

Authors: M Laubscher and WJ van Vollenhoven

**CYBERBULLYING: SHOULD SCHOOLS CHOOSE BETWEEN
SAFETY AND PRIVACY?**

eISSN 1727-3781



2015 VOLUME 18 No 6

<http://dx.doi.org/10.4314/pej.v18i6.06>

CYBERBULLYING: SHOULD SCHOOLS CHOOSE BETWEEN SAFETY AND PRIVACY?

M Laubscher*

WJ van Vollenhoven**

1 Introduction

Apparently, the term "cyberbullying" was coined by the Canadian Bill Belys when he attempted to describe the use of information and communication technologies to support deliberate, repeated and hostile behaviour by an individual or group to harm others.¹ In an article titled "Following you home from school: A critical review and synthesis of research on cyberbullying", Tokunaga² refers to Olweus who contends that cyberbullying is any behaviour performed through electronic or digital media by individuals or groups that communicate hostile or aggressive messages intended to inflict harm or discomfort on others. In their article written for a 2014 edition of the *Cardozo Law Review*, the likes of Calvoz, Davis and Gooden³ were happy to simply equate this phenomenon to "bullying via electronic means".

However, given that a study recently conducted by the Centre for Justice and Crime Protection⁴ found that a third of South African learners experienced cyberbullying at school, the issue of cyberbullying in South African schools is a serious one, especially in schools where young children are victimised.

According to a study published by an organisation going under the name of *Ditch the Label*, cyberbullying is often linked to "low self-esteem, family problems, academic problems, school violence, and delinquent behaviour [and] suicidal

* Michael Laubscher MA LLB. Lecturer, Faculty of Law, North-West University. E-mail: michael.laubscher@nwu.ac.za.

** Willie(J) van Vollenhoven B Ed M Ed PhD. Associate Professor: Academic Manager for the Faculty of Education Sciences: Unit for Open Distance Learning, North-West University, Potchefstroom Campus. E-mail address: willie.vanvollenhoven@nwu.ac.za.

¹ Kift, Campbell and Butler 2010 *JLIS* 352-359.

² Olweus as quoted by Tokunaga 2010 *Comput Hum Behav* 277-287.

³ Calvoz, Davis and Gooden 2014 *Cardozo L Rev* 104-112.

⁴ Rondganger 2012 <http://www.iol.co.za/dailynews/opinion/cyberbullying-a-cause-for-concern-1.1261733#.VTSdBJP06Kg>.

thoughts".⁵ Likewise, studies conducted amongst youngsters who have contemplated suicide revealed that victims of cyberbullying were almost twice as likely to attempt suicide as those who had not been exposed to this phenomenon⁶ – which makes all the more shocking the finding that only 2% percent of the participating learners could report a positive intervention by way of their school governing bodies on reporting alleged cyberbullying.⁷

What makes cyberbullying even more menacing and potentially lethal than bullying the way it was originally known (that is, physical and mental bullying) is that children and technology are in a sense synonymous. According to Tokunaga,⁸ more than 97% of youths in the United States are connected to the internet, implying that children have a myriad of opportunities readily on hand to bully one another on social media and can do this even with a false identity or under the expectancy of privacy in terms of identity. Clearly, the rapid increase in the popularity of social media implies that opportunities for this type of bullying have the potential to multiply overnight.

What is of importance here, though, is to keep the very nature of cyberbullying in mind. Based on his study, Tokunaga⁹ found that when it comes to cyberbullying, the person(s) being bullied often do not know the identity of the bully, or bullies, and that the bullying can occur either at school or outside of school. Slonje and Smith¹⁰ found that cyberbullying offers bullies anonymity and the opportunity to hound their victims relentlessly without the need to be physically present in order to do the deed. The plot thickens when bullies use fake internet identities, or even take on other people's identities, which means victims often have no idea who the bullies are or why they are being bullied.¹¹ To quote Bonnono and Shelley, "cyberbullying is

⁵ Taran 2011 http://www.huffingtonpost.com/randy-taran/cyberbullying-10-ways-to-_b_807005.html.

⁶ Hinduja and Patchin Date Unknown http://www.cyberbullying.us/cyberbullying_and_suicide_research_fact_sheet.pdf.

⁷ Hinduja and Patchin Date Unknown http://www.cyberbullying.us/cyberbullying_and_suicide_research_fact_sheet.pdf.

⁸ See Tokunaga 2010 *Comput Hum Behav* 277-287.

⁹ Tokunaga 2010 *Comput Hum Behav* 277-287.

¹⁰ See Slonje and Smith 2008 *Scand J Psychol* 147-154.

¹¹ See Hinduja and Patchin Date Unknown http://www.cyberbullying.us/cyberbullying_and_suicide_research_fact_sheet.pdf.

pervasive and persistent" and once instigated, "very difficult to eradicate or eliminate",¹² which might account for Hinduja and Patchin's finding that a bullied person seemingly experiences or is under the impression that the entire school, neighbourhood and/or community is participating in the bullying.¹³ Cyberbullying offers a very wide, and potentially huge, audience,¹⁴ and due to its electronic medium knows no geographical boundaries.¹⁵ Everything can be accomplished in a matter of seconds with just a few keystrokes, reaching far and wide beyond physical borders and limitations.¹⁶

Furthermore, the effect of cyberbullying can be lasting. Due to the nature of electronic media, cyberbullying can be, and often is, permanent and follows the victim. Locally, a survey by Tustin, Zulu and Basson¹⁷ clearly revealed that the consequences of cyberbullying have a lasting emotional effect on secondary school learners. Rojas' article in the *Los Angeles Times* concurs: "The Web never stops and it never forgets".¹⁸ In this regard, victims of cyberbullying revealed feelings of sadness, depression and degradation. Their rights to human dignity and to be a child had therefore been violated. Using technology as a vehicle in the act of bullying means that perpetrators have no visible feedback as to the consequences of their actions. Traditionally, one of the most effective ways to end bullying behaviour is to get the bullies to feel empathy for their victims. In an online situation, though, even when youngsters know that their actions are hurtful, they can easily convince themselves that they have not hurt anyone. As one elementary school student in Toronto put it: "I don't think a lot of people would have enough confidence to walk up to someone and be like, 'I hate you, you're ugly.' But over the Internet ... you don't have to look in their eyes and see they're hurt."¹⁹

¹² Bonnono and Shelley 2013 *J Youth Adolesc* 685-697.

¹³ Hinduja and Patchin Date Unknown
http://cyberbullying.us/Cyberbullying_Identification_Prevention_Response.pdf.

¹⁴ Slonje and Smith 2008 *Scand J Psychol* 147-154.

¹⁵ See Hinduja and Patchin Date Unknown
http://www.cyberbullying.us/cyberbullying_and_suicide_research_fact_sheet.pdf.

¹⁶ Hinduja and Patchin Date Unknown
http://www.cyberbullying.us/cyberbullying_and_suicide_research_fact_sheet.pdf.

¹⁷ Tustin, Zulu and Basson 2014 *CARSA* 13-25.

¹⁸ Rojas 2011 <http://articles.latimes.com/2011/mar/27/local/la-me-college-speech-20110327>.

¹⁹ Leishman 2005 <http://www.njbullying.org/CBCNewsInDepthBullying.htm>.

The extent and effect of this never-ending and faceless haunting clearly came to the fore in the Canadian case of Amanda Todd. This case has been one of the most prolific instances of cyberbullying and has led Canadian authorities to seriously consider amendments to and the expansion of legislation in an attempt to combat cyberbullying more effectively.²⁰

Amanda, a British Columbia teenager, posted a YouTube video that had more than 17 million views.²¹ In the video titled "My story: Struggling, bullying, suicide, self-harm", she uses flash cards to highlight her plight.²² The video recounts her cyberbullying ordeal which stemmed from someone (online) who had convinced Amanda to bare her breasts on camera and then used that picture to blackmail her. The picture circulated on the web, and despite Amanda's efforts to put an end to this, she was mercilessly haunted and bullied by her stalker. Soon after posting the video referred to above, Amanda committed suicide.²³ This sad tale is just one of various examples of the devastating effects of cyberbullying.

Cyberbullying cannot be ignored. It is real, it can be lethal, and it needs to be addressed by schools, since at their tender age children's psyches can be permanently damaged, the damage in some instances being so severe that it might even cause them to take their own lives. The question of how schools ought to go about dealing with this scourge raises many issues, though.

To begin with, which test or principles should be applied to combat and discipline cyberbullying, given the framework and spirit of South Africa's *Constitution*? The matter becomes even more complicated when one considers that cyberbullying often occurs and originates away from or outside the school grounds; for instance, at a private party attended by school children. Can school principals and school governing bodies discipline learners for activities that occur away from or outside the school? One can argue that the safety of learners is the responsibility of the school

²⁰ Meissner 2013 <http://www.ctvnews.ca/canada/amanda-todd-s-legacy-a-look-at-canada-s-anti-bullying-efforts-a-year-after-her-death-1.1490889>.

²¹ Nguyen and Tepper 2014 http://www.thestar.com/news/gta/2014/04/17/amanda_todd_man_arrested_in_netherlands_in_connection_with_canadians_online_bullying.html.

²² Dean 2012 <http://www.newyorker.com/culture/culture-desk/the-story-of-amanda-todd>.

²³ Dean 2012 <http://www.newyorker.com/culture/culture-desk/the-story-of-amanda-todd>.

while they are at school or on an official school excursion. It becomes more difficult to guarantee the safety of the learners, however, if they attend a private party. One can continue to argue the authority and responsibility of the school ends at a point. Can a school be held accountable if, for instance they would have heard that drugs would be available at a private party attended by learners and did nothing to intervene? The need to balance an array of fundamental human rights in the process only adds to the complexity of the conundrum. Besides the obvious issue of freedom of expression, which has been well-documented,²⁴ the right to privacy cannot be ignored in this matter.

Clearly, as found by Cassim,²⁵ cyberbullying is on the increase amongst young people in South Africa. In an attempt to add to the discourse on the questions raised above, this article will first attend to the obvious issues around the right to freedom of expression before turning to the rights of the child as a minor as reflected in section 28 of the *Constitution*.²⁶ The argument then would continue to focus on a far more contentious issue: the right to privacy of the cyber user when cyberbullying is at stake. We will therefore begin by discussing the first issue.

2 Freedom of expression and cyberbullying

In terms of section 16(1)(a-d) of the *South African Constitution* of 1996 (the *Constitution*), everyone has the right to freedom of expression, which includes, *inter alia*, freedom to receive or impart information and freedom of artistic creativity. However, this right is inherently limited by section 16(2)(a-c), which claims that freedom of expression does not extend to incitement of imminent violence or the advocacy of hatred based on race, ethnicity, gender, religion or any action that constitutes incitement to cause harm. This implies that the right of the cyber bully to exercise his artistic creativity on the Internet or social networking site as well as his expectations of privacy (section 14 of the *Constitution*) will have to be weighed

²⁴ Mawdsley, Smit and Wolhuter 2013 *De Jure* 9.

²⁵ Cassim 2013 *SACJ* 1-20.

²⁶ Section 28 of the *Constitution of the Republic of South Africa, 1996* (the *Constitution*).

against the victim's rights to life (section 11 of the *Constitution*) and dignity (section 10 of the *Constitution*).²⁷

To date, South African courts have been called on to apply constitutional standards *inter alia* to rule on the limits of freedom of expression in the education or school context concerning physical symbols,²⁸ ²⁹ personal expression,³⁰ the publication of untrue statements in the media,³¹ student protests³² and student-generated electronic cyber expressions created outside the school setting but having an effect on school discipline.³³

From these court cases it is clear that the issue of freedom of expression with regard to cyberbullying is well documented.³⁴ ³⁵ ³⁶ ³⁷ ³⁸ ³⁹ Here it ought to be noted, though, that social media heralded the introduction of a much wider platform with infinite opportunities to speak one's mind. This phenomenon has substantially affected schools and their learners. In fact, schools seem to be at the very heart of the matter, since teenagers are the ones who are, technologically speaking, extremely adept and involved in the electronic media, often more so than their elders.

American educational institutions have had to deal with the issue of freedom of expression for decades, with the case of *Tinker*, brought against the Des Moines Independent Community School District in 1969, undoubtedly serving as a landmark.⁴⁰ In this case, students were planning on wearing black armbands to school to protest America's involvement in the Vietnam War. School officials learnt of the intended protest action and promptly banned the wearing of armbands at

²⁷ Sections 10, 11 and 14 of the *Constitution*.

²⁸ *Antonie v Governing Body, Settlers High School* 2002 4 SA 738 (C).

²⁹ *Pillay v KwaZulu-Natal MEC of Education and Cronje* 2006 JOL 17833 (N).

³⁰ *Western Cape Residents' Association obo Williams v Parow High School* 2006 3 SA 542 (C).

³¹ *Hamata v Chairperson, Peninsula Technikon Internal Disciplinary Committee* 2000 4 SA 621 (C).

³² *Acting Superintendent-General of Education of KwaZulu-Natal v Ngubo* 1996 3 BCLR 369 (N).

³³ *Le Roux v Dey* 2011 3 SA 274 (CC).

³⁴ Van Vollenhoven, Beckmann and Bignaut 2006 *Journal of Education* 119-140.

³⁵ Van Vollenhoven *Learners' Understanding*.

³⁶ Wood 2001 *SAJE* 142-146.

³⁷ Alston *Constitutional Right to Freedom of Expression*.

³⁸ Mawdsley, Smit and Wolhuter 2013 *De Jure* 132-161.

³⁹ Currie and De Waal *Bill of Rights Handbook*.

⁴⁰ *Tinker v Des Moines Independent Community School District* 1969 393 US 503, 89 (S Ct) 733.

school. The students disregarded this new rule and came to school wearing the armbands, which act resulted in their summary suspension.

In the court case that followed, the Supreme Court found that the conduct of the students amounted to speech and that this speech could not be regulated by the school without considering the constitutional rights and, specifically, the freedom of expression of individuals. As the court stated: "Neither learners nor teachers shed their constitutional rights to freedom of speech or expression at the school gate".⁴¹ From this finding, the "substantial disruption test" – or the Tinker test as it has become known – emanated.⁴²

Despite this finding, Brunsmas⁴³ holds that learners do not share the same measure of protection of freedom of expression at school as adults do outside the school grounds. Basically, according to Bray,⁴⁴ the right to freedom of expression can be limited in schools if such an expression leads to a material and substantive disruption of school operations, activities or the rights of others, a view which is supported by Alexander and Alexander.⁴⁵ Accordingly, the Tinker test basically states that school authorities may regulate learner speech if the regulation has the aim to prevent (1) a foreseeable material or substantial disruption to the school environment or (2) an invasion of the rights of others.⁴⁶

Based on these premises, school authorities in the Americas ought to be in a position to regulate speech, provided they are of the opinion that such speech will disrupt the school or infringe on the rights of others. They ought also to be able to do so without fear of violating the right to freedom of expression as contained in the First Amendment, an amendment which could be equated to section 16 of the *Constitution of South Africa*.⁴⁷ In short, the obvious deduction in so far as the right to freedom of expression is concerned ought to be that should cyberbullying, or

⁴¹ *Tinker v Des Moines Independent Community School District* 1969 393 US 503, 89 (S Ct) 733.

⁴² See Calvo, Davis and Gooden 2014 *Cardozo L Rev* 104-112.

⁴³ Brunsmas *School Uniform Movement*.

⁴⁴ Bray *Human Rights in Education*.

⁴⁵ Alexander and Alexander *American Public School Law*.

⁴⁶ See Calvo, Davis and Gooden 2014 *Cardozo L Rev* 104-112.

⁴⁷ See s 16 of the *Constitution*.

bullying for that matter, resort under any of these categories, it can be prohibited and punished without violating this right as such.⁴⁸

Nevertheless, in *Morse v Frederik*⁴⁹ the court held that the Tinker test was a mere starting point when regulating speech, and that schools often regulate speech if they are of the opinion that such speech could lead to the disruption of school or infringe on the rights of others. This finding, according to Starks,⁵⁰ led to various interpretations and applications of the substantial disruption standard, with American lower courts seemingly focusing on two crucial factors when applying Tinker. The first one asks if a school district can point to past incidents originating from similar speech that would lead to the establishment of a well-founded expectation of disruption. Secondly, if past instances cannot be cited, the question is asked if the school can demonstrate substantial facts that can reasonably support a specific and significant fear of disruption. Should the answer to any of the two foregoing questions be in the affirmative, the restriction of student (learner) expression can be regarded as constitutional.⁵¹

Starks⁵² is of the opinion that the standard applied in *United States v O'Brien*⁵³ offers a better standard for content-neutral regulations. This, he argues, is so because the standard used in O'Brien firstly differentiates between content-based and content-neutral regulations, which enables the appropriate level of scrutiny to be applied and, secondly, confers the proper level of deference on school officials.

In contrast with Starks, Clay⁵⁴ bemoans the dwindling effect and application of Tinker, citing the decision in *Fraser*⁵⁵ as an example of courts moving further and further away from the Tinker findings, and even abandoning these findings all together.

⁴⁸ See Calvoz, Davis and Gooden 2014 *Cardozo L Rev* 104-112.

⁴⁹ *Morse v Frederik* 2007 551 US 393, 127 (S Ct) 2618.

⁵⁰ Starks 2010 <http://www.yalelawjournal.org/forum/tinkers-tenure-in-the-school-setting-the-case-for-applying-obrien-to-content-neutral-regulations>.

⁵¹ Starks 2010 <http://www.yalelawjournal.org/forum/tinkers-tenure-in-the-school-setting-the-case-for-applying-obrien-to-content-neutral-regulations>.

⁵² Starks 2010 <http://www.yalelawjournal.org/forum/tinkers-tenure-in-the-school-setting-the-case-for-applying-obrien-to-content-neutral-regulations>.

⁵³ *United States v O'Brien* 1968 US 232, United States Supreme Court.

⁵⁴ Clay 2009 *Am U L Rev* 1167-1192.

⁵⁵ *Bethel School District No 403 v Fraser* 1986 478 US 675, 106 (S Ct) 3159.

In addition to implying that enforcing the Tinker test might infringe on parental rights, Clay⁵⁶ merely echoed the sentiments of many who are of the opinion that this test is not sufficient or applicable when dealing with cyberbullying, stating that Tinker was never designed for cases involving activities away from school, and that creating and/or posting on a website at home cannot be regarded as an in-school activity. To strengthen his argument, Clay points out that the Tinker case dealt with a mode of expression (clothing) targeted at a specific government policy, ie participation in the Vietnam War. It does not address the cyberspace issues where the dignity of specific individuals (teachers, principals or classmates) and the attempts to cause them harm or injury are at stake, as was the case in *Doninger*⁵⁷ and *Wiesniewski*⁵⁸ (discussed later).

Nevertheless, if the Tinker test does not hold the answer, where should we turn? In an attempt to answer this question, the matter of *Fraser*⁵⁹ will be dealt with next, seeing that this case applied the fundamental value standard as a guideline to deal with issues relating to the concept "right to freedom of expression".

Fraser, a student, delivered a potentially offensive speech during a school activity and was duly suspended. He sued the school, claiming that his First Amendment rights had been violated.⁶⁰ In this instance the court did not apply the Tinker test. Instead, it ruled in favour of the school, claiming that the school's regulation of Fraser's speech was acceptable based on the notion that schools have a duty and obligation to teach fundamental values which would, among others things, not favour "the use of terms of debate highly offensive or highly threatening to others".⁶¹ The court pointed out that:

Surely it is a highly appropriate function of public school education to prohibit the use of vulgar and offensive terms in public discourse. Indeed, the 'fundamental values necessary to the maintenance of a democratic political system' disfavor the use of terms of debate highly offensive or highly threatening to others. The inculcation of these values is truly the 'work of the schools.' The determination of

⁵⁶ *Bethel School District No 403 v Fraser* 1986 478 US 675, 106 (S Ct) 3159.

⁵⁷ *Doninger v Niehoff* 2008 527 F 3d 41, 233 Ed Law Rep.

⁵⁸ *Wiesniewski v Board of Education of the Weedsport Central School District* 2007 494 F 3d 34.

⁵⁹ See *Bethel School District No 403 v Fraser* 1986 478 US 675, 106 (S Ct) 3159.

⁶⁰ *Bethel School District No 403 v Fraser* 1986 478 US 675, 106 (S Ct) 3159.

⁶¹ *Bethel School District No 403 v Fraser* 1986 478 US 675, 106 (S Ct) 3159.

what manner of speech in the classroom or in school assembly is inappropriate properly rests with the school board.⁶²

In this instance, the court thus held that schools can regulate speech and that such regulation may include a prohibition on the terms of debate where these could be regarded as highly offensive or highly threatening to others. The reasons cited for this finding were based on the premises that schools should foster, nurture, cultivate and protect fundamental values that will maintain the democratic political system of American society, and although the school might not be under the obligation to instil, foster or nurture fundamental values amongst scholars, it was highly desirable.

Even though this flexible approach led to considerable debate and wide-ranging interpretations, the message is obvious: a balance needs to be created between the students' "right to advocate unpopular and controversial views" and the "school's interest in teaching students [learners] the boundaries of socially appropriate behaviour".⁶³ In this vein one can argue that the school has the responsibility to teach learners about the dangers of social media and how to avoid the violation of other users' human rights.

On the subject of boundaries, Lorillard⁶⁴ is of the opinion that the doctrine of fundamental values, as established in *Fraser*, is more appropriate than those set out in *Tinker*. As much as she agrees with *Tinker* that children's rights do not stop at the school gate, she is of the opinion that children's rights sometimes need to be modified because of the fact that a school environment is a special place with special characteristics.

School authorities act *in loco parentis* and have a captive audience. For this reason, these authorities ought to be placed in a position where they are able to decide whether expression that originates away from or outside the school ought to be restricted, should substantial disruption or a collision of rights be at stake. The issue becomes more complicated if one needs to balance the position of trust between the teacher and learners. Furthermore, a school environment is not a work or an 'adult'

⁶² *Bethel School District No 403 v Fraser* 1986 478 US 675, 106 (S Ct) 3159.

⁶³ See Calvoz, Davis and Gooden 2014 *Cardozo L Rev* 104-112.

⁶⁴ Lorillard 2011 *Miss LJ* 189-263.

environment. In fact, it is an environment in which children are educated, where they are protected and where fundamental values, such as the right to freedom of expression, the right to privacy and the right to safety are taught and entrenched, all in the best interest of the child, Lorillard contends.⁶⁵ In so doing, she echoes Fraser's notion of 'fundamental values necessary to the maintenance of a democratic political system'⁶⁶ and the duty contingent upon schools to promote these values.

The school has this duty in respect of each and every learner who attends the institution. Consequently, when disruption is at stake, this should be considered not only when large-scale disruption is likely to occur. What if a learner struggles academically and his or her academic progress is being disrupted because he or she is being bullied by another learner through cyberspace? Surely disruption is at stake here too? In instances such as these, the learner being bullied will be experiencing major disruptions, even though the rest of the school, seemingly oblivious to his or plight, carries on as usual. Therefore, should the school become aware of the situation, it definitely has an obligation to address this issue of disruption. It should intervene in the matter to ensure that the child's best interests are served, and this is surely what the court intended in Fraser when it referred to the fostering of democratic rights and values by schools.⁶⁷

For this reason, if an expression that originated with a learner outside the school, targeted at a fellow learner or even a teacher, is created with the intention to attract viewers, and is shown to have a causal relationship (a "nexus") with the school by being transferred intentionally to the school grounds by its creator, it should be seen as a product of an in-school activity and should be dealt with by the school authorities.⁶⁸

In cases such as *Doninger v Niehoff*,⁶⁹ the court considered and applied the principle of a nexus between speech that originated away from school and its in-school effect, before turning to Tinker. The Appeals Court agreed with the district court's ruling

⁶⁵ Lorillard 2011 *Miss LJ* 189-263.

⁶⁶ See *Bethel School District No 403 v Fraser* 1986 478 US 675, 106 (S Ct) 3159.

⁶⁷ *Bethel School District No 403 v Fraser* 1986 478 US 675, 106 (S Ct) 3159.

⁶⁸ See Lorillard 2011 *Miss LJ* 189-263.

⁶⁹ See *Doninger v Niehoff* 2008 527 F 3d 41, 233 Ed Law Rep.

that Doninger's posting, although designed away from school, was purposefully intended to reach the school, and a clear nexus had thus been established between her action (speech away from school) and the in-school effect this could potentially have. The court was of the opinion that Doninger's posting, due to its language and the fact that she tried to cause confusion in school with her posts, created a foreseeable risk of disruption to the work and discipline at the school and that the school had been justified in its punishment of Doninger.⁷⁰ Yet, according to Calvoz, Davis and Gooden,⁷¹ the majority of cases still apply the Tinker standard, irrespective of whether the speech originated in-school or away from school.

When balancing the right to freedom of expression on the one hand and rights such as the right to dignity and the right to an education, safety and security on the other, one thus has Tinker with its disruption test as the starting point and Fraser with its standard of fundamental values to consider. Added to this, if the expression originated outside the school – which happens in the majority of cyberbullying cases – one also needs to establish whether a nexus exists between the activities away from school and activities in-school.

When considering the issue of cyberbullying, the crux thus seems to be that the school authorities must determine if this expression can, or potentially will, cause a disruption of school activities. They should also consider the balancing of the respective rights, keeping in mind that the school has the responsibility to enhance fundamental democratic values. If a nexus between the away-from-school and in-school activities does indeed exist, and if disruption is a definite possibility, the school can and should act and discipline the individuals involved, without having to fear that it will be infringing upon the concerned individuals' right to freedom of expression or right to privacy.

Given that the decision in Tinker dates back to 1969, one might question the relevance thereof when dealing with the issue of cyberbullying in an ever-changing world. Although it does offer a solid point of departure, a more advanced, wider-ranging approach is called for, such as the one Lorillard suggests. This approach,

⁷⁰ *Doninger v Niehoff* 2008 527 F 3d 41, 233 Ed Law Rep.

⁷¹ See Calvoz, Davis and Gooden 2014 *Cardozo L Rev* 104-112.

which seems to be a combination of *Tinker*, *Fraser* and the principle of the establishment of a clear nexus also seems to have a definite link with the *South African Constitution*. Sections 9, 10, 14, 16 and 28 deal with the issues of discrimination, human dignity, privacy, freedom of expression and the best interests of the child. Although this article is not intended as an in-depth discussion of all the different rights affected by cyberbullying, it is crucial to realise that in a specific scenario, there is always an array of rights of different persons to be balanced, and an approach such as the one suggested above will definitely also promote such a balancing of rights.

Being guided by the best interests of the child, as required in section 28(2) of the *Constitution*, will be critical during the process of balancing all the various applicable rights in a situation where cyberbullying is dealt with. The following section will focus on this essential right.

3 The right of the child (section 28 of the *Constitution*) and cyberbullying

As cyberbullying affects the young child at school, we need to look at section 28(2) of the *Constitution*, which states that the best interest of the child is of paramount importance in every matter concerning the child.⁷² This provision echoes article 3 of the *Convention on the Rights of the Child* (CRC).⁷³

Acknowledging the fact that no right is absolute and that it may, therefore, be limited, we argue that the rights or freedom of children may be limited in order to save them and those around them from harm caused by themselves because of their lack of *judicium* (meaning lack of discretion). However, when balancing the rights of children, one should be guided by the best interest of the child, a principal which is a well-established standard and guideline used by South African courts^{74 75} and an approach which fosters the application of fundamental values whilst protecting the child against potential danger and abuse.

⁷² See s 28(2) of the *Constitution*.

⁷³ *Convention on the Rights of the Child* (1990).

⁷⁴ *S v Petersen* 2008 2 SACR 355 (C).

⁷⁵ *Fish Hoek Primary School v G W* 2010 2 SA 141 (SCA).

It seems, therefore, that Fraser's value standard test should be used to ensure that the principle of the best interest of the child is adhered to. It could be that although a cyber bully may not necessarily disrupt the school, he or she is certainly infringing upon the rights of the victim. Juxtaposed with the victim's rights is the bully's right to privacy or his/her expectations of privacy. As the school aims to develop learners as balanced, value-driven citizens, and as there is a nexus between the bully and the victim as learner, the school needs to intervene in the best interest of the child. However, despite the fact that the above-mentioned approach is certainly commendable, it also raises some pertinent issues. The obvious ones that come to mind have to do with the right to privacy, together with the expectation of such a right, and the right to freedom of expression.

An issue that is not that often tackled when it comes to cyberbullying is privacy. The focus of this article will now move to the more contentious matter of the right to privacy, as guaranteed by section 14 of the *Constitution*.

4 The right to privacy in the context of cyberbullying

One can argue that a cyber user might have an expectation of privacy. Issues surrounding the intent of privacy of expression via cyberspace are not always clear. What if a child, after having set his or her privacy settings on Facebook so that his or her Facebook page can be accessed only by his/her friends, posts a comment about a scholar or educator at school and then shares this with his or her friends only? His or her intention was never for this to be distributed publicly beyond his or her circle of friends, yet one of his/her friends decides to circulate this wider, and ultimately this post comes to the attention of the school authorities and leads to the disciplining of the individual.

Did the child not have an expectation of privacy? The Facebook settings certainly suggest this, and what if he or she never intended for this expression to go beyond his or her circle of friends? In addition, consider that Facebook is set up in such a manner as to allow individuals the choice to add to or subtract from their circle of friends and to determine their privacy settings. This manner of operation by Facebook, which every Facebook user utilises, might definitely create an expectation

of privacy. Furthermore, what if the comment or expression might just have been a personal comment or expression that merely reflects someone's frustration with another person, as we all often do in private conversations, and the intention was never for the person or persons or institution which was spoken about to become aware of these comments?

Further, what if a learner sends an SMS to his/her best friend and in this SMS comments that the principal is an incompetent, bumbling fool and that everyone will be better off if he is taken out? This could be considered as a comment between close friends, not meant to be circulated, a personal opinion, and an expression of personal feelings, and yet if the friend forwards the SMS, it could lead to disciplinary steps against the learner.

The question then is how far the school's authority should go in balancing the right to privacy against the rights to freedom of expression, dignity and the best interest of the child in such scenarios. Where do schools draw the line? In an attempt to address cyberbullying, law was passed on 1 January 2015 in Illinois, that basically can legally compel students in that state to give their teachers access to their social media accounts.⁷⁶

The school and state officials indicated that the new cyberbullying legislation empowers educators with the ability to access the social media accounts of their students. This can happen if it is pertinent to preventing any hostile online behaviour, including cyberbullying outside the classroom and school hours.⁷⁷ The obvious intention with legislation such as this is to combat cyberbullying, but if students are expected to start handing over their passwords and personal information to educators, this raises definite privacy concerns.

American schools seem to have dealt with the issue of cyberbullying far more extensively, and often than is the case in South Africa. It would therefore make sense to look towards foreign law for possible guidance as to the manner in which

⁷⁶ Thalen 2015 <http://www.infowars.com/new-cyberbullying-law-will-force-illinois-students-to-give-up-social-media-passwords/>.

⁷⁷ Thalen 2015 <http://www.infowars.com/new-cyberbullying-law-will-force-illinois-students-to-give-up-social-media-passwords/>.

South African schools and courts should deal with this thorny issue. Legislation which comprehensively regulates the use of mobile phones and other electronic devices should be implemented by the stakeholders of South African education. However, what is also clear is that there seems to be a difference of opinion as to which approach to follow, and as Calvoz, Davis and Gooden⁷⁸ indicates, the Supreme Court of America has not dealt with this issue yet, a fact which muddies the waters even further.

This still leaves many questions unanswered, especially in a country such as South Africa, where cyberbullying legislation seems to lag behind that of other countries. The issue of the balancing of the right to freedom of expression and the dignity and safety of the individual will always remain central to this debate, but clearly the issue of the right to privacy is a matter that also needs to be addressed.

Increasingly, more stringent cyberbullying legislation, such as Bill C-13,⁷⁹ which was recently passed in Canada, has pushed the issue of the right to privacy even further to the forefront. This bill, which was the subject of prolonged discussions and which elicited an array of different opinions, is aimed at combating cyberbullying. Unfortunately, due to its far-reaching scope and the manner in which it had been drafted, it has alarmed many people and has raised issues of privacy as well as the extent to which the authority of law enforcement agencies in Canada should stretch.

No one contends that the scourge of cyberbullying should not be addressed by legislation and that the involvement of the various law enforcement agencies in the battle against this disease is needed, but in the process, the fundamental issue of the right to privacy should not be neglected. Herein lies the challenge for the drafters of legislation, law enforcement agencies and school authorities.

In terms of section 14 of the *South African Constitution*, everyone has the right to privacy, which includes the right not to have:

- (a) their person or home searched;

⁷⁸ See Calvoz, Davis and Gooden 2014 *Cardozo L Rev* 104-112.

⁷⁹ CBA 2014 <http://www.cba.org/cba/submissions/pdf/14-33-eng.pdf>.

- (b) their property searched;
- (c) their possessions seized; or
- (d) the privacy of their communications infringed upon.⁸⁰

The constitutionally entrenched right to privacy, including the privacy of one's communications, poses a challenge when dealing with and identifying anonymous cyber bullies, and implies that there will be a conflict between the right to freedom of expression and the right to privacy. The issue here is whether or not private expression in cyberspace should be seen as its creator's possession, because if it is then it could be searched and seized, since it qualifies as a possession. Surely if a school bag can be searched for a weapon if there is reasonable suspicion that the bag does indeed contain a weapon, authorities need a similar procedure they can follow if reasonable suspicion exists that a child is a victim of a cyber bully and the search for and seizure of the material, be it tangible or intangible, that constitutes the cyberbullying is warranted.

Thus, within a South African context the issue of privacy is just as contentious as is the case in other countries. As pointed out above, the right to privacy is indeed a fundamental right entrenched in the *South African Constitution* (as well as in the *Canadian Charter*⁸¹), and this right to privacy extends to all spheres of a person's life – including his or her expressions and communications. Nevertheless, this right must be balanced against other important rights. If one's expressions and communications infringe on others' right to dignity, or discriminate against others in an unfair manner, this could lead to the search for and seizure of these expressions and communications, which will have an effect on one's right to privacy.

The case of Nicola Brookes in the United Kingdom illustrated the importance of dealing with cyberbullying timeously, as well as the absolute necessity to put relevant and effective procedures in place to combat the evil of cyberbullying.⁸²

Nicola Brookes was tormented for months by anonymous internet bullies after she left an innocent message of support for an X Factor contestant on the social

⁸⁰ See s 14 of the *Constitution*.

⁸¹ *Canadian Charter of Rights and Freedoms*, 1982 (part I of the *Constitution Act* 80 of 1982).

⁸² Allen 2012 <http://www.dailymail.co.uk/news/article-215636>.

networking site. She went to the police to make a complaint but claimed that they failed to act and take her complaint seriously. The High Court eventually granted an order compelling the site to disclose the bullies' names, their email addresses, and their computers' internet protocol (IP) addresses, which can be used to determine a computer's location.⁸³ This is just one example of the various privacy issues around IP privacy that proved to be contentious and highlighted the need to address these issues through legislation.

Canada recognised this very fact and proposes to tackle these issues with the acceptance of Bill C-13: *Protecting Canadians from Online Crime Act*.⁸⁴ The Bill has elicited wide-ranging criticism, and lots of this criticism centres around privacy issues. These concerns seem legitimate and will surely be tested by the courts, as they should. No human right is exercised and applied in isolation and should, in practice, be balanced not only against the person's obligations but also against all other human rights that could be applicable in a specific scenario. The pertinent question remains: How should schools deal with the issue of the right to privacy, which every learner should enjoy, and the right, and need, to discipline cyberbullying? In an attempt to answer these questions, this article will now focus on Canada's Bill C-13.

5 Bill C-13: *Protecting Canadians from Online Crime Act*

The recent introduction of Bill C-13: *Protecting Canadians from Online Crime Act*, by the Canadian government has pushed the issue of privacy even further into the limelight when it comes to cyberbullying. When Peter Mackay, the Minister of Justice and Attorney General of Canada, introduced Bill C-13 in March 2015, he stated:

Our Government is committed to ensuring the safety of our children and youth, who deserve to feel safe in their communities and in their homes. When cyberbullying reaches the level of criminal activity, it can destroy lives. Sadly, cyberbullying is a harmful reality experienced by many young Canadians across the country. That is why I was proud to introduce the *Protecting Canadians from Online Crime Act*, to help better protect young Canadians from the harmful and devastating effects of cyberbullying. We are proud to announce that these important measures come into force today. For too long, the justice system was

⁸³ Allen 2012 <http://www.dailymail.co.uk/news/article-215636>.

⁸⁴ See CBA 2014 <http://www.cba.org/cba/submissions/pdf/14-33-eng.pdf>.

about protecting the rights of criminals, but our Government understands that the rights of victims need to be at the heart of the criminal justice system.⁸⁵

The obvious aim of the bill is to help protect "young Canadians from the harmful and devastating effects of cyberbullying", as Mackay pointed out.⁸⁶ At the official announcement and introduction of the law, he reiterated the fact that Bill C-13 will make Canadians, especially young people, safer while protecting their "personal integrity".⁸⁷ Mackay also stated that without the ability to "pre-emptively prevent online crime", Bill C-13 would not be effective.⁸⁸

The bill provides for two amendments to the *Criminal Code*,⁸⁹ and these are:

- it creates a new offence of the non-consensual distribution of intimate images, making it an offence to publish an intimate image of a person knowing that he or she did not provide consent or being reckless regarding the person's lack of consent; and
- it institutes new investigative powers (preservation demands, preservation orders and production orders) that allow law enforcement officers to collect electronic evidence relating to individuals that are subject to an investigation.⁹⁰

The bill also provides immunity from criminal and civil liability to a person (for example TSP, ISP or financial institution) who voluntarily preserves or provides data to a law official during an investigation. The bill also deals with "tracking data", "transmission data" and the securing of individuals' "transmission data", and makes provision for a new production order regarding transmission data and tracking data.

⁸⁵ Etobicoke 2015 <http://news.gc.ca/web/article-en.do?nid=945879&tp=1>.

⁸⁶ Etobicoke 2015 <http://news.gc.ca/web/article-en.do?nid=945879&tp=1>.

⁸⁷ Puzic 2015 <http://www.ctvnews.ca/politics/anti-cyberbullying-law-bill-c-13-now-ineffect-1.2270460>.

⁸⁸ Puzic 2015 <http://www.ctvnews.ca/politics/anti-cyberbullying-law-bill-c-13-now-ineffect-1.2270460>.

⁸⁹ *Criminal Code* RSC 1985.

⁹⁰ Handa, Birbilas and Di Fazio 2015 <http://www.blakes.com/English/Resources/Bulletins/Pages/Details.aspx?BulletinID=2057>.

A production order is a judicial order requiring a person to reveal the relevant computer data that may or may not have been the subject of a preservation order.⁹¹

Transmission data often reveals core biographical information about individuals,⁹² and examples of this include IP addresses or websites visited or search terms utilised.⁹³ Tracking data is information that relates to the location of a transaction, individual or thing. The peace or public officer (law enforcement authority) only needs to show "reasonable grounds for suspicion" that an offence has been or will be committed to obtain an order to search and seize order relating to transmission data as well as tracking data.⁹⁴ This enables law enforcement authorities to utilise a lower threshold to obtain a warrant in order to secure information about an internet user.

Penalties for contravening the demands or orders contained in the bill are also substantial, with fines of up to \$5 000 for individuals and up to \$250 000 for institutions, or six months' imprisonment.⁹⁵ It is clear that Canadians are determined to rid themselves of cyberbullying. The issue, however, is how to engage with privacy issues without violating them.

Prior to its acceptance on 9 December 2014,⁹⁶ the bill elicited substantial criticism from various quarters. During May of that year, the Canadian Bar Association (CBA) published a document in which they discussed the proposed Bill C-13 and raised some of their concerns about it. The CBA also offered some suggestions as to amendments to and omissions of certain provisions of the bill.⁹⁷

⁹¹ Handa, Birbilas and Di Fazio 2015
<http://www.blakes.com/English/Resources/Bulletins/Pages/Details.aspx?BulletinID=2057>.

⁹² See CBA 2014 <http://www.cba.org/cba/submissions/pdf/14-33-eng.pdf>.

⁹³ See Handa, Birbilas and Di Fazio 2015
<http://www.blakes.com/English/Resources/Bulletins/Pages/Details.aspx?BulletinID=2057>.

⁹⁴ Handa, Birbilas and Di Fazio 2015
<http://www.blakes.com/English/Resources/Bulletins/Pages/Details.aspx?BulletinID=2057>.

⁹⁵ Handa, Birbilas and Di Fazio 2015
<http://www.blakes.com/English/Resources/Bulletins/Pages/Details.aspx?BulletinID=2057>.

⁹⁶ See Puzic 2015 <http://www.ctvnews.ca/politics/anti-cyberbullying-law-bill-c-13-now-ineffect-1.2270460>.

⁹⁷ See CBA 2014 <http://www.cba.org/cba/submissions/pdf/14-33-eng.pdf>.

In the document referred to above, the CBA rightly stated that Bill C-13 is primarily intended to protect children and youth from online predators and exploitation – a goal they supported wholeheartedly. However, they pointed out that the mechanism used to meet this goal must be drafted with precision to capture only the impugned conduct.⁹⁸ Furthermore, the CBA also dealt with the issue of privacy and law enforcement at length.

According to many, the privacy of members of the public would be seriously compromised by the bill, which definitely created the impression that "Big Daddy is watching", as it allowed for huge amounts of information to be gathered by an open-ended group of public officials "for purposes that stretch wider than the fight against cyberbullying and are less compelling".⁹⁹ This, of course, speaks directly to the issue of privacy.

Seemingly, the bill is downgrading privacy issues to a "reasonable suspicion" standard. This caused many concerned entities to call for a "more compelling case for the use of a reduced legal threshold to be presented and examined",¹⁰⁰ since this would give legal immunity to people or telecoms who voluntarily turned over sensitive information to law enforcement.

Carol Todd, Amanda Todd's mother, voiced the fear and concerns of many Canadians when, in reference to Bill C-13, she stated: "We should not have to choose between our privacy and our safety."¹⁰¹ She was "troubled" by portions of the bill and exhibited concerns about the possibility that children's privacy rights could be sacrificed by the bill, whilst voicing similar concerns about the provisions that condone "the sharing of Canadians' privacy information without proper legal process", which seems to be a reference to the reduced threshold for obtaining warrants and production orders, as well as the fact that legal authorities would be

⁹⁸ CBA 2014 <http://www.cba.org/cba/submissions/pdf/14-33-eng.pdf>.

⁹⁹ Payton 2014 <http://www.cbc.ca/news/politics/cyberbullying-bill-raises-alarm-for-privacy-commissioner-1.2842034>.

¹⁰⁰ Payton 2014 <http://www.cbc.ca/news/politics/cyberbullying-bill-inches-closer-to-law-despite-privacy-concerns-1.2795219>.

¹⁰¹ Geist 2014 <http://www.michaelgeist.ca/2014/11/carol-todd-bill-c-13-happened-democracy/>.

able to access loads of personal information about individuals.¹⁰² According to Dyer,¹⁰³ concerns in particular were that Bill C-13 would allow police to interfere in people's lives, stating that "fishing expeditions and snooping will become much more common". Seemingly, the bill also offered a no-liability guarantee to telecoms companies if they voluntarily disclosed information about their customers.¹⁰⁴

The fact that the bill, in the eyes of many, proposed to ask companies to hand over data on basically anyone at any time and offered the added incentive of exemption from prosecution to companies if they cooperated with the law authorities rang alarm bells for many. This prompted various role players to suggest that the bill be split, in order to address the more controversial aspects separately.¹⁰⁵ ¹⁰⁶ ¹⁰⁷ Government and law enforcement agencies, on the other hand, were of the opinion that the wider range of investigative powers Bill C-13 offered was necessary in order for them to be able to investigate cybercrimes properly and effectively.¹⁰⁸

Nevertheless, the CBA¹⁰⁹ claimed that according to section 8 of the *Canadian Charter*, which is in line with section 14(c) of the *Constitution of South Africa*, such information as is often contained in "transmission data" was actually protected from search and seizure, and thus private. Section 8 of the *Canadian Charter*¹¹⁰ stated that everyone has the right to be secure against unreasonable search or seizure, which implied that this section also covered the seizure of confidential information. If this was the case, Bill C-13 could already be regarded as unconstitutional. The issue at stake, however, was how to legally limit this constitutional right to privacy and how to ensure that the principle of suspicion, whilst enhancing this limitation, would

¹⁰² CTVNews 2014 <http://www.ctvnews.ca/canada/anti-cyberbullying-bill-could-harm-privacy-rights-Amanda-Todd-s-mother-warns-1.1819653>.

¹⁰³ Dyer 2014 <http://www.cbc.ca/news/politics/cyberbullying-bill-draws-fire-from-diverse-mix-of-critics-1.2803637>.

¹⁰⁴ Dyer 2014 <http://www.cbc.ca/news/politics/cyberbullying-bill-draws-fire-from-diverse-mix-of-critics-1.2803637>.

¹⁰⁵ Lubao 2013 <http://www.globalresearch.ca/canadian-conservatives-cyber-bullying-bill-a-pretext-for-expanding-police-surveillance/5361042>.

¹⁰⁶ See CBA 2014 <http://www.cba.org/cba/submissions/pdf/14-33-eng.pdf>.

¹⁰⁷ See Payton 2014 <http://www.cbc.ca/news/politics/cyberbullying-bill-raises-alarm-for-privacy-commissioner-1.2842034>; Payton 2014 <http://www.cbc.ca/news/politics/cyberbullying-bill-inches-closer-to-law-despite-privacy-concerns-1.2795219>.

¹⁰⁸ Mas 2014 <http://www.cbc.ca/m/touch/canada/story/1.2670736>.

¹⁰⁹ See CBA 2014 <http://www.cba.org/cba/submissions/pdf/14-33-eng.pdf>.

¹¹⁰ See s 8 of the *Canadian Charter of Rights and Freedoms*, 1982.

become the gateway to ensure that privacy would indeed not be violated. The CBA held that transparency and oversight should always be present when dealing with extraordinary state powers, and it was this principle that as the driving force behind most of their suggestions and proposals¹¹¹ in response to the fears and concerns many Canadians harboured with regard to Bill C-13.

In an attempt to ensure that the right to privacy would not be violated by Bill C-13, the CBA pointed out that the mechanism used to meet the commendable goal of combating online crime had to be drafted with precision to capture only the impugned conduct.¹¹² The CBA also commented on the lower threshold the bill created for preservation demands and orders. The CBA purported that the threshold of "reasonable grounds to believe" should be used to obtain data, which was a higher threshold than "reasonable grounds to suspect",¹¹³ and thus more acceptable, since the issue at hand, privacy, was an important one.

Furthermore, the CBA suggested that such a preservation demand should be utilised only in exigent circumstances where there was reason to believe that the data in question might be lost or destroyed before judicial authorisation could be secured, going on to say that when officers executed a preservation demand, written records had to be produced so as to indicate the bases on which the demand was made.¹¹⁴

Such an approach called for greater circumspection by the police and other government agencies in the execution of their duty when utilising preservation demands. It also called for measures to be put in place to ensure that Canadians' rights were not being infringed upon. One could also surmise that this proposal for written records to be produced would ensure that a record as well as procedural and substantive reasons was available for verification purposes. Such a proposal would then be "a step closer to a proper legal process".¹¹⁵

¹¹¹ See CBA 2014 <http://www.cba.org/cba/submissions/pdf/14-33-eng.pdf>.

¹¹² See CBA 2014 <http://www.cba.org/cba/submissions/pdf/14-33-eng.pdf>.

¹¹³ See CBA 2014 <http://www.cba.org/cba/submissions/pdf/14-33-eng.pdf>.

¹¹⁴ See CBA 2014 <http://www.cba.org/cba/submissions/pdf/14-33-eng.pdf>.

¹¹⁵ See CTVNews 2014 <http://www.ctvnews.ca/canada/anti-cyberbullying-bill-could-harm-privacy-rights-Amanda-Todd-s-mother-warns-1.1819653>.

In sum, although the CBA was in agreement with and understood the need to ensure effective criminal investigations in the modern age of technology, they were of the opinion that the enhanced state power that Bill C-13 offered ought to be accompanied by effective oversight mechanisms, which supported Payton's argument that the "potential level of government intrusion must be matched by commensurate judicial scrutiny and an appropriate legal standard for authorization".¹¹⁶ To this end, the CBA suggested the establishment of a single entity to consider the overall and nation-wide impact of the seizure, retention and use of personal information by Canadian law enforcement agencies.¹¹⁷

As pointed out, after lengthy discussion and deliberation, Bill C-13 was accepted in December 2014 and officially introduced in March 2015. However, before its final acceptance an important concession was made: the bill was passed but with the *proviso* that the investigative powers of the police and other state agencies be limited and were not to exceed the standard set by the court in *R v Spencer*.¹¹⁸ The decision in this case enshrined Canadians' rights to privacy and delivered a body blow to some of the provisions the government had in mind when proposing Bill C-13.¹¹⁹

By way of illustrating the concerns raised above, we will now focus on the *Spencer* case, recently decided in Canada, since this case dealt directly with privacy issues and search and seizure in cyberspace.

6 R v Spencer (2014)

In this matter, decided during June 2014, the Supreme Court of Canada had to address issues of privacy, information sharing and the lawfulness of search and seizure procedures. The appellant, *Spencer*, was convicted on a charge of the possession of child pornography and acquitted on a charge of making this pornography available. He appealed the conviction, which resulted in the Court of

¹¹⁶ See Payton 2014 <http://www.cbc.ca/news/politics/cyberbullying-bill-inches-closer-to-law-despite-privacy-concerns-1.2795219>.

¹¹⁷ See CBA 2014 <http://www.cba.org/cba/submissions/pdf/14-33-eng.pdf>.

¹¹⁸ *R v Spencer* 2014 CarswellSask 342, 2014 (SCC) 43.

¹¹⁹ CBC News 2014 <http://www.cbc.ca/news/technology/internet-users-privacy-upheld-by-canada-s-top-court-1.2673823>.

Appeal dismissing the accuser's appeal, but ordering a new trial. Yet again, the accused lodged an appeal against this decision, resulting in the Supreme Court dismissing his appeal and upholding the Court of Appeal's order for a new trial on the "making available" count.¹²⁰

Central to this issue was the fact that the police had identified the internet protocol (IP) address of a computer that someone had been using to access and store child pornography via an Internet file-sharing programme. Then, without judicial authorisation, the police obtained, from the internet service provider (ISP), the subscriber information associated with and linked to that specific IP address.¹²¹ It was this information that specifically led the police to Spencer, the appellant: He had downloaded child pornography and stored it in a folder that was accessible to other Internet users using the same file-sharing programme.

Spencer alleged that the police had conducted an unconstitutional search by obtaining subscriber information matching the IP address and that the evidence obtained by the police should, therefore, be excluded. The police had made a written "law enforcement request" to Shaw (the ISP) for the subscriber information, including the name, address and telephone number of the customer using the IP address. They made this request in terms of section 7(3)(c.1)(ii) of the *Personal Information Protection and Electronic Documents Act*, SC 2000 (PIPEDA)¹²² by indicating that the police were investigating a criminal offence under the Criminal Code's C-46,¹²³ which pertains to child pornography, and that the subscriber information was being sought as part of an ongoing investigation. Shaw complied with this request, which eventually led the police to Spencer and the latter's seizure of the relevant evidence used in the case.¹²⁴

The court had to decide whether this request to Shaw by the police constituted a "reasonable search". As pointed out, the court first had to establish whether the police's request to Shaw, which resulted in their obtaining the subscriber

¹²⁰ See *R v Spencer* 2014 CarswellSask 342, 2014 (SCC) 43.

¹²¹ *R v Spencer* 2014 CarswellSask 342, 2014 (SCC) 43.

¹²² *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (PIPEDA).

¹²³ See *Criminal Code* RSC 1985.

¹²⁴ *Criminal Code* RSC 1985.

information, could be considered as "search or seizure" within the meaning of section 8 of the *Canadian Charter*.¹²⁵ To arrive at this decision, the circumstances as a whole had to be considered, as well as whether Mr Spencer had a reasonable expectation of privacy and, had this indeed been the case, whether obtaining the information constituted a "search".

The court indicated that in order to determine the reasonable expectation of privacy given the circumstances as a whole, a couple of factors ought to be taken into account. The two circumstances the court specifically referred to in order to determine the reasonableness of Spencer's expectation of privacy are the nature of the privacy interest at stake and the statutory and contractual framework governing the ISP's disclosure of subscriber information.¹²⁶

The Crown contested that the subject matter of the alleged search was simply a name, address and telephone number matching a publicly available IP address, while Spencer alleged that this information revealed core biographical data which revealed intimate and private information about the people living at that address. The court disagreed with the Crown, stating that the subject matter did indeed reveal more than merely an address and a name: it revealed the identity of an Internet subscriber which corresponded with a particular form of Internet usage.¹²⁷

In their explication the court referred to *Trapp*,¹²⁸ in which the judge indicated that the significance of an IP address and what such an address, once identified with a particular individual, is capable of revealing about that individual's online activity in the home cannot be glossed over. Although details such as these might simply be referred to as "subscriber information", such a narrow definition does not sufficiently reveal the true nature and that which can be disclosed about a person.¹²⁹ In this case, the court held thus and concluded that the argument of the Crown was not sustainable since the identity of the subscriber was linked to particular monitored Internet activity and thus constituted far more than just a name and address.

¹²⁵ See s 8 of the *Canadian Charter of Rights and Freedoms*, 1982.

¹²⁶ See *R v Spencer* 2014 CarswellSask 342, 2014 (SCC) 43.

¹²⁷ *R v Spencer* 2014 CarswellSask 342, 2014 (SCC) 43.

¹²⁸ *R v Trapp* 2011 CarswellSask 785, 2011 (SKCA) 143.

¹²⁹ See *R v Spencer* 2014 CarswellSask 342, 2014 (SCC) 43.

In the case of *R v Spencer*, the court also dealt with the nature of the privacy interest potentially compromised by the actions of the state in this matter, which constituted another fundamental factor when assessing the reasonableness of expectation of privacy. The court reiterated that the privacy of the area or the thing being searched and the impact of the search on its target were the issues at stake, not the legal or illegal nature of the items sought.¹³⁰ For this reason, regardless of whether or not people in general have a privacy interest in subscriber information with respect to the computers they use in their homes for private purposes, the issue at stake here was whether Spencer had a legitimate privacy interest in concealing his use of the Internet to access child pornography.¹³¹

The court also discussed the issue of territorial privacy and stated that Internet users do not expect their online anonymity to cease when they make use of the Internet outside their homes (in other words, in a different territory). The reasonable expectation of privacy is still present. Importantly, the notion of privacy, according to the court, also related to the wider notion of control of, access to, and the use of information: situations did exist where people had a reasonable expectation that information would remain confidential and be used for the purposes for which it had been provided, despite the fact that the information had been communicated.¹³²

Furthermore, the court also emphasised the notion of anonymity when dealing with privacy and, echoing Westin,¹³³ identified anonymity as one of the basic states of privacy. It pointed out that this realisation and acceptance of anonymity as one of the basic states of privacy became particularly poignant within the context of Internet usage and conceded that anonymity may be the foundation of a privacy interest that ensured constitutional protection against unreasonable search and seizure.

Based on these premises, the court found that the police had had ample opportunity to obtain a production order which would have required Shaw to release subscriber

¹³⁰ *R v Spencer* 2014 CarswellSask 342, 2014 (SCC) 43.

¹³¹ *R v Spencer* 2014 CarswellSask 342, 2014 (SCC) 43.

¹³² *R v Spencer* 2014 CarswellSask 342, 2014 (SCC) 43.

¹³³ Westin 2003 *Journal of Social Issues* 431-453.

information relating to the IP address in question. From within this framework (recognition of the right to anonymity in certain circumstances), the court applied a particular set of facts to the *Spencer* case and found that the police's request to link a given IP address to subscriber information was in effect a request to link a certain person to specific online activities.¹³⁴ This triggered the activation of a high level of informational privacy.

The court then turned to the issue of *Spencer's* reasonable expectation of privacy. Here, *Shaw's* terms and conditions as the ISP were analysed, resulting in the court drawing the conclusion that *Shaw's* collection, use and disclosure of its subscribers' personal information was subject to PIPEDA, which protects personal information held by commercial organisations involved in commercial activities from being disclosed without the knowledge or consent of the person to whom the information relates. In this regard, the Crown relied on section 7(3)(c.1)(ii)¹³⁵ for disclosure without consent to a government institution where such an institution has identified its lawful authority to obtain information.¹³⁶

Nevertheless, the court then argued that the intention with PIPEDA was to establish rules that would govern the disclosure of "personal information in a manner that recognizes the right to privacy of individuals with respect to their personal information".¹³⁷ For this reason, the court held that it would be reasonable for an Internet user to expect that a simple request by the police would not set in motion an obligation to disclose personal information or defeat the general purpose of PIPEDA, seeing that the latter was aimed at the prohibition of the disclosure of personal information.¹³⁸

In sum, the court in this case found that, given the specific circumstances in question, a reasonable expectation of privacy in as far as subscriber information existed, and that a request by the police that an ISP voluntarily discloses information amounted to a search. The court then went on to explain that such a search was not

¹³⁴ See *R v Spencer* 2014 CarswellSask 342, 2014 (SCC) 43.

¹³⁵ See s 7(3)(c.1)(ii) of PIPEDA.

¹³⁶ See *R v Spencer* 2014 CarswellSask 342, 2014 (SCC) 43.

¹³⁷ See s 3 of PIPEDA.

¹³⁸ See *R v Spencer* 2014 CarswellSask 342, 2014 (SCC) 43.

lawful and that section 487.014(1) of the *Criminal Code*, which provides that a peace officer does not need a production order to ask a person "to voluntarily provide to the officer documents, data and information that the person is not prohibited by law from disclosing" did not apply in this instance.¹³⁹ This was the case because PIPEDA specifically prohibits disclosure of the information unless the requirements of the law enforcement provision have been met, which had not happened in this case. In the opinion of the court, the provisions of section 7(3)(c.1)(ii) also did not apply. As the court stated:

Since in the circumstances of this case the police do not have the power to conduct a search for subscriber information in the absence of exigent circumstances or a reasonable law, I do not see how they could gain a new search power through the combination of a declaratory provision and a provision enacted to promote the protection of personal information.¹⁴⁰

It is fundamental to realise that the decision in *R v Spencer* potentially reined in some of the wide-ranging powers Bill C-13 intended to lend to law enforcement authorities in so far as online crime is concerned. This decision effectively prohibits internet service providers from voluntarily disclosing the names, phone numbers and addresses of their customers in response to an informal request by the police.¹⁴¹ The court was clear in *R v Spencer* that Internet users, or for that matter users of electronic media, have a definite expectation of privacy, and by inference anonymity, and that if service providers were to hand out user information willy-nilly to police and other law enforcement agencies, this expectation, as protected by PIPEDA, would not be honoured.

To complicate matters even further, the matter *R v Spencer* also dealt with the lowering of the threshold for production orders. Despite the fact that the court in this case determined that law enforcement officers should obtain a warrant or order if they seek certain information concerning Internet users or want to compel internet service providers to supply such information about their clients, Bill C-13 still reads that "reasonable grounds to suspect", instead of "reasonable grounds to believe",

¹³⁹ See *Criminal Code* RSC 1985.

¹⁴⁰ See *R v Spencer* 2014 CarswellSask 342, 2014 (SCC) 43.

¹⁴¹ See Payton 2014 <http://www.cbc.ca/news/politics/cyberbullying-bill-inches-closer-to-law-despite-privacy-concerns-1.2795219>.

are all that is required for a law enforcement agency to obtain an order that would compel internet service providers to disclose information about their customers. In fact, the bill encourages internet service providers to share information about their users because, should they do so, they may be indemnified from prosecution.

Clearly, despite the issues raised in *R v Spencer*, Bill C-13 seemingly continues to circumvent certain issues as to privacy, and many Canadians are of the opinion that these compromises ought to be challenged in court. Despite the expectation *R v Spencer* raised as to the ability to challenge the right to privacy and anonymity as contained in PIPEDA and section 8 of the *Canadian Charter*, all of these rights can be shattered by a mere production order that shows "reasonable grounds to suspect a crime has been committed or will be committed". To appreciate the seriousness of the matter, do keep in mind that in 2011 alone, Canadian Wireless Telecommunications reported that it had received more than 1,2 million requests for customer information and had complied with 780 000 of these requests.¹⁴²

Judging by the opposition and reaction of many Canadians to Bill C-13, a fundamental right such as privacy cannot be easily overridden by new legislation. Such a transgression is bound to be challenged in court. With the lessons the Canadians have learnt with the promulgation of Bill C-13 and the *Spencer* case in mind, this paper will now propose a number of ways South African school authorities should go about addressing the issue of cyberbullying.

7 Implications for South African school authorities when dealing with cyber bullies

To date, the South African judicial system has not been at the forefront of taking any aggressive steps or instituting any processes to combat the problem of cyberbullying. Cassim¹⁴³ rightfully avers that South African legislation has not kept track with technology and cyber developments in as far as safeguarding learners' human rights in terms of cyberbullying is concerned. Clearly, the lessons the US, UK

¹⁴² See Payton 2014 <http://www.cbc.ca/news/politics/cyberbullying-bill-raises-alarm-for-privacy-commissioner-1.2842034>.

¹⁴³ See Cassim 2013 *SACJ* 1-20.

and Canada learnt in this regard could be of value when addressing this local lag in legislation.

The right to freedom of expression and the right to privacy are rights that are indeed entrenched in the *South African Constitution*, as is the case in the US, UK and Canada. Locally the challenge arises when these rights have to be balanced within a specific scenario and, specifically, in such a way that the spirit, notions and ideals of the *South African Constitution* would be enhanced.

Against this background, consider this: in a cyberbullying scenario, there is a victim, a bully and the authorities. Each party has rights and obligations, and each party's rights and obligations must be weighed and balanced in order to achieve the ideals of the *Constitution*.

The cyber bully, just like anyone else, has the right to freedom of expression and privacy. These rights ought to be balanced against the victim's rights to human dignity, life and a safe environment, in other words to the best interest of the child. The school has similar rights, but to this must be added its duty to act as a custodian that fosters fundamental constitutional and democratic values. In order to fulfil this duty, though, the school has to balance the rights of the victim, the rights of the bully and the rights of those scholars who have not been affected.

To date, the value standard as applied in the case of Fraser has seemingly acted as a focal point whenever matters relating to cyberbullying had to be addressed – and rightfully so, because the school's ultimate duty is to foster, nurture and promote democratic and constitutional values in the best interest of the child. Despite that noble intent, in a more recent case (*R v Spencer*), the court found that Internet users have a definite expectation of privacy and that this fundamental right should not be neglected.

Therefore, seeing that cyberbullying predominantly involves children who are often immature and still developing emotionally, spiritually and cognitively, schools clearly have a duty as per their well-documented *in loco parentis* role to limit children's right

to privacy in a substantial way should such a limitation serve the interest of the child better than neglecting to do so would.

Without doubt, all schools should formulate a policy that deals with cyberbullying. This should form part of the Code of Conduct for learners and should clearly state when cell phones or any form of social media may be used, and within which rules, to ensure that all learners are respected and their rights protected. As matters stand, and in accordance with section 16 of the *South African Schools Act*,¹⁴⁴ the governance of a public school is vested in its governing body, which implies that this body will have to be at the forefront of the battle against cyberbullying. Given the lack of guidance and legislation regarding this type of crime, though, governing bodies might well find themselves embroiled in acrimonious court battles about matters of privacy, freedom of expression and the like, if the history of similar cases abroad as cited in this paper is anything to go by.

A case in point is section 8A of the *Schools Act*,¹⁴⁵ which provides school governing bodies with the legal method and procedures to conduct search-and-seizures, yet limits learners' right to privacy as entrenched in section 14 of the *Constitution*.¹⁴⁶ In so far as section 8A provides for legal procedures to be followed during search and seizures at school when a fair and reasonable suspicion has been established that a dangerous object or illegal drug might be on a person or in his/her belongings, the provisions of this section in all likelihood do not cover the issues that have a bearing on suspicions of cyberbullying.

8 Conclusion

Although Cassim¹⁴⁷ contends that current South African legislation can deal with cyberbullying to a certain extent, several loopholes in the law need to be remedied and numerous practical solutions to curb instances of cyberbullying will have to be identified, as indicated by Canadian legislation.

¹⁴⁴ Section 16 of the *South African Schools Act* 84 of 1996.

¹⁴⁵ Section 8A of the *South African Schools Act* 84 of 1996.

¹⁴⁶ See s 14 of the *Constitution*.

¹⁴⁷ See Cassim 2013 *SACJ* 1-20.

It would indeed be a sad day if cyber bullies could indefinitely hide behind their right to privacy while they are tormenting others. In fact, to quote Arthur Goldstuck, bullies should know that "[i]t is a myth that people can remain anonymous on the internet or through BBM. There are ways that people can be traced..."¹⁴⁸

This said, it would be just as sad if people had to unnecessarily and unduly be exposed to the reality of having their privacy unscrupulously compromised by entities that abuse legislation by allowing an unbridled investigation into people's confidential matters and information.

For this reason, when legal mechanisms are designed and instituted against cyberbullying, we are under an obligation to ensure that these truly serve the best interest of the child and also balance all rights. This is the challenge South African law makers and school governing bodies are confronted with today.

All schools ought to have a disciplinary mechanism in place that will help the school governing body to put an end to cyberbullying, as per the advice offered by Hummingbird Education.¹⁴⁹ Depending on the severity of the misconduct, the cyber bully could face suspension, expulsion and even criminal charges, and sanctions imposed by way of this mechanism would be dependent upon the relevant school's Code of Conduct. In the long run, though, and irrespective of the actions instituted, it is contingent upon the school's governing body to ensure that all legislation, and in particular the *South African Constitution*, is adhered to at all times. Social media should be used at schools only perform scholastic assignments and not to enhance learners' personal profiles.

Currently, South Africa does not have legislation dealing with cyberbullying and the privacy of the internet user *per se*. Consequently, schools are often placed in a position where they have to choose between their learners' safety and their learners' privacy, with little regard to the fundamental rights learners ought to be able to enjoy at school. However, it is without doubt the legal duty of the school's governing

¹⁴⁸ See Rondganger 2012 <http://www.iol.co.za/dailynews/opinion/cyberbullying-a-cause-for-concern-1.1261733#.VTSdBJP06Kg>.

¹⁴⁹ Hummingbird Education Date Unknown <https://www.hummingbirdza.com/cyberbullying-advice-victims/>.

body to ensure that measures are in place to protect the victim of the cyber bullies. As parents need to know where their children are and what they are doing, they should also know which social media their children are connected to and what they are doing on them. Because they are *in loco parentis*, schools should therefore have social media policies in place where learners are given limited access to limited content with proper supervision.

Countries such as Canada, the United States of America and Britain have indeed had more extensive experience with the issue of balancing the rights of parties when it comes to dealing with cyberbullying. They have developed fairly comprehensive legislation with regards to cyberbullying and have a far greater volume of case law on the issue of cyberbullying than South Africa has. Therefore we suggest that we should look towards the action these countries have taken in the fight against cyberbullying and learn from them.

One must not forget, as pointed out in this article, that although these countries have made great strides in the area of combatting cyber bullying, they are still faced with many unanswered questions and significant uncertainty, as the discussion and application of Bill C-13 so clearly demonstrates. The latter will definitely be tested in Canadian courts, which test would, without a doubt, have an impact on the whole issue of cyberbullying and the manner in which the law deals with it.

In addition to the legislature's learning from the transatlantic experience, South African courts should also offer some guidance in this matter, and we foresee that future judgments will also be instrumental in shaping legislation and policy and the application thereof when it comes to cyberbullying.

BIBLIOGRAPHY**Literature**

Alexander and Alexander *American Public School Law*

Alexander K and Alexander MD *American Public School Law* (West St Paul Minn 1992)

Alston *Constitutional Right to Freedom of Expression*

Alston KS *The Constitutional Right to Freedom of Expression: An Exploration of its Relevance to the South African School Community* (PhD-thesis University of the Free State 2002)

Bonnono and Shelley 2013 *J Youth Adollesc*

Bonnono RA and Shelley H "Cyberbullying and Internalizing Difficulties Above and Beyond the Impact of Traditional Forms of Bullying" 2013 *J Youth Adollesc* 685-697

Bray *Human Rights in Education*

Bray W *Human Rights in Education* (CELP Pretoria 2000)

Brunsma *School Uniform Movement*

Brunsma DL *The School Uniform Movement and What It Tells Us About American Education: A Symbolic Crusade* (Scarecrow Education Lanham MD 2004)

Calvoz, Davis and Gooden 2014 *Cardozo L Rev*

Calvoz RR, Davis BW and Gooden MA "Constitutional Implications of Punishment for Cyber Bullying" 2014 *Cardozo L Rev* 104-112

Cassim 2013 *SACJ*

Cassim F "Formulating Adequate Legislation to Address Cyber-bullying: Has the Law Kept Pace with Advancing Technology?" 2013 *SACJ* 1-20

Clay 2009 *Am U L Rev*

Clay C "Tinker's Midlife Crisis: Tattered and Transgressed but Still Standing"
2009 *Am U L Rev* 1167-1192

Currie and De Waal *Bill of Rights Handbook*

Currie I and De Waal J *The Bill of Rights Handbook* 4th ed (Juta Cape Town
2001)

Kift, Campbell and Butler 2010 *JLIS*

Kift S, Campbell M and Butler D "Cyberbullying in Social Networking Sites and
and Blogs: Legal Issues for Young People and Schools" 2010 *JLIS* 352-359

Lorillard 2011 *Miss LJ*

Lorillard CM "When Childrens Rights 'Collide': Free Speech vs the Right to Be
Left Alone in the Context of Off-campus 'Cyber-bullying'" 2011 *Miss LJ* 189-
263

Mawdsley, Smit and Wolhuter 2013 *De Jure*

Mawdsley RD, Smit MH and Wolhuter CC "Students, Websites, and Freedom
of Expression in the United States and South Africa" 2013 46(1) *De Jure* 9

Slonje and Smith 2008 *Scand J Psychol*

Slonje R and Smith PK "Cyberbullying: Another Main Type of Bullying?" 2008
Scand J Psychol 147-154

Tokunaga 2010 *Comput Hum Behav*

Tokunaga RS "Following You Home From School: A Critical Review and
Synthesis of Research on Cyberbullying Victimization" 2010 *Comput Hum
Behav* 277-287

Tustin, Zulu and Basson 2014 *CARSA*

Tustin DH, Zulu GN and Basson A "Bullying Among Secondary School Learners
in South Africa with Specific Emphasis on Cyber Bullying" 2014 *CARSA* 13-25

Van Vollenhoven *Learners' Understanding*

Van Vollenhoven WJ *Learners' Understanding of their Right to Freedom of Expression in South Africa* (PhD-thesis University of Pretoria 2005)

Van Vollenhoven, Beckmann and Blignaut 2006 *Journal of Education*

Van Vollenhoven WJ, Beckmann JL and Blignaut AS "Freedom of Expression and the Survival of Democracy: Has the Death Knell Sounded for Democracy in South African Schools?" 2006 *Journal of Education* 119-140

Westin 2003 *Journal of Social Issues*

Westin AF "Social and Political Dimensions of Privacy" 2003 *Journal of Social Issues* 431-453

Wood 2001 *SAJE*

Wood NG "Freedom of Expression of Learners at South African Public Schools" 2001 *SAJE* 142-146

Case law

Canada

R v Spencer 2014 CarswellSask 342, 2014 (SCC) 43

R v Trapp 2011 CarswellSask 785, 2011 (SKCA) 143

South Africa

Acting Superintendent-General of Education of KwaZulu-Natal v Ngubo 1996 3 BCLR 369 (N)

Antonie v Governing Body, Settlers High School 2002 4 SA 738 (C)

Fish Hoek Primary School v G W 2010 2 SA 141 (SCA)

Hamata v Chairperson, Peninsula Technikon Internal Disciplinary Committee 2000 4 SA 621 (C)

Le Roux v Dey 2011 3 SA 274 (CC)

Pillay v KwaZulu-Natal MEC of Education and Cronje 2006 JOL 17833 (N)

S v Petersen 2008 2 SACR 355 (C)

Western Cape Residents' Association obo Williams v Parow High School 2006 3 SA 542 (C)

United States of America

Bethel School District No 403 v Fraser 1986 478 US 675, 106 (S Ct) 3159

Doninger v Niehoff 2008 527 F 3d 41, 233 Ed Law Rep

Morse v Frederik 2007 551 US 393, 127 (S Ct) 2618

Tinker v Des Moines Independent Community School District 1969 393 US 503, 89 (S Ct) 733

United States v O'Brien 1968 US 232, United States Supreme Court

Wiesniewski v Board of Education of the Weedsport Central School District 2007 494 F 3d 34

Legislation***Canada***

Canadian Charter of Rights and Freedoms, 1982

Constitution Act 80 of 1982

Criminal Code RSC 1985

Personal Information Protection and Electronic Documents Act, SC 2000, c 5

South Africa

Constitution of the Republic of South Africa, 1996

South African Schools Act 84 of 1996

International instruments

Convention on the Rights of the Child (1990)

Internet sources

Allen 2012 <http://www.dailymail.co.uk/news/article-215636>

Allen V 2012 *Victory Over Cyber Bullies: Legal First as High Court orders Facebook to Reveal Trolls Who Tormented Mother for Defending X Factor Star*
<http://www.dailymail.co.uk/news/article-2156365/> accessed 19 March

CBA 2014 <http://www.cba.org/cba/submissions/pdf/14-33-eng.pdf>

Canadian Bar Association 2014 *Bill C-13, Protecting Canadians from Online Crime Act* <http://www.cba.org/cba/submissions/pdf/14-33-eng.pdf> accessed 19 March 2015

CBC News 2014 <http://www.cbc.ca/news/technology/internet-users-privacy-upheld-by-canada-s-top-court-1.2673823>

CBC News 2014 *Internet Users' Privacy Upheld by Canada's Top Court* <http://www.cbc.ca/news/technology/internet-users-privacy-upheld-by-canada-s-top-court-1.2673823> accessed 23 March 2015

CTVNews 2014 <http://www.ctvnews.ca/canada/anti-cyberbullying-bill-could-harm-privacy-rights-Amanda-Todd-s-mother-warns-1.1819653>

CTVNews 2014 *Anti-cyberbullying Bill Could Harm Privacy Rights, Amanda Todd's Mother Warns* <http://www.ctvnews.ca/canada/anti-cyberbullying-bill-could-harm-privacy-rights-Amanda-Todd-s-mother-warns-1.1819653> accessed 12 March 2015

Dean 2012 <http://www.newyorker.com/culture/culture-desk/the-story-of-amanda-todd>

Dean M 2012 *The Story of Amanda Todd* <http://www.newyorker.com/culture/culture-desk/the-story-of-amanda-todd> accessed 18 March 2015

Ditch the Label 2015 <http://www.ditchthelabel.org/dealing-with-cyberbullying/>

Ditch the Label 2015 *Dealing with Cyber Bullying* <http://www.ditchthelabel.org/dealing-with-cyberbullying/> accessed 29 March 2015

Dyer 2014 <http://www.cbc.ca/news/politics/cyberbullying-bill-draws-fire-from-diverse-mix-of-critics-1.2803637>

Dyer E 2014 *Cyberbullying Bill Draws Fire from Diverse Mix of Critics* <http://www.cbc.ca/news/politics/cyberbullying-bill-draws-fire-from-diverse-mix-of-critics-1.2803637> accessed 19 March 2015

Etobicoke 2015 <http://news.gc.ca/web/article-en.do?nid=945879&tp=1>

Etobicoke ON 2015 *Legislation to Crack Down on Cyberbullying Comes Into Force* <http://news.gc.ca/web/article-en.do?nid=945879&tp=1> accessed 19 March 2015

Geist 2014 <http://www.michaelgeist.ca/2014/11/carol-todd-bill-c-13-happened-democracy/>

Geist M 2014 *Carol Todd on Bill C-13: "What Happened to Democracy?"* <http://www.michaelgeist.ca/2014/11/carol-todd-bill-c-13-happened-democracy/> accessed 16 March 2015

Handa, Birbilas and Di Fazio 2015 <http://www.blakes.com/English/Resources/Bulletins/Pages/Details.aspx?BulletinID=2057>

Handa S, Birbilas L and Di Fazio J 2015 *Bill C-13: Cyberbullying Bill Introduces New Lawful Access Measures* <http://www.blakes.com/English/Resources/Bulletins/Pages/Details.aspx?BulletinID=2057> accessed 4 April 2015

Hinduja and Patchin Date Unknown http://www.cyberbullying.us/cyberbullying_and_suicide_research_fact_sheet.pdf

Hinduja S and Patchin JW Date Unknown *Cyberbullying Research Summary: Cyberbullying and Suicide* http://www.cyberbullying.us/cyberbullying_and_suicide_research_fact_sheet.pdf accessed 17 March 2015

Hinduja and Patchin Date Unknown http://cyberbullying.us/Cyberbullying_Identification_Prevention_Response.pdf

Hinduja S and Patchin JW Date Unknown *Cyberbullying: Identification, Prevention, Response* http://cyberbullying.us/Cyberbullying_Identification_Prevention_Response.pdf accessed 17 March 2015

Hummingbird Education Date Unknown <https://www.hummingbirdza.com/cyberbullying-advice-victims/>

Hummingbird Education Date Unknown *Cyberbullying: Advice for the Victims Part 2 – What Do You Do if Your Child or a Learner in Your School is the Victim of Cyberbullying?* <https://www.hummingbirdza.com/cyberbullying-advice-victims/> accessed 23 March 2015

Leishman 2005 <http://www.njbullying.org/CBCNewsIndepthBullying.htm>

Leishman J 2005 *Cyber-bullying* <http://www.njbullying.org/CBCNewsIndepthBullying.htm> accessed 17 March 2015

Lubao 2013 <http://www.globalresearch.ca/canadian-conservatives-cyber-bullying-bill-a-pretext-for-expanding-police-surveillance/5361042>

Lubao D 2013 *Canadian Conservatives' Cyber-bullying Bill: A Pretext for Expanding Police Surveillance* <http://www.globalresearch.ca/canadian-conservatives-cyber-bullying-bill-a-pretext-for-expanding-police-surveillance/5361042> accessed 3 March 2015

Mas 2014 <http://www.cbc.ca/m/touch/canada/story/1.2670736>

Mas S 2014 *Daniel Therrien Grilled on Views About Police Powers in Cyberbullying Bill* <http://www.cbc.ca/m/touch/canada/story/1.2670736> accessed 17 February 2015

Meissner 2013 <http://www.ctvnews.ca/canada/amanda-todd-s-legacy-a-look-at-canada-s-anti-bullying-efforts-a-year-after-her-death-1.1490889>

Meissner D 2013 *Amanda Todd's Legacy: A Look at Canada's Anti-bullying Efforts a Year After Her Death* <http://www.ctvnews.ca/canada/amanda-todd-s-legacy-a-look-at-canada-s-anti-bullying-efforts-a-year-after-her-death-1.1490889> accessed 18 March 2015

Nguyen and Tepper 2014 http://www.thestar.com/news/gta/2014/04/17/amanda_todd_man_arrested_in_netherlands_in_connection_with_canadians_online_bullying.html

- Nguyen A and Tepper S 2014 *Amanda Todd: Man Arrested In Netherlands In Canadian's Online Bullying* http://www.thestar.com/news/gta/2014/04/17/amanda_todd_man_arrested_in_netherlands_in_connection_with_canadians_online_bullying.html accessed 18 March 2015
- Payton 2014 <http://www.cbc.ca/news/politics/cyberbullying-bill-inches-closer-to-law-despite-privacy-concerns-1.2795219>
- Payton L 2014 *Cyberbullying Bill Inches Closer to Law Despite Privacy Concerns* <http://www.cbc.ca/news/politics/cyberbullying-bill-inches-closer-to-law-despite-privacy-concerns-1.2795219> accessed 3 March 2015
- Payton 2014 <http://www.cbc.ca/news/politics/cyberbullying-bill-raises-alarm-for-privacy-commissioner-1.2842034>
- Payton L 2014 *Cyberbullying Bill Raises Alarm for Privacy Commissioner* <http://www.cbc.ca/news/politics/cyberbullying-bill-raises-alarm-for-privacy-commissioner-1.2842034> accessed 16 March 2015
- Puzic 2015 <http://www.ctvnews.ca/politics/anti-cyberbullying-law-bill-c-13-now-ineffect-1.2270460>
- Puzic S 2015 *Anti-cyberbullying Law, Bill C-13, Now in Effect* <http://www.ctvnews.ca/politics/anti-cyberbullying-law-bill-c-13-now-ineffect-1.2270460> accessed 4 April 2015
- Rojas 2011 <http://articles.latimes.com/2011/mar/27/local/la-me-college-speech-20110327>
- Rojas R 2011 *When Students' Controversial Words Go Viral, What is the University's Role?* <http://articles.latimes.com/2011/mar/27/local/la-me-college-speech-20110327> accessed 17 March 2015
- Rondganger 2012 <http://www.iol.co.za/dailynews/opinion/cyberbullying-a-cause-for-concern-1.1261733#.VTSdBJP06Kg>
- Rondganger L 2012 *Cyberbullying a Cause for Concern* <http://www.iol.co.za/dailynews/opinion/cyberbullying-a-cause-for-concern-1.1261733#.VTSdBJP06Kg> accessed 26 February 2015

- Starks 2010 <http://www.yalelawjournal.org/forum/tinkers-tenure-in-the-school-setting-the-case-for-applying-obrien-to-content-neutral-regulations>
- Starks GA 2010 *Tinker's Tenure in the School Setting: The Case for Applying O'Brien to Content-neutral Regulations* <http://www.yalelawjournal.org/forum/tinkers-tenure-in-the-school-setting-the-case-for-applying-obrien-to-content-neutral-regulations> accessed 18 March 2015
- Taran 2011 http://www.huffingtonpost.com/randy-taran/cyberbullying-10-ways-to-_b_807005.html
- Taran R 2011 *Cyberbullying: Strategies to Take Back Power* http://www.huffingtonpost.com/randy-taran/cyberbullying-10-ways-to-_b_807005.html accessed 17 March 2015
- Thalen 2015 <http://www.infowars.com/new-cyberbullying-law-will-force-illinois-students-to-give-up-social-media-passwords/>
- Thalen M 2015 *New "Cyberbullying" Law Will Force Illinois Students to Give Up Social Media Passwords* <http://www.infowars.com/new-cyberbullying-law-will-force-illinois-students-to-give-up-social-media-passwords/> accessed 2 April 2015

LIST OF ABBREVIATIONS

Am U L Rev	American University Law Review
Cardozo L Rev	Cardozo Law Review
CARSA	Child Abuse Research in South Africa
CBA	Canadian Bar Association
Comput Hum Behav	Computers in Human Behavior
CRC	Convention on the Rights of the Child
IP	Internet Protocol
ISP	Internet Service Provider
J Yourh Adolesc	Journal of Youth and Adolescence
JLIS	Journal of Law, Information and Science
Miss LJ	Mississippi Law Journal

PIPEDA	Personal Information Protection and Electronic Documents Act
SACJ	South African Journal of Criminal Justice
SAJE	South African Journal of Education
Scand J Psychol	Scandinavian Journal of Psychology