of the cyber-bully to exercise his artistic creativity on the Internet or social networking site will have to be weighed against the victim's rights to privacy and dignity. It is submitted that a person's dignity is also impaired when one is subjected to treatment which constitutes degrading or humiliating conduct such as the posting of abusive texts, messages or images on social networking sites. Cyber-bullying also has the potential to affect the physical, psychological and emotional integrity of the cyber victim. To illustrate this, incidents of cyber-bullying may cause the cyber victim to experience feelings of depression, low self-esteem, social anxiety and suicidal tendencies. It is noteworthy that the act of cyber-bullying may constitute a form of abuse that impacts on the emotional and psychological integrity of the cyber victim. The psychological impact of cyber-bullying is also regarded to be more traumatising than physical bullying because of the public and online nature of the bullying. Similarly, the ability of cyber-bullies to invade the privacy and sanctuary of one's home by electronic media infringes one's right to communication, access to information, and one's right to privacy. Thus the act of cyber-bullying has the potential to infringe various human rights such as the right to freedom of expression, right to dignity, right to bodily and psychological integrity and right to privacy. Therefore, an appropriate balance should be drawn between the right to freedom of expression and the rights to privacy, human dignity and bodily and psychological integrity. However, all rights in the Constitution are not absolute as they may be subject to the limitation clause in section 36. Measures taken to address the infringement of rights should be necessary and proportional to the extent of the infringement. To this end, legislation should be enacted to adequately protect the rights of online users and to promote tolerance and respect for diverse opinions in a fair manner.

28 See section 16(1)(a)-(d) of the Constitution.
29 See section 16(2)(a)-(c) of the Constitution. Messages which threaten other users with violence fall into the category of 'incitement to violence' and they constitute unprotected expression in terms of the Constitution. Also see Moodley op cit (n3) 544.
30 See section 14 of the Constitution which protects the right to privacy. This includes inter alia the right not to have the privacy of one's communications infringed. Also see section 10 of the Constitution which affords everyone the right to human dignity.
31 Agosto et al (n7) 39.
32 For further discussion on the impact of cyber-bullying on freedom of expression, human dignity and children's rights, see Moodley op cit (n3) 541-549.
33 See section 36(1) of the Constitution.
American courts have also faced the challenge of balancing the First Amendment right to free speech against the rights of students to safety and privacy at school. The *Tinker v Des Moines* case is regarded as the landmark case for courts to follow when a student's free speech is infringed.\(^3\) This case demonstrates that education authorities don't have *carte blanche* to violate students' constitutional rights to ensure maintenance of order and proper discipline in schools. Therefore, it is advocated that parents should endeavour to safeguard their children's privacy, their freedom of expression and their right to access these new communication and information technologies in a safe and responsible manner. The right to freedom of expression must be considered in the context of other core values such as human dignity, psychological integrity, privacy and equality. This will involve a difficult balancing act that considers all competing interests in a fair and equitable manner.

5. An overview of cyber-bullying legislation and policies – a comparative perspective

The following discussion will address cyber-bullying legislative frameworks and policies introduced in the United States of America, the United Kingdom and South Africa.

5.1 United States of America

The National Information Infrastructure Protection Act of 1996 (hereinafter, the NIIPA) protects individuals against various crimes involving 'protected computers'.\(^3\) The Electronic Communications Privacy Act of 1986 (hereinafter the ECPA) is also aimed at non-

---

\(^3\) The Supreme Court overturned the suspension of three students who wore black armbands in protest of the Vietnam war. The court found that the wearing of the armbands did not constitute substantial disruption of schooling operations. Also see Hayward op cit (n5) 102-117 for a detailed discussion about the constitutionality of cyber-bullying statutes. It is noteworthy that the First Amendment of the US Constitution ranks the freedom of expression as pre-eminent over all other rights. The South African Constitution does not grant the right to freedom of expression superior status over other human rights. See E de Waal, R Mestry and CJ Russo 'Religious and cultural dress at school: A comparative perspective' (2011) 14(6) PER 62/217-95/217 at 80, available at http://dx.doi.org/10.4314/pelj.v14i6.3, accessed on 5 March 2013.

\(^3\) See section 1030 of Title 18 of the NIIPA. This includes a computer involved in interstate commerce or communications or any computer attached to the Internet. Offences include the prohibition of access to information without authorisation or computer hacking. See section 1030(a) regarding the types of offences and definition of electronic storage. See S Brenner and B Koops 'Approaches to cybercrime jurisdiction' (2004) 4 J High Tech Law 1-46 at 25.
traditional crimes such as hacking and electronic storage. Federal offences include cyber fraud, identity theft, spamming, cyber stalking, making intentional false representations online, the use of password sniffers, the decimation and creation of worms as well as the writing of viruses and Trojan horses, website defacements and web-spoofing. However, there is no specific legislation addressing cyber-bullying.

The Children's Internet Protection Act ('CIPA') was passed in 2000 to address inter alia, online protection measures for children using school or library computers. Although some of these measures have been criticised, the United States Supreme Court has upheld the law requiring libraries to obstruct access to information on the Internet as being constitutional, as the need for libraries to prevent minors from accessing obscene materials is said to outweigh free speech rights of library patrons and website publishers. However, no federal or state law presently exists in the United States which provides adequate redress for adolescents who are victimised by cyber-bullying or suitable punishment for minors who engage in cyber-bullying. To illustrate this, in the Finkel v Dauber case, the courts could not find in favour of the plaintiff as the state of New York did not recognise cyber-bullying as a tort action. The court held that schools may only censor student-initiated expression when it leads to substantial disruption of the educational environment. This case demonstrated the lack of adequate legislation or case law to address cyber-bullying in New York. Thus, the authority of schools to regulate Internet-related speech or expression remains unclear as the Supreme Court has not pertinently decided on the matter.

However, many states are making valiant attempts to protect children who are interacting online. Although laws and policies addressing cyber-bullying behaviours vary from state to state, there has been a growing trend to introduce more stringent measures to

---

36 See section 2701(a) of the ECPA.
37 For further information, see S Snail and S Madziwa 'Hacking, cracking and other unlawful online activities' (2008) Without Prejudice 30-31.
38 However, it only took effect on 20 April 2001. See Title XV1 – Children’s Internet Protection Act.
39 Kierkegaard op cit (n8) 52-53.
40 Manuel op cit (n5) 220.
41 29 Misc.3d 325 (2010). In this case, an Internet user brought a defamation suit against adolescent members of a secret Facebook page, alleging negligent entrustment against their parents. The defendants had posted defamatory remarks about the plaintiff. However, the Supreme Court of Nassua County found that the postings did not constitute defamation and a computer could not be regarded as a 'dangerous instrument' to fulfill a negligent entrustment claim. It should be stated that the phrase 'torts' refers to defamation actions or personal actions.
42 Cannazzaro op cit (n1) 66.
counteract this scourge. As a result of the Megan Meier incident, the state of Missouri amended its harassment and stalking statutes to prohibit the use of electronic means to intentionally “frighten, intimidate, or cause emotional distress to another person.”\(^{43}\) To protect children from sexual misconduct, the state of Missouri has enacted legislation making it illegal for teachers and students to interact via social media.\(^{44}\) In New Jersey, the new ‘Anti-bullying bill of rights’ was introduced requiring all public schools in New Jersey to adopt detailed anti-bullying policies, to provide staff education and training, and to follow strict new requirements for reporting online and offline bullying incidents.\(^{45}\) However, the above legislations have been criticised as they are seen to address online aggression ‘after the fact’ rather than before it occurs.\(^{46}\) Recently, New York State took steps to address cyber-bullying by introducing legislation to protect students from online harassment.\(^{47}\) Similarly, the social media site Facebook has made attempts to introduce safety features to address bullying. To this end, young users can report troubling content to the site, to their parents and teachers.\(^{48}\)

As stated earlier, the federal government has not enacted specific cyber-bullying legislation. However, many states have taken steps to develop policies or programmes to control and prevent bullying including cyber-bullying. Forty-five states have introduced bullying statutes which permit schools to prohibit bullying if it occurs on school property or on school computers, whilst seventeen states have amended their bullying statutes to incorporate cyber-bullying.\(^{49}\) The states that have introduced cyber-bullying statutes are Oregon,
Formulating adequate legislation to address cyber-bullying: Has the law kept pace with advancing technology?

California, Pennsylvania and Washington. However, these statutes have been criticised for not offering proper guidance on school intervention regarding electronic communications and guidelines on the prohibition of off-campus cyber-bullying.\(^{50}\) According to John Hayward, many statutes were introduced as a result of hysteria over Megan Meier’s death and without affording proper consideration to the threat posed to freedom of speech.\(^{51}\) Therefore, he maintains that anti-cyber-bullying laws pose a serious threat to students’ right to free speech and expression at a critical time in their lives, because such laws are aimed at curbing student speech rather than conduct.\(^{52}\)

The issue also arises whether schools can extend their right to discipline students beyond the school grounds and into virtual space. Anti-cyber-bullying advocacy organisations have proposed that school policies be amended to allow the disciplining of off-campus behaviour that adversely affect the safety and behaviour of students while in school.\(^{53}\) However, courts have been reluctant to follow suit.\(^{54}\) Indeed, the _Tinker_ case or standard has been used by courts to determine whether the cyber-bullying activity causes substantial disruption of school operations to warrant regulation of freedom of speech.\(^{55}\) Therefore, no adequate legislation or case precedent exists in the United States to criminalise cyber-bullying. Therefore, a call has been made for the introduction of a federal statute to regulate and criminalise cyber-bullying and to provide adequate redress for victims of cyber-bullying.\(^{56}\) It is hoped that this legislation will dissuade future cyber-bullies from victimising their peers. However, Hayward maintains that

\(^{50}\) Manuel op cit (n5) 236.

\(^{51}\) Hayward op cit (n5) 87.

\(^{52}\) Id 110.

\(^{53}\) Cannizzarro op cit (n1) 66.

\(^{54}\) Manuel op cit (n5) 237.

\(^{55}\) Also see Manuel op cit (n5) 237-242 and Hayward op cit (n 5) 102-110 for a detailed discussion about such case law. Also see E de Waal, R Mestry and CJ Russo op cit (n34) 82, for a discussion of the _Tinker_ case.

\(^{56}\) It should be noted that attempts by Congressman Linda Sanchez to introduce the Megan Meier Cyber-Bullying Prevention Act on 2 April, 2009 did not succeed because it was found to be vague and it would lead to violations of the First Amendment. Similarly, a call by Nancy Willard, the Director of the Centre for Safe and Responsible Internet Use to introduce legislation adopting the _Tinker_ standard and affording schools the right to intercede and discipline cyber-bullies and their parents, has been criticised as most cases do not meet the _Tinker_ standard and schools do not want to be burdened with taking on the role of parents. See Manuel op cit (n5) 244-249 for a discussion about the proposed federal legislation. She proposes _inter alia_ adopting the reasonable person test, disciplining offenders through community service, counselling, imposing mandatory Internet classes for proper use of the Internet and imposing a prison sentence for not more than two years. It is submitted that the use of community service, counselling and Internet classes seems feasible. However, the suggested punishment may be severe for adolescent cyber-bullies.
anti-cyber-bullying statutes pose a threat to student free speech. He therefore proposes a model anti-cyber-bullying statute which strikes a balance between students' right to free speech and the maintenance of academic order and discipline. This model defines the bullying or cyber-bullying activity that is outlawed, addresses the reporting of such incidents, sets out the development and implementation of an anti-cyber-bullying and bullying policy by schools, contains notification of criminal charges, proposes procedures for counselling victims and aggressors, and a procedure for training concerned parties such as teachers, students, parents and school administrators to prevent and respond to bullying and cyber-bullying.57 This model is commendable as it proposes less restrictive measures for schools to follow in addressing cyber-bullying, addresses the concerns of victims and it respects students' right to freedom of expression. Therefore, the need arises for the introduction of anti-cyber-bullying legislation which protects the human rights of both the cyber victim and the cyber bully in a fair and equitable manner.

5.2 United Kingdom

As a result of the growing use of the Internet by criminals, the United Kingdom government introduced the National High Tech Crime Unit during April 2001 to counteract such threats.58 Concerns have also been raised in United Kingdom about the emergence of cyber-bullying in the workplace.59 It has also been reported that 22% of children and young people have become targets of cyber-bullying in the United Kingdom.60 There is currently no legislation regulating cyber-bullying in the United Kingdom. However, a teenager who posted a death threat on Facebook, has become the first person to be convicted of cyber-

57 Hayward op cit (n5) 99-101; 123.
bullying in the United Kingdom.61 The sentencing of Keeley Houghton for cyber-bullying has set an important precedent as cyber-bullying has become a worrying trend in the United Kingdom.62 However, valiant attempts are being made in the United Kingdom to address the spectre of cyber-bullying. Schools in the United Kingdom have begun teaching subjects such as online safety and cyber-bullying.63 An organisation called Childnet was commissioned by the Department for Children, Schools and Families to provide advice and guidance for schools on ways to prevent and respond to cyber-bullying.64 Childnet has worked in consultation with a number of sectors including children, young people, schools, industry, law enforcement, professional bodies, parent groups and child welfare organisations. This collaborative effort to tackle cyber-bullying is commendable and demonstrates how different sectors can work together to fight the scourge of cyber-bullying.

However, social networking sites such as Facebook can be held accountable. In a recent case, a victim of cyber-bullying, Nicola Brookes won a court order to compel Facebook to disclose the cyber bullies' names, and to provide e-mail addresses and the computer internet protocol (IP) addresses of those individuals responsible for bullying her on Facebook and on other online sites.65 Ms Brookes instituted her campaign to disclose the identities of the ‘internet trolls’ who were bullying her online after she was unsuccessful in enlisting the aid of

61 Keeley Houghton (18) received a three-month prison sentence for bullying on a social networking site. Ms Houghton had threatened to kill Emily Moore who she had bullied for four years since they were in school together. See L Salkeld ‘Facebook bully jailed: Death threat girl 18, is the first person put behind bars for vicious internet campaign’, (2009) Mail Online, 21 August 2009, available on http://www.dailymail.co.uk/news/article-1208147/First-cyberbully-jailed-Facebook-death-threats.html, accessed on 5 March 2013.
62 Another teenager, Megan Gillan also committed suicide after bullies targeted her on a social networking site. See L Salkeld op cit (n61).
64 ‘Cyber bullying’ op cit (n3) 1.
65 This is the first of its kind in the United Kingdom. It is submitted that an IP address can be used to determine a computer’s location. See V Allen ‘Victory over cyber bullies: Legal first as High Court orders Facebook to reveal trolls who tormented mother for defending X factor star’, Mail Online, 8 June 2012, available at http://www.dailymail.co.uk/news/article-215635/Nicola-Brookes-victim-internet-trol, accessed on 5 March 2013; A Boxall ‘Facebook compelled to hand over IP addresses in UK cyber-bullying case’, Digital Trends, 8 June 2012, available at http://www.digitaltrends.com/international/facebook-compelled-to-band-over-ip-addr..., accessed on 5 March 2013.
the police to track down the perpetrators.66 This case demonstrates that social networking sites are ‘no places for harassment’ and that the anonymity of cyber bullies can be stripped away leaving them vulnerable to prosecution.67 This case has also raised issues regarding the privacy rights of online users. According to campaigners against acts of cyber-bullying, online bullying has become the ‘weapon of choice’ among children and teenagers with the police and prosecution authorities failing to keep abreast with the digital age.68 As a result of the rise in cyber-bullying in the United Kingdom, calls have been made for the introduction of new cyber-bullying laws. To this end, the government is considering introducing stalking as a criminal offence which is a step in the right direction.69 However, the introduction of any new legislation should endeavour to provide adequate protection for the competing interests of online users and victims of cyber-bullying in a fair and equitable manner.

5.3 The position in South Africa

There has been an increase in the cyber-bullying of young people in South Africa.70 The current South African school legislation protects

---

66 Her troubles began in November 2011 when she posted a message of support for a contestant who was receiving unpleasant messages on a local talent show’s Facebook page. However, this resulted in the trolls bullying her online and they published her home address, targeted her daughter online and created a fake Facebook profile suggesting that she was a paedophile. Mrs Brookes first tried to enlist the help of the local police in tracking down her cyber-bullies but the police’s inaction and apathy led her to engage the services of lawyers to bring the cyber-bullies to justice. She succeeded in being granted a High Court order compelling Facebook to provide the IP addresses of the individuals responsible for the abuse and the fake profile. Mrs Brookes also intends pursuing private prosecutions against the cyber-bullies or trolls. Ibid.

67 However, the trolls have not stopped taunting Ms Brookes as they have now created a fake law firm on the Facebook page offering support to victims of online bullying. Ibid.

68 Ibid.


children from traditional bullying but not cyber-bullying.\textsuperscript{71} This presents a problem as South African adolescents are increasingly using digital devices and media to communicate with their friends and family, and they may well use such technologies to bully other children. It is noteworthy that the Children’s Act defines ‘abuse’ as “any form of harm or ill-treatment deliberately inflicted on a child” and includes \textit{inter alia}, “bullying by another child” and “exposing or subjecting a child to behaviour that may harm the child psychologically or emotionally”.\textsuperscript{72} The rights of children to be protected from \textit{inter alia}, abuse or degradation is enshrined in section 28 of the Constitution. This section also stresses that the ‘best interests’ of the child is paramount in all matters affecting the child.\textsuperscript{73} This demonstrates that children’s rights are given ‘primary consideration’ in the Constitution. It is noteworthy that the United Nations Convention on the Rights of the Child, 1989 (UNCRC) was ratified by South Africa in 1995. The Convention strives to ensure that states take appropriate measures to protect children according to internationally accepted standards.\textsuperscript{74} Article 19 was revised during 2011 to include psychological bullying by adults and other children and to include acts committed via digital media and the Internet.\textsuperscript{75}

The South African Schools Act currently regulates the conduct of learners.\textsuperscript{76} The Guidelines for a Code of Conduct for Learners was introduced by the Department of Education in 1998 to inculcate a culture of tolerance and positive discipline in schools.\textsuperscript{77} The education authorities are expected to ensure that school practices do not impede access to education or infringe the constitutional rights of learners.\textsuperscript{78} Acts of cyber-bullying may well constitute degrading or abusive treatment meted out to a child. Acts of cyber-bullying may also constitute a violation of children’s rights in terms of section 28 of the Constitution and the Children’s Act.\textsuperscript{79} However, school governing bodies should be encouraged to adopt anti-cyber-bullying policies that

\textsuperscript{71} Moodley op cit (n3) 539.

\textsuperscript{72} See the Children’s Act 38 of 2005.

\textsuperscript{73} See s 28(2) of the Constitution.


\textsuperscript{75} This demonstrates that the UNCRC recognises the seriousness of cyber-bullying. See Badenhorst op cit (n21) 4.

\textsuperscript{76} South African Schools Act 84 of 1996.

\textsuperscript{77} See Notice 776 of 1998. Also see Moodley op cit (n3) 551 regarding a discussion of such document.

\textsuperscript{78} de Waal, Mestry and Russo op cit (n34) 63.

\textsuperscript{79} This author agrees with Moodley’s comments. See Moodley op cit (n3) 541.
consider the rights of all learners (irrespective of whether they are the aggressor or the victim) in a fair and equitable manner in line with core constitutional values.

There is no specific legislation addressing cyber-bullying in South Africa. However, the following laws in South Africa may provide victims of cyber-bullying with remedies. Cyber-bullying can be addressed by remedies found in criminal law or civil law.\(^80\) The criminal offences of *crimen injuria*, assault, criminal defamation and extortion can be used to apply to acts of cyber-bullying.\(^81\) Snyman defines *crimen injuria* as the unlawful, intentional and serious violation of the dignity or privacy of another person.\(^82\) This definition encapsulates the act of cyber-bullying. The crime of assault comprises the unlawful and intentional act or omission which results in another person's bodily integrity being impaired directly or indirectly.\(^83\) Any act of cyber-bullying which involves the threat of personal violence may fall under the ambit of assault.\(^84\) Criminal defamation involves the unlawful and intentional publication of a matter concerning another person which results in injury to that person's reputation.\(^85\) Defamatory remarks made on social media platforms may fall within the ambit of this offence. Extortion refers to the instance when a person unlawfully and intentionally obtains some advantage over another person which is of a patrimonial or non-patrimonial nature, inducing the latter to hand over an advantage.\(^86\) Any act of cyber-bullying which involves a threat to post disturbing or compromising images on the Internet unless a monetary advantage is handed over, constitutes an act of extortion. The above discussion demonstrates that acts of cyber-bullying may fall under the ambit of these criminal offences. Civil remedies may include an application for an interdict and a defamation claim.\(^87\) However, civil remedies may prove to be costly. It is noteworthy that there is no specific legislation addressing the regulation of online content or social media law in South Africa. However, it has recently been held that Facebook users may be sued for damages as a result of defamatory

\(^80\) The question arises whether these remedies provide sufficient or adequate redress for victims. Also see South African Law Reform Commission Discussion Paper 108 (Project 130) ‘Stalking’ (2004) at 66.

\(^81\) For a more detailed discussion of these offences, see Badenhorst op cit (n 21) 8.


\(^83\) This action should also ‘inspire a belief or fear of impending impairment of a person’s bodily integrity’. Id 455.

\(^84\) Badenhorst op cit (n21) 8.

\(^85\) Snyman op cit (n82) 475.

\(^86\) Id 426.

\(^87\) An interdict is a court order where a person is ordered to perform a specific act or not to perform a specific act. See *inter alia*, section 30 of the Magistrate’s Courts Act 32 of 1944 and Rule 6 of the Uniform Rules of Court.
The remarks made on Facebook.88 The judgment also stressed the need for the law to develop to keep abreast with technological innovations.89

The Protection from Harassment Act 17 of 2011 came into effect on the 27th April 2013.90 The definition of harassment in the Act is considered to be wide enough to encompass cyber-bullying.91 To illustrate this, the Act refers to the use of ‘electronic communications’ and the sending of messages by ‘electronic mail’ in the definition of harassment. The enactment of this legislation is a step in the right direction because it provides a viable option for vulnerable persons to rely on in the face of harassment by electronic means. However, the legislation has been criticised because protection for victims of cyber-bullying is dependent on the victims knowing the identity and location of the perpetrators.92 It is submitted that this requirement is burdensome as the anonymity and accessibility of the Internet makes it difficult for victims and enforcement agencies to track down offenders.

The Electronic Communications and Transactions Act 25 of 2002 (‘ECT’) was introduced to address inter alia, the facilitation and regulation of electronic communications and to prevent abuse of information systems. The focus of the ECT is said to protect “data” or data messages. The ECT deals comprehensively with cybercrime in Chapter 13. Cyber-bullying may involve the potential abuse of electronic communications or information systems to degrade, humiliate or bully another person. Similarly, a person may ‘hack’ into a person’s computer to intimidate, harass or threaten him or her. Therefore, it can be argued that the act of cyber-bullying may conceivably fall under the scope of cyber crime, and it can therefore be addressed by Chapter 13 of the ECT. Although the ECT does not specifically address cyber-bullying, it is submitted that the ambit of sections 86-88 can

88 See H v W (12/10142) [2013] ZAGPJHC1; 2013 (2) SA 530 (GSJ); 2013 (5) BCLR 554 (GSJ); [2013] 2 All SA 218 (GSJ), 30 January 2013. The offender was ordered to remove all postings relating to the victim or applicant on all social media sites and to pay the costs of the application. Also see K Ajam ‘Man wins interdict for slander on Facebook’ Saturday Star, 2 February 2013 1; 5.

89 See H v W supra (n88) at para 31; also see E Sadler ‘No need to go to court over offensive Facebook posts’ (2013) Saturday Star, 2 February 2013 5.


92 C Badenhorst op cit (n21) 15.
be widened to address the act of cyber-bullying. Therefore, a need arises for current South African law to develop to keep up with new criminal behaviours such as cyber-bullying. However, such legislation should consider the competing interests of online users and victims of cyber-bullying in a fair manner.

6. Conclusion

The rise in Internet use and the advent of new social media has opened up new channels of communication. However, it has also brought new challenges and introduced new criminal behaviours such as cyber-bullying. The above discussion has demonstrated that existing laws have not kept pace with modern technological advancements. Therefore a need arises to address the emergence of cyber-bullying.

Cyber-bullying has become rife in the school environment. Parents and teachers can collectively help adolescents who are being cyber-bullied by teaching them about cyber safety and methods to prevent bullying. Regular consultations should also be held involving students, teachers, school administrators, parents and community members to raise awareness about the prevalence of cyber-bullying and the risks posed by the Internet, and to introduce measures to address cyber-bullying. Parents should also learn more about the online tools used by their children as well as parental tools to control access. Indeed educating children about online safety and privacy is the key to reducing cyber-bullying. Children should be taught to become more responsible users of the Internet which entails smarter and safer users of social media platforms and to respect other online users. On the other hand, children may also target their teachers at schools. Teachers can also become victims of Internet messaging which may

93 Section 86 prevents unauthorised access to or interception of or interference with data; section 87 refers to computer-related extortion, fraud and forgery whilst section 88 refers to attempt and aiding and abetting. See DP Van der Merwe 'Computer crime – recent national and international developments' (2003) THRHR 30 at 43-44 and DP Van der Merwe 'Information technology crime – a new paradigm is needed' (2007) THRHR 309 at 313 for further discussion about these provisions.

94 Some of these methods should include: not responding to cyber-bullies, deleting messages without reading them, reporting bullying incidents to appropriate channels and Internet service providers (ISPs) and website administrators, exercising care and not disclosing too much personal information online, keeping a paper trail or record of abusive texts sent, and educators should introduce intervention programmes to help identify and help teenagers with social, emotional and academic problems. Also see Agosto et al op cit (n 7) 40. Also see Moodley op cit (n3) 558; Badenhorst op cit (n21) 16-17; See Poullet op cit (n 1) 13.

95 'Understanding cyber bullying' op cit (n15) 2. Also see Hayward op cit (n5) 89 and O’Neill op cit (n 2) 557.
ridicule or threaten them.\textsuperscript{96} To illustrate this, in a recent case in South Africa, school children manipulated the photographs of a principal and a deputy principal. They published a computer-generated image in which the face of a deputy principal was super-imposed alongside that of a school principal on an image of two naked men sitting in a sexually suggestive posture.\textsuperscript{97} The Constitutional Court found that the common law should be developed to include the value of an apology and stressed that matters should be discouraged from coming to court without an attempt being made to resolve the matter through restorative justice means. This decision stressed the need to explore restorative or reconciliatory proceedings in matters involving children. This case also demonstrates that children should also be taught by their parents and educators that the practice of insulting teachers online is unacceptable. Caution should also be exercised in granting schools the right to discipline students for off-campus behaviour if it impacts on the safety and well-being of students while in school. After all, “the mere fact that the Internet may be accessed at school does not authorise school officials to become censors of the world-wide web.”\textsuperscript{98} Internet Service Providers (‘ISP’) should also improve their methods of handling misuse of their services.\textsuperscript{99} Police and other law enforcement agencies should also receive appropriate training and resources to investigate and prosecute the unlawful use of online services.\textsuperscript{100} At the end of the day, a concerted and collaborative effort by all role players is important to help children cope with this form of abuse.

The question also arises whether victims of cyber-bullying can bring any action against the schools, Internet Service Providers or institute a private action against the bully. It may be problematic for schools as they need to consider \textit{inter alia}, the student’s right to free speech versus the victim’s right to protection against victimisation, the issue of whether the cyber-bullying takes place on the school property, the

\textsuperscript{96} Id 3.

\textsuperscript{97} See \textit{Le Roux and Others v Dey} (CCT 45/10) [2011] ZACC 4; 2011 (3) SA 274 (CC); 2011 (6) BCLR 577 (CC); BCLR 446 (CC). The principal accepted the apology of the accused but the deputy principal sued for defamation. The deputy principal was awarded damages in the amount of R45 000 by the North Gauteng High Court, Pretoria because it was found that the publication defamed him. The Supreme Court of Appeal affirmed the decision of the North Gauteng High Court, Pretoria and confirmed the award of damages. The matter was then taken on appeal to the Constitutional Court to determine the liability of children for defamation or for injured feelings in terms of the Constitution. The Court upheld the appeal and reduced the award of damages to R25 000.

\textsuperscript{98} Hayward op cit (n5) 85 quoting \textit{Layshock v Hermitage Schools District} 496 F Supp. 2d 587 at 597 (2007).

\textsuperscript{99} Anderson and Sturm op cit (n3) 26. Also see O’Neill op cit (n2) 554 regarding the role of industries in safeguarding the users who use their services.

\textsuperscript{100} Poullet op cit (n 1) 12.
extent to which schools can regulate or prevent cyber-bullying on its property or whether there is any applicable law that may hold them liable for failure to act. In the United States, the Communications Decency Act, 1996 ('CDA') has been interpreted by the courts to absolve ISPs from liability. The CDA is aimed at publishers rather than conduits and the ISPs are regarded as conduits because they cannot be held liable for Internet activity. It has been mooted that the victim’s best chance of redress is to institute a private action against the cyber-bully via stalking laws, defamation laws or state statutes. However, these remedies have been criticised as they do not provide adequate relief for victims of cyber-bullying. Instead, the introduction of specific legislation criminalising cyber-bullying has been punted as the way forward.

Thus, a need arises for adequate legislation to address the spectre of cyber-bullying. Such legislation should consider the competing interests of online users and cyber victims in a fair, equitable and balanced manner. Cyber-bullying results in physical and emotional harm and its effects can be devastating. Indeed, introducing legislation that would make cyber-bullying a criminal act will provide remedies for victims of cyber-bullying and also send a strong message to potential cyber bullies to take note that their behaviour will not go unpunished irrespective of whether they are adults or minors. At the same time, such legislation should also consider the rights of online users to express their free speech and diverse opinions. Therefore, an appropriate balance should be struck between these competing rights. Outdated laws should also be replaced by new equitable laws to keep abreast with technological innovations. It is submitted that the advent of the Protection from Harassment Act, 2011 in South Africa is a step in the right direction. However, the scope of the ECT can also be widened to address cyber-bullying. At the end of the day, countries should strive to create a more trusted, fair and safe Internet environment which all online users can embrace with confidence.

101 See Manuel op cit (n 5) 229-231.
102 Id 231.
103 Id 232.
104 However, it is submitted that such legislation should not impose stringent penalties on adolescent cyber-bullies. Ibid.