Sticks and stones may break my bones, but cyberbullying is illegal – Is cyberbullying a crime, and should it be?

Rosa McPhee

A dissertation submitted in partial fulfilment of the requirements for the degree of Bachelor of Laws (Honours) at the University of Otago.

October 2014

Table of Contents

Acknowledgements

To my supervisor, Geoff Hall, for your invaluable encouragement, guidance and advice throughout the year.

To my friends and flatmates over the last five years for keeping me motivated, your patience, and your proof reading and formatting skills.

Most importantly to Mum, Dad, Elena and Holly, for your unconditional love and support.

Introduction

> Increasingly victims of cyberbullying are turning to law, both civil and criminal, as a means of addressing the power imbalance between them and their bullies or at least obtaining some form of vindication. While this might seem an extreme response to conduct that might be considered by some to be trivial or 'just a joke', the potential harm that victims may suffer makes the effectiveness of the various laws that may be called into play worthy of scrutiny.[1]

Extensive media coverage of the harm cyberbullying can cause to vulnerable people has made it one of the most visible negative consequences of our increasing use of technology. While bullying in its traditional forms continues to exist, cyberbullying has adapted to and is shaped by the presence of digital communications technologies in our lives.

The challenges for the law posed by cyberbullying include demand from the public for safety online, the need to protect freedom of speech and opposition from service providers to increased regulation. In light of this, it is timely to consider what cyberbullying is and whether our current laws already render it illegal. If there are gaps in our current law, we must determine how effectively the Harmful Digital Communications Bill 2013 (168-1) (HDC Bill) fills them, and what the consequences of the Bill could be. Finally, we must assess whether the criminalisation and regulation of cyberbullying is necessary and desirable in the long term. This requires considering the consequences of enacting the Bill as it is currently drafted, and comparing the scheme proposed in the Bill to alternative approaches to this problem taken by other countries.

In considering these points, this dissertation will examine the adequacy of our current laws, analyse the HDC Bill and compare New Zealand's approach to the

[1] Des Butler, Sally Kift and Marilyn Campbell "Cyber Bullying In Schools and the Law: Is There an Effective Means of Addressing the Power Imbalance?" (2009) 16(1) Murdoch University Electronic Journal of Law 84 at 85.

regulation of harmful communication with that of the UK and Australia. Finally, this research will consider the role of self-regulation and education in addressing bullying, ask whether the HDC Bill should be confined to cyberbullying, and suggest changes to the proposed scheme.

A. Outline of the Harmful Digital Communications Bill

The Bill would create a three-tiered system to deal with the issue of harmful digital communications, which are the key component of cyberbullying. At the lowest level, the Bill would establish an Approved Agency that would be the 'go-to' source for advice and mediation in disputes over allegedly harmful digital communications. The second stage of regulation would grant the District Court new powers to make orders that harmful digital content be removed, anonymous authors be identified, corrections be published or that a right of reply be given to the target of a harmful digital communication. Finally, the Bill would create a new criminal offence designed to combat harmful digital communications, punishable by a fine or a period of imprisonment. The Bill also proposes alterations to other Acts, including the Crimes Act 1961, Harassment Act 1997 and Privacy Act 1993, to ensure that they can adequately respond to the challenges posed by digital communications.

Chapter one: Background to the issue of cyberbullying

A. What is cyberbullying?

Traditional bullying involving overt or covert verbal, relational and physical aggression has been the subject of social commentary for a long time. Most of this discussion has focused on bullying between children and young people, however recent research has shown that bullying among adults in the workplace can also have serious consequences.[2] There is currently no academic consensus on what behaviour constitutes cyberbullying. Media representations of cyberbullying have focused on interactions between young people using mobile phones and the Internet, highlighting cases where cyberbullying has been a factor in suicides or self-harm.[3] This has contributed to a popular perception that cyberbullying occurs solely among young people and is more serious than traditional face-to-face bullying, a perception supported by the lack of adult knowledge about the means through which cyberbullying occurs.[4] However, academics like Campbell contend that cyberbullying is merely a new form of traditional bullying that has adapted to new technologies.[5]

Supporting the characterisation of cyberbullying as an old problem in a new form is the fact that when compared, both traditional bullying and cyberbullying involve an intention to harm the target, an imbalance of power, repetition or a threat of further aggression and the inability of the target to defend themselves.[6] While normally the imbalance of power lies in the bully's physical strength or social status, in a cyberbullying situation "the very act of bullying" creates an imbalance of power, as does the anonymity offered to bullies online.[7] This is

---

[2] See Carmel Privitera and Marilyn Anne Campbell "Cyberbullying: The New Face of Workplace Bullying" (2009) 12(4) CyberPsychology & Behaviour 395 at 395.
[3] The Nova Scotia Task Force on Bullying and Cyberbullying *Respectful and Responsible Relationships: There's No App for That. The Report of the Nova Scotia Task Force on Bullying and Cyberbullying* (February 29 2012) at 10.
[4] At 91-92.
[5] Marilyn A Campbell "Cyberbullying: An Old Problem in a New Guise?" (2005) 15(1) Australian Journal of Guidance and Counselling 68 at 69.
[6] Butler, Kift and Campbell, above n 1, at 85.
[7] At 85.

particularly evident when cyberbullying occurs on websites premised on anonymity, like Ask.fm.[8]

Digital communications can involve repetition in both the traditional form of a series of repeated communications, but also in the sense of the digital longevity of communications.[9] One harmful comment on a social networking site like Facebook can be viewed by hundreds of other people, who may 'like' or 'share' the comment, maintaining it in the public view and causing the same harm to the target as traditional repetition. The HDC Bill recognises the problems caused by digital longevity, proposing an amendment to the Harassment Act to reflect the fact that a communication can be 'ongoing.'[10]

As well as these similarities, cyberbullying poses unique problems not present in offline bullying incidents. In addition to the problems of longevity and anonymity, the global reach of the Internet means that digital communications have a much larger potential geographic scope than non-digital communications. Combined with the speed with which digital communications travel, this creates significantly larger audiences for cyberbullying incidents, increasing the likelihood of harm to the target.

Cyberbullying is primarily conducted over the Internet or on mobile phones. Fenaughty's 2013 study of cyberbullying in New Zealand schools found that of the two methods cyberbullying on mobile phones was slightly more common, with 24.5 per cent of his sample reporting that they had been bullied on mobile phones at least once in the past year, and 17.5 per cent reporting being bullied on the Internet.[11] However as more mobile phones allow users to access the

[8] Ask.fm is a social media site that allows users to post anonymous questions on the profiles of other members.
[9] See Sally Adams "Cyberbullying: An emerging form of student aggression for the 'always-on' generation" (2007) 2 The Australian Educational Leader 16 at 17. See also Robert Slonje, Peter K. Smith and Ann Frisén "The nature of cyberbullying, and strategies for prevention" (2013) 29 Computers in Human Behaviour 26 at 27.
[10] Harmful Digital Communications Bill 2013 (168-1) [HDC Bill], cl 26.
[11] John Fenaughty, "Challenging Risk: NZ High-school Students' Activity, Challenge, Distress, and Resiliency, within Cyberspace" (PhD Thesis, University of Auckland, 2010) at 150-151.

Internet and online messaging services, the distinction between the two becomes blurred. Cyberbullying can take different forms, including flaming (deliberate, hostile insults), online harassment, cyberstalking, denigration, masquerade, outing and exclusion. The content of cyberbullying messages can include threats, abuse, name calling, death threats, the ending of friendships or relationships, demands, humiliation and rumours.[12]

B. A definition of cyberbullying

As mentioned above, there is no accepted definition of cyberbullying, which prevents accurate comparisons between different studies.[13] NetSafe defines cyberbullying as "using the Internet, a mobile phone or other technology like a digital camera to hurt somebody, harass or embarrass them."[14] While this definition is easy to understand, it does not identify the element of repetition that distinguishes bullying from an isolated incident. Tokunaga defines cyberbullying as "any behaviour performed through electronic or digital media by individuals or groups that repeatedly communicates hostile or aggressive messages intended to inflict harm or discomfort on others". This definition captures the need for repetition and intention, but the wide scope of "any behaviour" and the low threshold of "discomfort" could capture irrelevant material, such as repetitive adverts intended to cause discomfort to their viewers.

This dissertation will define 'cyberbullying' as the repeated or continuing use of digital communication technologies to intentionally cause harm to others, or where the perpetrator knows such harm will result. This definition includes the

---

[12] Slonje, Smith and Frisén, above n 9, at 27-28.
[13] Robert S. Tokunaga "Following you home from school: A critical review and synthesis of research on cyberbullying victimization" (2010) 26 Computers in Human Behaviour 277 at 278.
[14] NetSafe "I am being cyberbullied what can I do?" <www.netsafe.org.nz>. NetSafe is a non-profit organisation that advises people about safe behaviour on the Internet. NetSafe is discussed in more detail in Chapters Two and Three.

elements of repetition, intention and the use of communication technologies, and requires harm rather than mere discomfort to be caused.[15]

C. How common is cyberbullying in New Zealand?

Fenaughty defines cyberbullying as "intentional acts of interpersonal aggression involving one or more people in cyberspace."[16] Applying this definition, Fenaughty found that of his 1665 participants, 34.8 per cent of 12-14 year old girls and 36.9 per cent of 15-19 year old girls had been targeted by Internet and mobile cyberbullying at least once in the prior year, compared to 31.2 per cent of 12-14 year old boys and 27.2 per cent of 15-19 year old boys.[17] These percentages can be compared with the percentage of respondents reporting *frequent* experiences as targets of cyberbullying on the Internet and via mobile phones in the prior year: 2.4 per cent of 12-14 year old girls, 2.1 per cent of 15-19 year old girls, 6.8 per cent of 12-14 year old boys and 5.7 per cent of 15-19 year old boys.[18] Of the students who reported any experience of cyberbullying in the prior year, frequent or infrequent, 52.9 per cent reported that it caused them distress.[19] From these figures, it appears that between 10-20 per cent of New Zealand school students are experiencing distressing cyberbullying. The exact incidence of cyberbullying is difficult to determine, partly because young people often do not report cyberbullying to adults, and partly because there is no official, national record of cyberbullying incidents kept by schools or the Ministry of Education.[20]

---

[15] For 'bullying' to occur, harm must necessarily be caused to the target. However this can be distinguished from the discussion of the appropriateness of the requirement in the HDC Bill's provisions that actual harm be suffered, discussed in Chapter Three.
[16] Fenaughty, above n 11, at 87.
[17] At 148.
[18] At 149.
[19] At 152.
[20] See Barbara Spears and others *Research on youth exposure to, and management of, cyberbullying incidents in Australia. Part C: An evidence-based assessment of deterrents to youth cyberbullying - Appendix A (SPRC report 12/2014)* (Australian Government Department of Communications, June 2014) at 47.

Cyberbullying also occurs among adults. Half of the 60-80 complaints NetSafe receives every month relating to aggressive, threatening, intimidating or bullying online behaviours are from adults "often, although not exclusively … in their professional lives."[21] It also appears that 'digital natives' (young people who have grown up with widespread digital communication) take their patterns of behaviour, including cyberbullying behaviour, with them into the workforce.[22] In an American study of bullying in the workplace, 34 per cent of participants were targets of bullying behaviour in the form of face-to-face victimisation, email and telephone.[23]

Although there is a common perception that bullying in New Zealand is increasing, any change is difficult to measure due to the changing definitions of the terms 'bullying' and 'violence.' Sally Boyd suggests that our definition of bullying has changed mirroring a change in our attitudes towards violence, especially violence towards children.[24] Boyd found that:[25]

> … perceptions of bullying are changing from it being viewed as an 'almost inevitable' part of growing up to be increasingly unacceptable… and there is an increasing understanding that bullying is a violation of an individual's human rights.

D. Who are the cyberbullies?

While the negative impact of cyberbullying is obvious, it is sometimes difficult to draw a clear line between bullies and targets, both in relation to their roles and

---

[21] NetSafe "Submission to the Justice and Electoral Select Committee on the Harmful Digital Communications Bill 2013" at 8.
[22] Butler, Kift and Campbell, above n 1, at 84.
[23] Privitera and Campbell, above n 2, at 397.
[24] Sally Boyd *"Wellbeing@School: Building a safe and caring school climate that deters bullying. Overview paper"* (2012) New Zealand Council for Educational Research at 17. An example of society's changing attitude towards violence against children is the recent 'anti-smacking' law, the Crimes (Substituted Section 59) Amendment Act 2007, which removed the defence of "reasonable force" for parents prosecuted for assaulting their children.
[25] At 18.

the distress they experience.[26] Illustrating this point, Fenaughty has found that targets are more likely to report cyberbullying others than non-targets.[27] Similarly, NetSafe has observed that the majority of cases they are alerted to concern parties who are "closely connected in some way, familial, peer group, romantic or professional," and involve an element of reciprocity meaning that the "the roles of victim and defendant may not be easily delineated."[28]

Of the participants in Fenaughty's survey, 16.1 per cent of 12-14 year old girls and 16.6 per cent of 15-19 year old girls were 'producers' of cyberbullying on the Internet and/or on mobile phones at least once in the prior year, compared to 18.6 per cent of 12-14 year old boys and 15.9 per cent of 15-19 year old boys.[29] This can be compared to the percentages of respondents who reported being the 'producers' of *frequent* cyberbullying in the prior year: 0.9 per cent of 12-14 year old girls, 0.5 per cent of 15-19 year old girls, 3.5 per cent of 12-14 year old boys and 3.9 per cent of 15-19 year old boys.[30]

These statistics indicate that 12-14 year old males are the most likely to be perpetrators of cyberbullying in one off incidents, and boys in general are more likely to be the perpetrators of frequent cyberbullying, with little variation between 12-14 year old boys and older 15-19 year old boys. In contrast, the percentage of girls involved in frequent cyberbullying almost halves between the 12-14 year old age group and the 15-19 year old group.

Even when bullies can be identified, research shows that they, as well as their victims, are often in need of help. Fenaughty notes that "young people who self-reported harassing others in cyberspace were significantly more likely to report aggression and rule breaking problems … than those who did not."[31] A study from the Netherlands has found that boys who bully others were almost four times more likely to experience suicidal thoughts, while girls who bullied others

[26] NetSafe "Submission", above n 21, at 10.
[27] Fenaughty, above n 11, at 94.
[28] NetSafe "Submission", above n 21, at 10.
[29] Fenaughty, above n 11, at 148.
[30] At 149.
[31] At 94.

were eight times more likely.[32] Students who reported bullying others also reported "higher levels of school loneliness" and lack of school connectedness compared to those who did not.[33] The relationship between the distress reported by cyberbullies and their bullying behaviours is unclear, but these findings indicate that this relationship needs investigation. If factors like loneliness, lack of school connectedness and aggression are found to be a cause of bullying behaviours, then they need to be addressed before bullying and cyberbullying can be reduced or eradicated. An anti-bullying education campaign that addresses the causes and consequences of bullying could aid both bullies and their targets.

E. The impact of cyberbullying on society

In the New Zealand Bill of Rights Act 1990, all New Zealanders have the right not to be subjected to torture or cruel treatment, the rights to freedom of expression, thought, conscience and religion and the right to be free from discrimination.[34] In 1993 New Zealand ratified the United Nations Convention on the Rights of the Child, which asserts the rights of children to freedom of expression, safety, health, education and dignity.[35] Bullying and cyberbullying behaviours can infringe these rights by discouraging freedom of expression, thought, conscience and religion, unfairly discriminating against people, affecting the ability of children to learn, having detrimental effects on the mental and physical health of targets and causing people to fear for their safety. The physical consequences of bullying can include "suicidal ideation, eating disorders, and chronic illness",[36] as well as "poor health … a range of psychological, psychosomatic and behavioural problems including anxiety and insecurity, low self esteem, … sleeping

[32] Sameer Hinduja and Justin W. Patchin "Bullying, Cyberbullying and Suicide" (2010) 14(3) Archives of Suicide Research 206 at 209.
[33] Fenaughty, above n 11, at 94.
[34] New Zealand Bill Of Rights Act 1990, ss 9, 13, 14, 19.
[35] United Nations Convention on the Rights of the Child (opened for signature 20 November 1989, entered into force 2 September 1990), arts 13, 19, 24, 28.
[36] Justin W. Patchin and Sameer Hinduja "Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying" (2006) 4 Youth Violence and Juvenile Justice 148 at 151.

difficulties, bed wetting, feelings of sadness, frequent headaches and abdominal pain and considerable mental health problems."[37]

It has been argued that the negative consequences of cyberbullying could be more severe than the consequences of traditional bullying.[38] This is often argued in relation to young people, who are less able to perceive risks than adults, and therefore more likely to engage in unsafe digital behaviours.[39] However while school behaviour problems like skipping school, detentions and suspensions are more frequently reported by youth who are harassed online than those that are not,[40] the claim that cyberbullying causes more serious distress than traditional bullying is hard to substantiate as cyberbullying and traditional bullying often occur simultaneously.[41]

A form of negative behaviour frequently associated with cyberbullying is suicide, and there have been a number of high profile instances of suicide following a period of cyberbullying in New Zealand and around the world. In 2006, 13-year-old Megan Meier committed suicide after being cyberbullied by Lori Drew, the mother of one of Megan's friends. Drew used the anonymity of social media to pretend to be a teenage boy interested in Megan, and used the information she gained to humiliate Megan, encouraging her to commit suicide.[42] In New Zealand, 12-year-old Alex Teka committed suicide following an "orchestrated campaign" of email and text bullying,[43] and many people attributed the suicide of Charlotte

---

[37] Carolyn Coggan and others "Association between Bullying and Mental Health Status in New Zealand Adolescents" (2003) 5(1) International Journal of Mental Health Promotion 16 at 16.
[38] Butler, Kift and Campbell, above n 1, at 87.
[39] The Prime Minister's Chief Science Advisor *Improving the Transition: Reducing Social and Psychological Morbidity During Adolescence* (Office of the Prime Minister's Science Advisory Committee, May 2011) at 124.
[40] Michele L. Ybarra, Marie Diener-West and Philip J. Leaf "Examining the Overlap in Internet Harassment and School Bullying: Implications for School Intervention (2007) 41 Journal of Adolescent Health s42 at s46.
[41] Fenaughty, above n 11, at 189. See further discussion in Chapter Four at 55-56.
[42] Tokunaga, above n 13, at 277.
[43] Simon O'Rourke "Teenage bullies hound 12-year-old to death" *New Zealand Herald* (online ed, Auckland, 11 March 2006).

Dawson (a New Zealand model and television celebrity) to the cyberbullying she had experienced over Twitter and Facebook.[44]

While New Zealand's high youth suicide rate makes the possible relationship between cyberbullying and suicidal ideation important,[45] Fenaughty emphasises that not all instances of cyberbullying lead to distress.[46] Headlines like "Teenage bullies hound 12 year old to death" create a distorted view of the consequences of cyberbullying, which is often only one of a number of factors in a suicide, including "offline mistreatment, emotional and psychological problems, academic difficulties," and inadequate support structures.[47] The media's focus on suicide is also troubling because exposure to news items on suicide contributes to suicidal behaviour.[48] Finally, denouncing the actions of cyberbullies as the sole cause of their target committing suicide may discourage cyberbullies from seeking help themselves.[49]

i. Impact on the workplace

Workplace bullying results in negative consequences for employees, the employer and the workplace as a whole. The increased stress caused by bullying can harm the target's health, emotional wellbeing and relationships.[50] Bullying can also lead to increased absenteeism, "negative impacts on efficiency, productivity and profitability, high staff turnover and damage to the reputation of the workplace as it becomes known as a difficult place to work."[51] These impacts warrant further research into the prevalence of workplace bullying in New Zealand, and indicate the need for further education for employers and employees about how to prevent and address workplace bullying.

---

[44] "Charlotte Dawson found dead" (22 February 2014) Stuff <www.stuff.co.nz>.
[45] Coggan and others, above n 37, at 17.
[46] Fenaughty, above n 11, at 152. Fenaughty reports that 52.9 per cent of children who experience cyberbullying over the Internet and/or mobile phones suffer distress.
[47] Hinduja and Patchin, above n 32, at 208. See headline at n 43.
[48] Russell A. Sabella, Justin W. Patchin and Sameer Hinduja "Cyberbullying myths and realities" (2013) 29 Computers in Human Behaviour 2703 at 2705.
[49] Hinduja and Patchin, above n 32, at 209.
[50] Privitera and Campbell, above n 2, at 395.
[51] At 396.

F. Conclusion

Cyberbullying is a real problem in New Zealand society. It can have serious consequences on the health of targets, including becoming a factor in suicide, and has also been connected to distress among bullies. New Zealand's changing attitude towards violence, combined with the increasing importance of digital communication technologies in our lives, has led to calls for a legal solution to the problem of cyberbullying. This prompts the need to re-examine our current laws and assess the value of the proposed HDC Bill.

Chapter two: How does New Zealand currently address cyberbullying?

A. Introduction

Society's attitude towards bullying is influenced by the location where the bullying takes place, and the age of those involved. Bullying amongst adults in the workforce is considered an employment issue to be dealt with through the personal grievance process. In wider society, the Harassment Act and other torts provide protection against some bullying behaviours, as does the criminal law. New Zealand's obligations, rights and responsibilities towards young people who are the targets or perpetrators of bullying are implemented through many extra- or quasi- legal attempts to address the issue of bullying while avoiding the involvement of the criminal law.

B. Non legislative approaches

i. Responses to bullying within schools

While bullying outside school hours is considered the responsibility of parents, this responsibility is transferred to teachers during the school day. Under National Administration Guideline 5 (NAG 5) Boards of Trustees are required to provide a safe physical and emotional environment for their students and to comply with any legislation designed to ensure student safety.[52] The Bullying Prevention and Response guidelines recommend that schools meet this obligation by developing and implementing a bullying policy, but this is not a mandatory requirement.[53]

Other relevant legislation includes ss 60A and 77 Education Act 1989, which require principals to provide students with guidance and counselling, and to

[52] The Ministry of Education provides guidance to Boards of Trustees through National Administration Guidelines, issued under the Education Act 1989, s 60A.
[53] Bullying Prevention Advisory Group "Bullying prevention and response: A guide for schools" (Ministry of Education, 2014) at 31.

inform parents of matters affecting the student's progress or relationships at school. Under the Health and Safety in Employment Act 1992 schools have a duty to minimise bullying, which can be considered a care and protection issue or a criminal matter under the Children, Young Persons and Their Families Act 1989.[54]

The key Ministry of Education programme designed to address bullying in schools is Positive Behaviour for Learning (PB4L).[55] PB4L views bullying as a socio-ecological phenomenon involving multiple risk and protective factors, and is designed to create a positive school atmosphere.[56] PB4L provides schools with a behaviour crisis response unit for extreme events and an intensive wraparound service that supports children with challenging behavioural, social and educational needs.[57]

However the ability of cyberbullying to happen anywhere at anytime limits the impact of these guidelines and programmes and challenges the traditional division of adult responsibility between the realms of 'home' and 'school'. The Bullying Prevention and Response guidelines acknowledge this, saying that "the very notion of behaviour that occurs 'outside school' is becoming irrelevant due to the ubiquity of technology."[58] Because of the way in which cyberbullying transcends these boundaries, teachers feel that society has "potentially unrealistic" expectations about the ability of schools to tackle bullying alone. Instead, teachers consider that the responsibility for addressing and responding to cyberbullying "should be shared between children's home and school lives."[59] The line-crossing nature of cyberbullying makes it all the more important that the creation of anti-bullying policies becomes mandatory, and also indicates

---

[54] *Submission by the New Zealand Human Rights Commission: Consideration of New Zealand's third periodic report on the implementation of the International Covenant on Economic, Social and Cultural Rights* (New Zealand Human Rights, March 2012) at 7.
[55] Ministry of Education "Positive behaviour for learning" <www.pb4l.tki.org.nz>.
[56] Ministry of Education "Understanding bullying behaviours" <www.pb4l.tki.org.nz>.
[57] Ministry of Education "Programmes and initiatives" <www.pb4l.tki.org.nz>.
[58] Bullying Prevention Advisory Group, above n 53, at 42.
[59] Vanessa A. Green and others, "Bullying in New Zealand Schools: A Final Report" (Victoria University of Wellington, 2013) at 10, 12.

education programmes need to inform parents about their role in preventing and addressing bullying, which is no longer confined to the school grounds.

ii. NetSafe

Alongside measures taken by schools, the non-profit organisation NetSafe aims to help people use the Internet safely. NetSafe is a "multi-partnership which represents a range of perspectives from New Zealand's cybersafety community." NetSafe coordinates relationships with the government, the education sector, industry, parents and the legal community to "promote cybersafety and champion digital citizenship by educating and supporting individuals, organisations and industry".[60]

NetSafe's website offers advice to young people, parents and teachers on how to recognise and prevent cyberbullying and how to support victims of cyberbullying. Members of the public can make complaints to NetSafe about cyberbullying or other Internet harms, and NetSafe uses its connections, influence and expertise to help to resolve them.[61]

C. Civil law

i. Harassment

The Harassment Act regulates both civil and criminal harassment. However because the Act was drafted to deal with harassment in the non-digital world it is not well adapted to respond to cyberbullying. Criminal harassment requires intent to cause the target to fear for their safety, or knowledge that such fear will be caused.[62] Where this intent or level of knowledge is absent, the court may

[60] NetSafe "About NetSafe" <www.netsafe.org.nz>.
[61] NetSafe "Submission", above n 21, at 8.
[62] *R v D* [2000] 2 NZLR 641 (CA) at [12]. Harassment Act 1997, s 8: Criminal harassment occurs when one person (A) harasses another (B), when A intended that harassment to cause B to fear for their safety or the safety of any person in B's family; or where A knows that the harassment is likely to cause B to reasonably fear for their own safety or the safety of someone in B's family. A conviction for criminal harassment carries a maximum sentence of two years imprisonment.

issue a civil restraining order if it is satisfied that the respondent "has harassed, or is harassing, the applicant."[63]

Although minors can apply for orders (through a representative if they are under 17), there are some significant barriers preventing the use of the Harassment Act as a tool to deter cyberbullying.[64] Courts cannot issue a restraining order "against a minor under the age of 17 years" unless that minor is or has been married, in a civil union or de facto relationship.[65] Restraining orders also cannot be made against someone who the applicant has been in a relationship with, preventing them being used to deter cyberbullying by ex-partners.[66]

Another major hurdle to the use of the Harassment Act in cyberbullying situations is the Act's definition of 'harassment,' which requires "doing any specified act" to a person on at least two occasions within 12 months.[67] The specified acts do not specifically address digital communications. The three most relevant to a cyberbullying situation are:[68]

(d) making contact with that person (whether by telephone, correspondence, or in any other way):
(e) giving offensive material to that person, or leaving it where it will be found by, given to, or brought to the attention of, that person:
(f) acting in any other way—
    (i) that causes that person (person A) to fear for his or her safety; and
    (ii) that would cause a reasonable person in person A's particular circumstances to fear for his or her safety.

In *Brown v Sperling*, these specified acts were considered in relation to blog posts. Illustrating the uncomfortable fit of the acts to digital communications, Judge Harvey found that publishing on a blog could only fall under s 4(1)(e) if the

[63] Section 16. This is subject to a defence of lawful purpose in s 17 of the Act.
[64] Section 11(2).
[65] Section 12.
[66] Section 9(4). This is intended to encourage former parties to a relationship to utilise domestic violence legislation instead: Section 6(2)(b).
[67] Section 3(1).
[68] Section 4(1).

author knew that the target visited the blog and the communication would come to their attention.[69]

The requirement that the specified act occur at least twice in 12 months is also ill suited to the features of digital communications. In *MJF v Sperling*, where the two acts occurred outside the 12 month timeframe, Judge Harvey circumvented this time limit, holding that by 'revitalising' her blog (which *Brown v Sperling* ordered she take down) and making previous posts available again,[70] Ms Sperling had "wound the clock back" allowing the republication of the original comments to be viewed as occurring within the time limit.[71]

The Bill does not adopt Judge Harvey's 'revitalisation' theory, but creates a new s 3(3) stating that harassment occurs if a person does "any specified act to the other person that is one continuing act carried out over any period."[72] This is more effective than Judge Harvey's 'revitalisation' idea, as the Judge did not address the problem posed by the longevity of digital communications which can be posted once and remain online, having the same effect as traditional repetition but not satisfying the elements of the Act. The Bill also creates a specified act designed for digital communications, s 4(1)(ea): "giving offensive material to a person by placing the material in any electronic media where it is likely that it will be seen by or brought to the attention of, that person".[73] This recognises that online communication is often not person-to-person, but rather involves posts to locations where the intended audience is likely to view them.

ii. Privacy

An individual's privacy may be infringed when cyberbullying involves the unauthorised publication of private facts online.

<u>The Privacy Act</u>

---

[69] *Brown v Sperling* [2012] DCR 753 (DC) at [74]. As Ms Sperling had reason to believe Ms Brown read her site, the elements of s 4(1)(e) were met: at [78-79].
[70] *MJF v Sperling* [2013] NZFLR 715 at [8].
[71] At [26]
[72] HDC Bill, cl 26.
[73] Clause 27(2).

The Privacy Act operates around a series of privacy principles, set out in s 6 of the Act, relating to the collection, storage, security, access, retention and disclosure of personal information by "agencies."[74] When information is held by a private agency, s 67 of the Act states "any person may make a complaint to the Commissioner" regarding an interference with their privacy, including breaches of the privacy principles.[75] There is no age requirement to make a complaint, and an adult can complain on behalf of a child.[76]

The Privacy Act's applicability to cyberbullying is currently limited by the exceptions to the application of the Act. Section 56 states that the principles do not apply to personal information "collected or held by an individual solely or principally for the purposes of, or in connection with, that individual's personal, family or household affairs." This could prevent the victims of 'revenge porn' from controlling the ways in which their ex-partners use their private images.[77] Where information is located in a "publically available publication," principles 10(a) and 11(b) contain exceptions to the rules that information obtained for one purpose should not be used for another and that information should not be disclosed to third parties. The definition of "publically available publication" in s 2 is likely to include information published on websites, preventing liability for sharing or reposting online content.[78] The HDC Bill amends these sections to ensure the applicability of the Act to digital communications. Clause 35 of the Bill limits the exceptions in principles 10(a) and 11(b) to situations where using or disclosing the information would not be unfair or unreasonable. Clause 36

[74] Privacy Act 1993, s 2 states that "agencies" include "any person or body of persons."
[75] Section 66(1)(a).
[76] Section 67(1).
[77] 'Revenge porn' is the malicious publication of naked or otherwise compromising pictures taken of an ex-partner during the relationship, which were intended for private use. As opposed to other breaches of privacy, the pictures used in revenge porn are initially taken with the consent of the subject rather than covertly. See Myles Hume "Explicit page done 'out of respect'" *The Press* (online ed, Christchurch, 8 October 2014).
[78] Section 2: "publically available publication means a magazine, books, newspaper, or other publication that is or will be generally available to members of the public". See discussion of the application of the exceptions to the Privacy Act in: Paul Roth "Data Protection Meets Web 2.0: Two Ships Passing in the Night" (2010) 33(2) UNSW Law Journal 532.

amends s 56, stating that the exception "ceases to apply … if that collection, disclosure or use would be highly offensive to an ordinary reasonable person."

Privacy Torts

The tort of breach of privacy could be employed against revenge porn cyberbullying. It requires "(1) the existence of facts in respect of which there is a reasonable expectation of privacy and (2) publicity given to those private facts that would be considered highly offensive to an objective reasonable person."[79] *L v G* held that intimate photos are "private facts," and the publication of such pictures would be "highly offensive to an objective reasonable person."[80] When no publication takes place, the tort of intrusion into seclusion may be available.[81] However, like the Crimes Act intimate visual recording sections, *C v Holland* states that the intrusion must be "unauthorised", indicating that the tort will not apply unless the pictures were taken without the subject's consent.[82]

iii. Broadcasting Act 1989

The wide definitions in the Broadcasting Act 1989 of 'broadcasting' and 'programmes' mean it is possible that cyberbullying in the form of videos posted online (as happened to the 'Star Wars Kid' Ghyslain Raza[83]) could come under the jurisdiction of the Act, and be controlled by the Act's standards and complaints procedures.[84] These include observing "good taste and decency," maintaining law and order and respecting the privacy of individuals.[85]

---

[79] *Hosking v Runting* [2005] 1 NZLR 1 (CA) at [117].
[80] *L v G* [2002] DCR 234 (DC) at 25: a man published intimate photographs of a woman in a magazine without her consent, which the court held was a breach of privacy.
[81] *C v Holland* [2012] NZHC 2155, [2012] 3 NZLR 672.
[82] At [94]. In *C v Holland* the video concerned was taped without the subject's knowledge through a camera hidden in a bathroom.
[83] Matthew Manarino "'Star Wars Kid' Ghyslain Raza Breaks 10-Year Silence In New Magazine Interview" (9 May 2013) New Media Rockstars <www.newmediarockstars.com>. A video of Raza imitating Star Wars characters was released online, attracting more than 900 million views. The consequent cyberbullying forced Raza to seek psychiatric treatment.
[84] Broadcasting Act 1989, s 2 defines 'broadcasting' as "the transmission of programmes … by … telecommunication" and 'programmes' as a combination of visuals and sounds intended for entertainment.
[85] Section 4.

However the process for making a complaint about an alleged breach of the broadcasting standards is relatively complicated, subject to time limits and requires a formal written complaint, meaning it is unsuited to the rapid removal of material needed in a cyberbullying context.[86]

iv. Wilkinson v Downton: intentional infliction of emotional distress

The *Wilkinson v Downton* tort of intentional infliction of emotional distress appears to be relevant in situations where a cyberbully causes their target to suffer emotional harm.[87] However, *C v Holland* recently affirmed the House of Lords comment in *Wainright v Home Office* that the tort has "no leading role in the modern law."[88] If the tort were recognised in New Zealand, it is likely that applicants would have to prove harm to the *Wainwright* standard of "recognised psychiatric injury" which would be hard to reach in most cyberbullying cases.[89]

v. Defamation

The Defamation Act 1992 covers all online and offline statements published after 1 February 1993.[90] The plaintiff must prove that the statement is defamatory, that it refers to the plaintiff and that it has been published to a third party.[91] Each repetition of a defamatory statement creates a new cause of action.[92]

Wishart v Murray held that statements made on a Facebook page can be defamatory, and also concluded that if the host of a Facebook page knows of a defamatory statement on their page (or ought to know that the posts are likely to be defamatory) and "fails to remove it in circumstances that give rise to an inference that they are taking responsibility for it", the host can be liable as a

---

[86] Sections 6-9.
[87] *Wilkinson v Downton* [1897] 2 QB 57.
[88] *Wainwright v Home Office* [2003] UKHL 53, [2004] 2 AC 406 at [41] cited in *C v Holland*, above n 81, at [51], [89].
[89] *Wainwright v Home Office* at [47].
[90] *Karam v Parker* [2014] NZHC 737 at [29]. *Karam v Parker* rejected the argument that the 'thrust and parry' nature of Internet communications calls for a different standard than that applied to communications offline, saying that communications on the Internet have the "same capacity for harm."
[91] Defamatory in the sense that it was capable of lowering the applicant in the estimation of right thinking members of society: *Karam v Parker* at [25].
[92] *Simunovich Fisheries Ltd v Television New Zealand Ltd* [2008] NZCA 350 at [94].

publisher.[93] This reasoning was affirmed in *Karam v Parker*, where the court emphasised that a person who "takes part in or contributes to the publication of someone else's statement is, prima facie, liable as a publisher."[94] Courtney J repeated his statement in *Wishart v Murray* that Facebook pages are comparable to notice boards, and that where hosts have "the power to control who can access the site to post material and who can also edit the posts, they cannot, realistically, be regarded as … mere conduits of content."[95]

The same defences of consent, truth, honest opinion or privilege would be available to the maker of a defamatory statement online as they are offline, and search engines (such as Google) may be able to use the defence for innocent processors and distributors in s 21 of the Defamation Act.[96]

vi. Employment law

Under the Health and Safety in Employment Act 1992 (HSE Act), employers are obliged to "take all practicable steps to ensure the safety of employees while at work".[97] This includes "defining hazards and harm in a comprehensive way so that all hazards and harm are covered, including harm caused by work-related stress",[98] which is a common consequence of workplace bullying.[99] The Court of Appeal in *Attorney-General v Gilbert* affirmed that the HSE Act covers stress, as it makes "no distinction between physical, psychiatric or psychological illness or injury."[100] The Court determined that failing to take reasonably practicable steps to avoid psychological harm in the form of stress would be contrary to the purpose of the Act and the employer's duty of trust and confidence.[101]

---

[93] *Wishart v Murray* [2013] NZHC 540, [2013] 3 NZLR 246 at [117].
[94] *Karam v Parker*, above n 90, at [9].
[95] At [12]. The 'notice board' analogy is drawn from *Byrne v Deane* [1937] 1 KB 818 cited in *Wishart v Murray* at [86], and refers to a person's refusal to exercise their power to remove defamatory content once it is brought to their attention, from which responsibility for the content can be inferred.
[96] *Blunt v Tilley* [2006] EWHC 407 (QB), [2007] 1 WLR 1243; *Metropolitan International Schools Ltd v Designtechnica Corporation* [2009] EWHC 1765 (QB), [2011] 1 WLR 1743, cited in *Wishart v Murray* at [84], [107].
[97] Health and Safety in Employment Act 1992, s 6.
[98] Section 5.
[99] Privitera and Campbell, above n 2, at 395.
[100] *Attorney-General v Gilbert* [2002] 2 NZLR 342 (CA) at [72].
[101] At [77].

D. Criminal law

Any discussion of the use of the criminal law to address cyberbullying must take into account the fact that in New Zealand, criminal responsibility is limited by age. No child under the age of 10 can be convicted of an offence, while children aged 10 or older but under the age of 14 can only be held liable if they knew their act or omission was wrong or contrary to law.[102] At a pre-trial level, police do not tend to investigate reports involving young people unless they involve a serious offence.[103] Combined with the Youth Court's focus on preventing young people under 17 from entering the criminal justice system, this means that the bullies of children like Alex Teka are unlikely to be convicted of any crime.[104]

i. Suicide

As discussed in Chapter One, suicides are frequently linked to cyberbullying in the media. Currently it is a crime to incite, counsel or procure a person to commit suicide, but only if "that person commits or attempts to commit suicide in consequence thereof".[105] This leaves a gap in the law where incitement occurs but the target does not attempt suicide. This inconsistency is being addressed in cl 24 of the HDC Bill, which criminalises incitement where no attempt occurs.

The Minister of Justice considered that the current maximum penalty of 14 years imprisonment reflects the serious nature of suicide and attempted suicide, and a maximum of three years imprisonment would be appropriate where no attempt results.[106] It is arguable that this is an inappropriate distinction to make, as the same actions and intention may be present in both instances. However it is a

---

[102] Crimes Act 1961, ss 21 and 22.
[103] Matthew Keeley and others *Research on youth exposure to, and management of, cyberbullying incidents in Australia. Part B: cyberbullying incidents involving Australian minors, the nature of the incidents and how they are currently being dealt with (SPRC Report 10/2014)* (Australian Government Department of Communications, 2014) at 41.
[104] Alex Teka committed suicide aged 12: see above n 43.
[105] Crimes Act, s 179.
[106] Cabinet Social Policy Committee Paper "Harmful Digital Communications" (April 2013) at 12.

distinction made in other areas of the law, for example in the different penalties for murder and attempted murder in ss 172 and 173 of the Crimes Act.

ii. Threatening to kill or cause grievous bodily harm

It is an offence punishable by up to 7 years imprisonment to threaten to kill or commit grievous bodily harm, either in person or by sending or causing to be received "any letter or writing containing any threat to kill or do grievous bodily harm."[107] This is wide enough to encompass sending a threatening message in writing over a social networking site, and was used in *R v Pengelly* and *R v Hutton* to convict defendants for threatening to kill over text.[108] However the restricted application to "letters or writing" requires amendment in light of the ability of digital technology to communicate videoed and spoken threats.

iii. Publishing an intimate visual recording

The offence of publishing an intimate visual recording is dealt with in sections 216G-216N of the Crimes Act. However its application to cyberbullying is limited, as s 216G defines 'intimate visual recording' as a recording that is made "without the knowledge or consent" of the subject, excluding recordings that were initially made with consent.

In the Ministerial Briefing Paper, the Law Commission recommended that the unauthorised publication of intimate visual recordings taken with consent be added to the Crimes Act with the other intimate visual recording sections, subject to the same maximum penalty of 3 years imprisonment.[109] However this recommendation was rejected on the grounds that the Commission's approach would criminalise behaviour that "could be more appropriately dealt with by existing civil remedies" and that it would be "an uncomfortable fit with the covert filming offences, which require a lack of knowledge of the filming

---

[107] Crimes Act, s 306.

[108] In *R v Pengelly* [2013] NZHC 527 at [4-6], the accused sent a series of text messages to his ex-girlfriend threatening to kill her and her community health nurse. In *R v Hutton* HC Hamilton CRI-2005-419-379, 20 May 2005 at [9], the accused threatened his ex-girlfriend through a combination of phone calls and text messages.

[109] Law Commission *Harmful Digital Communications: The adequacy of the current sanctions and remedies* (Ministerial Briefing Paper, 2012) [Ministerial Briefing Paper] at 91.

itself."[110] The reasoning behind this decision is unclear, as it would be easy to avoid any 'inconsistency' with the existing provisions if they were amended, and it would create a more consistent scheme of offences if the Crimes Act definition were simply expanded.[111] Instead, the gap in the law is addressed by the new offence in cl 19 of the Bill, which defines 'harmful digital communications' widely to include intimate visual recordings made with or without knowledge or consent.[112]

iv. Indecency offences

In *New Zealand Police v Beange*, the defendant was charged under s 126 of the Crimes Act with doing an indecent act with intent to insult or offend after he created a fake Facebook profile featuring a topless photograph of the victim.[113] However this decision appears to stretch the interpretation of the section, as other s 126 cases have involved offenders performing an indecent physical act (such as masturbating in public). Requiring a physical act accords better with the language of the section: "does any indecent act in any place".[114]

Section 124 Crimes Act prohibits the distribution or exhibition of indecent matter, but does not apply to "publications" within the definition of the Films, Videos and Publications Classification Act 1993.[115] This prevents the application of s 124 to cyberbullying situations involving written comments, photographs or videos.[116] Prosecutions under s 124 also require the leave of the Attorney-

---

110 Cabinet Social Policy Committee Paper, above n 106, at [81].
111 The cl 19 penalty is discussed further in Chapter Three at 40-41.
112 Clause 19(4)(a).
113 *New Zealand Police v Beange* DC Dunedin CRI-2012-012-003856, 3 May 2013.
114 Masturbation in front of other people: *George v Police* [2014] NZHC 1725; *R v Bailey* [2012] NZHC 1276; *Trower v R* [2011] NZCA 653. Groping a woman: *T (CA662/2012) v R* [2013] NZCA 550. *New Zealand Police v Beange* at [48], [52] commented on the stigma attached to the offence.
115 Films, Videos and Publications Classification Act 1993, s 2: "publication" is defined as "any film, book, sound recording, pictures, newspaper, photograph, … any print or writing".
116 This section has been used to convict a man for posting naked pictures of his ex-girlfriend to Facebook: "Naked photo sends jilted lover to jail" (13 November 2010) Stuff <www.stuff.co.nz>. However it is arguable that this was not a correct use of the section, as s 124(6) states that the section does not apply to "publications" as defined in the Films, Videos and Publications Classification Act, s 2, which includes pictures.

General, meaning that this section is unlikely to facilitate the speedy removal of images from the internet.[117]

v. Objectionable publications

Sections 123 and 124 of the Films, Videos and Publications Classification Act create a strict liability offence of making, possessing or distributing an objectionable publication, and are similar to cl 19 of the HDC Bill in their aim to regulate offensive, harmful or objectionable material. The Act applies to publications considered objectionable because they deal with matters "such as sex, horror, crime, cruelty or violence" in a manner likely to be injurious to the public good.[118] In *R v Broekman*, the defendant was convicted under s 124 for encouraging a drunken teenager to perform sexually explicit acts, videoing her and publishing the video online, making her "instantly notorious."[119]

While these sections can be applied to situations involving graphic sexual content, the definition of what amounts to "objectionable" material is not well suited to cyberbullying through insults or rumours, which can also have a serious impact. The Act also defines "objectionable" with reference to the likelihood of injury to the public good, rather than the impact it may have on an individual. This could be seen as inconsistent with cl 3 of the HDC Bill, which focuses on the harm occasioned to individuals by harmful digital communications.[120]

vi. Blackmail and Intimidation

Section 237 of the Crimes Act prohibits threats to "disclose something about any person… to cause the person to whom the threat is made to act in accordance with the will of the person making the threat." When revenge porn is combined with threats, prosecutions for blackmail could be an alternative to a prosecution under the Crimes Act intimate visual recording sections.[121]

---

[117] Section 124(5).
[118] Films, Videos and Publications Classification Act, s 3.
[119] *R v Broekman* [2012] NZCA 213. Broekman was sentenced to 12 months imprisonment.
[120] See the text of cl 3 in Appendix B.
[121] This combination of revenge porn and blackmail could include a demand that the subject sends them more pictures: David Clarkson "Woman feared nude pics posted

Intimidation may be present in cyberbullying situations involving threats of violence. Under s 21 of the Summary Offences Act 1981 it is an offence if, intending to frighten or intimidate or knowing that your conduct is likely to frighten or intimidate, you threaten to injure a person or their family, or to damage their property. Intimidation carries a penalty of up to three months imprisonment or a fine not exceeding $2000.[122]

vii. Misuse of a telephone device

The closest section New Zealand has to a specific harmful communications provision is s 112 Telecommunications Act 2001. Section 112 states that a person commits an offence if (while using a telephone device) they use language or make a suggestion that is profane, indecent or obscene or if they use a telephone device to disturb, annoy or irritate another person or to knowingly give a fictitious message, order or instruction.[123] "Telephone device" is defined in s 5 of the Act as "any terminal device capable of being used for transmitting or receiving any communications over a network designed for the transmission of voice frequency communication." This section also carries a penalty of imprisonment for a maximum of 3 months or a fine not exceeding $2000.[124]

Section 112 was used in *Fenandos v Police* where the defendant was convicted for sending abusive texts to his ex-partner.[125] However the definition of "telephone devices" in the Act excludes computer based online behaviours and employs a distinction that (as mentioned in Chapter One) is becoming increasingly irrelevant as more people access the Internet from their mobile phones. It could be argued that as fax machines were recognised as "telephone

online" *The Press* (online ed, Christchurch, 25 August 2014); or in the case of Feng Xiao, a demand that his ex-girlfriend pay him money and clean his apartment, or he would release a sex tape: Rob Kidd "Man gets home detention for blackmailing partner into cleaning" *The New Zealand Herald* (online ed, Auckland, 30 September 2014).

[122] Section 21(3).

[123] Telecommunications Act 2001, s 112(1) and (2).

[124] Section 112(3).

[125] *Fenandos v Police* HC Auckland CRI-2010-404-280, 12 November 2010. In 2012 Liam Ryan-Morris was convicted under s 112 for using text messages to threaten to post naked pictures of a woman on Facebook: David Clarkson "Man in court over naked pic threats" *The Press* (online ed, Christchurch, 31 May 2012).

devices" in *McLachlan v Police*, computers capable of transmitting "voice frequency communication" (over programs like Skype) could be included in the definition, but amending the definition would provide greater clarity.[126] The Law Commission has also suggested that the broad scope and low threshold of s 112 could breach the New Zealand Bill of Rights Act 1990 freedom of expression provisions.[127]

E. International approaches

i. Australia

Cyberbullying occurs at approximately the same rate in Australia as it does in New Zealand, with 21 per cent of 14-15 year olds and 16 per cent of 16-17 year olds reporting being cyberbullied.[128] Australia has a number of non-legislative cybersafety measures, including a voluntary, non-enforceable "Cooperative Arrangement for Complaints Handling on Social Networking Sites" (the Protocol) agreed to by Facebook, Google, Yahoo!7 and Microsoft. The Protocol is designed to simplify the reporting of complaints and to "educate users on mechanisms to deal with problems which arise on their sites."[129]

The Australian Government intends to establish a "Children's e-Safety Commissioner", and create a complaints system for the speedy removal of harmful or distressing content on social media sites. The Government has also committed to "investigating options for a simplified cyberbullying offence."[130] In

---

[126] *McLachlan v Police* HC Auckland CRI-2010-404-106, 29 June 2010: McLachlan sent faxes accusing people of selling poisonous plant food and claiming they were headed to hell.

[127] Ministerial Briefing Paper, above n 109, at [4.20]. For further discussion of s 112 see Chapter Four at 49-50.

[128] *Enhancing Online Safety for Children: Public consultation on key election commitments* (Australian Government Department of Communications, January 2014) [*Enhancing Online Safety for Children*] at 3.

[129] Australian Government Department of Communications "Online Safety" <www.communications.gov.au>.

[130] Australian Government Department of Communications "Online Safety" <www.communications.gov.au>.

January 2014, the Department of Communications released a paper detailing their proposals and seeking feedback from the public.[131]

A Children's e-Safety Commissioner

Like the Approved Agency in the HDC Bill, the Commissioner in intended to resolve complaints, facilitate dispute resolution and enable the rapid removal of harmful content from social media. In comparison to the Agency, the Commissioner will have a much more explicit and detailed educational role, including involvement in public education, the provision of advice to parents and researching the impact of online behaviours.[132]

Removal of harmful material from social media sites:

In response to concerns that the Protocol provides no means of redress for complainants dissatisfied with how their complaints have been handled,[133] as well as comments by the Australian Police that the Protocol has not made service providers more cooperative with Police requests,[134] the 2013 National Bullying, Young People and the Law Symposium recommended the creation of a tribunal with the power to require the removal of material from the Internet.[135] The Australian Government proposes that the Commissioner will take on this role, monitoring a new scheme requiring social media sites to create acceptable complaints procedures that conform to Government criteria, and investigating complaints from the public if these mechanisms failed.[136] This solution is similar to the cl 20 safeharbour provisions in the HDC Bill, discussed in Chapter Three.

On receipt of a complaint, the Commissioner would assess whether "a reasonable person would consider that the material would be likely to cause harm or

---

131 *Enhancing Online Safety for Children*, above n 128.
132 At 5.
133 At 11.
134 Keeley and others, above n 103, at 54-55.
135 *Enhancing Online Safety for Children*, above n 128, at 9-10. Currently, the Australian Communications and Media Authority (ACMA) receives complaints from the public about inappropriate or harmful online content. If the ACMA finds that content is or is likely to be prohibited, it can direct the content provider to remove or prevent access to it.
136 At 13-14.

distress to the child." Unlike cl 10(1)(a) and cl 11(2)(b) of the HDC Bill's proposed District Court orders, there is no requirement that actual harm be caused.[137] If the test is met, the Commissioner may issue take down notices to the author or the social media site.[138]

A potential new cyberbullying offence:

The existing Australian offence regulating digital communications is s 474.17 of the Criminal Code Act 1995 (Australia).[139] Section 474.17 makes it an offence to use a "carriage service" in a way that reasonable persons would consider menacing, harassing or offensive. "Carriage service" is defined in the Telecommunications Act 1997 (Australia) as "a service for carrying communications by means of guided and/or unguided electromagnetic energy."[140] The offence is punishable by 3 years imprisonment and/or a fine of up to $30,600.[141] The language and penalty of the section have been criticised, creating debate about whether Australia should enact a new offence of bullying (including cyberbullying).[142]

The discussion paper notes that the current offence has been used to prosecute instances of cyberbullying successfully, for example in *Agostino v Cleaves*.[143] The paper expresses concerns that a new offence may "over extend to behaviour which should not be treated as criminal," encourage over-reporting of incidents, and lead to more minors being charged with criminal offences.[144] In submissions on the paper, the Australian Federal Police and the Australian Law Council considered that the current offence was "more than adequate" and that "the breadth of section 474.17 is its strength, capturing a wide range of behaviours in

[137] At 15.
[138] At 16.
[139] See the text of s 474.17 in Appendix A.
[140] Section 7.
[141] *Enhancing Online Safety for Children*, above n 128, at 20.
[142] At 22.
[143] *Agostino v Cleaves* [2010] ACTSC 19. Agostino used Facebook to threaten his ex-girlfriend's new partner.
[144] *Enhancing Online Safety for Children*, above n 128, at 23.

a rapidly evolving online environment."[145] It therefore seems unlikely that a new bullying offence will be created in Australia in the near future.

ii. The United Kingdom

The UK, like New Zealand, has a variety of civil and criminal laws that address different aspects of cyberbullying behaviour, including a requirement that all school have an anti-bullying policy.[146] The UK also has two communications offences: s 127 of the Communications Act 2003 (UK) and s 1 of the Malicious Communications Act 1988 (UK).[147]

Section 127 Communications Act 2003 (UK): Improper use of public electronic communications network

Section 127 is a descendant of s 43 of the Telecommunications Act 1984 (UK), which dealt with postal and telephone communications.[148] There have been some concerns about the potential for the wide scope of this section to censor legitimate, frivolous or trivial comments. These were raised in *Chambers v Director of Public Prosecutions*, after Paul Chambers was convicted under s 127 for a tweet expressing his annoyance that an airport was closed: "Crap! Robin Hood Airport is closed. You've got a week and a bit to get your shit together otherwise I am blowing the airport sky high!!"[149] On appeal the High Court overturned his conviction, saying "a message which does not create fear or apprehension … falls outside this provision, for the very simple reason that the

---

[145] Australian Federal Police "Submission to the Government's Discussion Paper on Enhancing Online Safety for Children" at [15]. See also Australian Law Council "Submission to the Government's Discussion Paper on Enhancing Online Safety for Children" at [8]. In contrast, the New Zealand Police support the creation of a new communications offence in cl 19 of the HDC Bill: see New Zealand Police "Submission to the Justice and Electoral Select Committee on the Harmful Digital Communications Bill 2013" at [2].

[146] School Standards and Framework Act 1998 (UK), s 61(4)(b), discussed in Magdalena Marczak and Iain Coyne "Cyberbullying at School: Good Practice and Legal Aspects in the United Kingdom" (2010) 20(2) Australian Journal of Guidance & Counselling 182 at 187.

[147] See the text of both sections in Appendix A.

[148] Lilian Edwards "Section 127 of the Communication Act 2003: Threat or Menace?" (September 2012) panGloss <www.blogscript.blogspot.co.uk>.

[149] *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (Admin), [2013] 1 WLR 1833 at [12].

message lacks menace."[150] The approach taken by the High Court was affirmed in recent Crown Prosecution Service guidelines, discussed below.

Section 1 Malicious Communications Act 1988 (UK): Offence of sending letters etc with intent to cause distress or anxiety

The Malicious Communications Act (UK) was created following a UK Law Commission report on "Poison Pen" letters in 1985. The Law Commission considered that the distress and anxiety caused by poison pen letters warranted a new offence to criminalise the distribution of "material which is abusive, frightening, or menacing but is not defamatory."[151] However unlike cl 19 of the HDC Bill, the Act does not require the message to cause anxiety and distress as an element of the offence. Recently, s 1 has been used to charge people for offensive comments made on social networking sites and for death threats made over text.[152]

UK Crown Prosecution Service Guidelines

In December 2012 the UK Crown Prosecution Service issued guidelines detailing when it is appropriate to prosecute someone for comments made on social media. The House of Lords Communications Committee endorsed these guidelines, also saying that it did not think that a new offence of 'cyberbullying' was needed to supplement the current communications offences.[153]

The guidelines recognise the potential for prosecutions to have a chilling effect on free speech, emphasising that a communication that is merely "in bad taste, controversial or unpopular, and may cause offence to individuals or a specific community," is not illegal. The guidelines also identify the importance of considering the age and maturity of the authors of online communications, as

[150] At [30].
[151] United Kingdom Law Commission *Report on Poison Pen Letters* (Law Com. No. 147, 1985) at [1.2], [2.17].
[152] Henry McDonald "Man charged over Ronan Kerr social network comments" *The Guardian* (online ed, London, 30 June 2011); "Man in BNP expose sent abusive text messages" *The Guardian* (online ed, London, 26 August 2004).
[153] House of Lords Select Committee on Communications *Social media and criminal offences* (House of Lords, HL Paper 37, July 2014) at [30], [32].

"[c]hildren may not appreciate the potential harm and seriousness of their communications."[154] A requirement to consider the characteristics of authors in the HDC Bill's District Court orders provisions and cl 19 would allow recognition of the overlap that exists between bullies and targets, and would help address the challenges facing bullies, creating a fairer outcome overall.

F. Conclusion

Both New Zealand and Australia have identified the need for a new civil takedown regime. Although New Zealand's current privacy, defamation and harassment laws encompass some aspects of cyberbullying, they are not a comprehensive solution, and victims would be forced to incur costs pursuing them as a remedy. New Zealand also lacks a dedicated communications offence similar to those in Australia and the UK, although amendments to current law could fill this gap. Australia is considering whether to create a new offence in addition to s 474.17 Criminal Code Act, while the House of Lords has recently said that the UK does not require a new cyberbullying offence to supplement their current communications offences. Parliament's response to the gaps present in our law has been to create the HDC Bill. The three-stage proposal in the Bill is controversial, however, and requires examination.

[154] The Crown Prosecution Service "Guidelines on prosecuting cases involving communications sent via social media" <www.cps.gov.uk>.

Chapter Three: The Proposed Harmful Digital Communications Bill

A. Origins of the Bill

In October 2010 the Law Commission was asked "to review the adequacy of the regulatory environment in which New Zealand's news media is operating in the digital era." Specifically, the Commission was asked "whether the existing criminal and civil remedies for wrongs such as defamation, harassment, breach of confidence and privacy are effective" and if not, what alternative remedies could be available.[155] In response to a request from the Minister Responsible for the Law Commission, the Honourable Judith Collins, the Law Commission published a Ministerial Briefing Paper entitled "Harmful Digital Communications: Adequacy of current sanctions and remedies" in August 2012.

In the Briefing Paper, the Commission noted that the current criminal law provides limited protection against communications causing mental distress without physical harm, and recommended the creation of a new offence targeting digital communications that are of a "grossly offensive or of an indecent, obscene or menacing character."[156] Alongside the new offence, the Commission recommended the creation of a statutory "Approved Agency" to resolve complaints about digital communications through mediation.[157] In serious situations where the Agency could not resolve the problem, the Commission suggested that a Communications Tribunal be created to provide victims with speedy civil remedies.[158] It also recommended changes to the Harassment Act, Privacy Act and changes to the Crimes Act incitement to suicide and intimate visual recordings provisions. Finally, the Commission proposed that that the Ministry of Education monitor bullying levels and require all schools to

[155] Law Commission *The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age* (NZLC IP27, 2011) at 3.
[156] Ministerial Briefing Paper, above n 109, at 15.
[157] At 18.
[158] At 17.

implement anti-bullying programmes.[159] The Law Commission attached a draft Bill detailing their recommendations to the Ministerial Briefing Paper, entitled the Communications (New Media) Bill.

After the publication of the final Report of the Law Commission in March 2013, the Minister of Justice recommended the introduction of a new civil orders regime and changes to existing legislation to meet the challenges posed by digital communications.[160] The Minister agreed with the Law Commission's recommendation to create a new cyberbullying offence, and considered that this offence could address the publication of intimate pictures without consent, rather than adding a new section to the intimate visual recordings offences. The Minister also considered that enlarging the powers of the District Court to administer the civil orders regime would be more appropriate than creating a specialist Communications Tribunal.[161]

The debates during the first reading of the Bill reflected the public's impression that the Bill was designed to prevent harmful online behaviours among young people.[162] This impression was strongly influenced by the 'Roast Busters' scandal that emerged during the Bill's first reading, which involved a group of young men boasting online about having sex with drunk, underage girls.[163] The publicity given to this scandal drew attention to the Bill, which the media reported as containing measures to prevent and punish this type of behaviour.[164]

---

159 At 19-20.
160 Cabinet Social Policy Committee Paper, above n 106, at 1.
161 Cabinet Social Policy Committee Paper, above n 106, at 7. The Minister proposed to reduce the costs associated with applications to the District Court by waiving filing fees.
162 The first reading of the Harmful Digital Communications Bill took place on the 14th of November and 3rd of December 2013.
163 Talia Shadwell "Top cop fronts over Roast Busters case" (11 December 2013) Stuff <www.stuff.co.nz>.
164 Andrea Vance and Jody O'Callaghan "'Time's up' for cyber tormentors" *The Press* (online ed, Christchurch, 5 November 2013).

B. The Bill as at its first reading

i. Purpose (Clause 3):

The purpose of the Bill is to "mitigate the harm caused to individuals by digital communications and to provide victims of harmful digital communications with a quick and efficient means of redress." However as the Internet itself is merely a tool that enables harmful behaviours, a more accurate purpose would refer to "victims of the harmful use of digital communications."[165]

ii. The Approved Agency (Clauses 7 - 9):

Under cl 7, the Governor General (on the recommendation of the Minister responsible for the Bill) may appoint any person, organisation, department or Crown entity to be the Approved Agency.[166] Before recommending the appointment, the Minister must be satisfied that "the appointee has the appropriate knowledge, skills and experience" to perform the Agency's required functions.[167] Both the Law Commission and the Minister of Justice envisage that NetSafe will be the Approved Agency, due to NetSafe's efforts to raise awareness about cybersafety and established relationships with Internet service providers. NetSafe's current focus on victim advocacy has led to concerns that it would not be a neutral adjudicator between complainants and alleged perpetrators.[168] However, NetSafe's submission on the Bill assuages these concerns, emphasising the importance of respecting Internet culture and the need for both parties to participate in the resolution process.[169]

The functions and powers of the Approved Agency are stated in cl 8, and can be expanded under cl 7(1)(b). They include receiving, assessing, investigating and resolving complaints, establishing and maintaining relationships with service providers and content hosts and providing education and advice "on policies of

---

[165] Gareth Hughes MP, First Reading of the Harmful Digital Communications Bill 2013 (3 December 2013) 695 NZPD 15164.
[166] Clause 7(1)(c) states that the Governor General may prescribe any reporting or accountability measures that the Agency must comply with.
[167] Clause 7(2).
[168] Clare Curran MP, First Reading of the Harmful Digital Communications Bill 2013 (3 December 2013) 695 NZPD 15164.
[169] NetSafe "Submission", above n 21, at 13, 16.

online safety and conduct on the Internet."[170] While carrying out their functions and exercising their powers under the Act, the Approved Agency and the District Court must "take account of" the communication principles listed in cl 6.[171]

In view of the fact that defining and measuring cyberbullying are essential to this area of law, it is surprising that the Bill does not impose any monitoring responsibilities on the Agency. For example, collecting data on the numbers of cyberbullying incidents reported to schools, NetSafe and the Police and the age of those involved would help the Ministry of Education create targeted anti-bullying programmes. The wording of cl 8 also does not indicate what "advice" the Agency is expected to provide, and to whom. Finally, the lack of any clear educational role in cl 8, commented on in the Australian Cyberbullying Research Report, is a major weakness in the Bill's attempts to address cyberbullying.[172]

iii. The District Court (Clauses 10 – 18):

Clause 10 states that the Police, individuals who allege they have suffered harm, a parent or guardian on their behalf or a principal of the school where the individual is a student (with the student's consent) can apply for a District Court order. Before an application can be made to the Court, the Approved Agency must have "had a reasonable opportunity to consider and decide what action (if any) to take."[173] However this does not make the Agency a gatekeeper to the District Court. Applicants can apply to the Court if they are dissatisfied with the Agency's decision, or before a decision is reached if the Agency fails to make a decision despite having a "reasonable opportunity" to do so.[174] This is not consistent with the Minister's prediction that the orders "would only be used as a last resort," and that "only serious cases… should come to court."[175]

---

[170] Clause 8.
[171] Clause 6(2)(a).
[172] Spears and others, above n 20, at 32; see also Ilan Katz and others *Research on youth exposure to, and management of, cyberbullying incidents in Australia: Synthesis report* (Australian Government Department of Communications, June 2014) at 8. The importance of education is discussed in Chapter Four at 52-55.
[173] Clause 11(1).
[174] Clause 11(2).
[175] Cabinet Social Policy Committee Paper, above n 106, at [43], [51].

The District Court can reject frivolous or vexatious applications or applications that do not meet the threshold requirements of cl 11(1), but it would be more efficient for this to happen at the Agency level.[176] In their submission on the Bill, the Judges of the District Court predicted that determining oral applications would occupy 75 days of judge time a year, with more time and resources required to deal with applications that do not proceed to a full oral hearing. The Judges were also concerned about the logistical challenges of orders that require determination at short notice by a judge with knowledge of digital communications.[177]

The concerns expressed by the Judges indicate that the District Court is unlikely to be able to efficiently administer the new orders unless it receives additional resources. Given the need for investment in the District Court, creating a Communications Tribunal as suggested by the Law Commission is an option that requires more consideration. Tribunals are generally perceived as more approachable than courts, and a Tribunal structure would more accurately reflect the reality that a small number of specialist judges are likely to move around the country responding to applications as they arise.

However, if the District Courts retained responsibility for the orders, efficiency could be improved and resources saved if the Approved Agency was given control over referrals to the Court. As a safeguard against abuse of this referral power, applicants could have the option of seeking leave from the Court to apply for an order, which would require them to present an arguable case before the court committed to hearing it.

iv. The District Court Orders

If the Court is satisfied that there has been a serious or repeated breach of the communications principles that has caused or is likely to cause harm, it can issue takedown orders, orders for corrections, apologies, replies and orders that the defendant cease the conduct concerned and not encourage others to engage in

[176] Clause 11(3).
[177] The Judges of the District Courts "Submission to the Justice and Electoral Committee on the Harmful Digital Communications Bill 2013" at 10.

it.[178] If an online content host is not protected by the safeharbour provisions in cl 20, the Court can order that they remove material, disable public access, release the identity of anonymous authors, publish a correction or allow a right of reply.[179] When determining whether to make an order the Court must take into account the factors listed in cl 17(4), including the content and context of the communication, the vulnerability of the victim, the truth of the statement, any public interest in the communication and the "technical and operational practicalities, and the costs, of an order."[180]

Clause 17(4) indicates that considerations of truth or falsity and the public interest are less decisive in the HDC Bill than in the Defamation Act. The truth of a statement is referred to in principle 6, which says that "[a] digital communication should not make a false allegation," but this does not clarify the status of a true communication that causes harm. Clause 17(4) also allows the truth or falsity of a communication or the public interest in it to be outweighed by other factors, such as context. The difference in approach between the Defamation Act and the HDC Bill raises questions - why, merely because a statement is published online, should there be no defence of truth to it? Does damage to an individual's feelings outweigh the importance of the truth or the public interest, recognised through case law and in defamation legislation?

The difference between the two Acts can be traced to their different purposes. The Defamation Act is designed to ensure that individuals hold the reputation they are entitled to, and considers that people should bear whatever consequences the truth may have on their reputations. In contrast, the purpose of the HDC Bill is to prevent or mitigate harm, and provide individuals with a means of redress. From this perspective, the truth or falsity of a statement seems less important, as even a true statement (for example a private photo) can cause harm. Although these distinctions may appear justified, in practice the lack of a defence of truth to the District Court orders undermines the rationale of the

[178] Clauses 11 and 17.
[179] Clause 17(2).
[180] The Court can seek advice from a technical expert when considering these factors: cl 15.

Defamation Act by permitting individuals to use the orders to prevent the publication of a true communication because it would cause them harm.

The Law Commission acknowledged the problems arising in the Bill regarding issues of truth and falsity, but considered that principle 6 and cl 17 safeguard the public interest.[181] However when faced with an applicant arguing that a true statement that has been the subject of a failed defamation action breached a communication principle and caused them harm, judges confined to the communication principles and cl 17 factors may struggle to avoid granting an order. The judge would have to reject the application on the ground that it was frivolous or vexatious,[182] because of the conduct of the complainant, the "truth or falsity" of the communication or the "occasion, context and subject matter of the communication."[183] These grounds do not accurately reflect the need to balance the goals of the Defamation Act and HDC Bill.

The District Court Judges have suggested allowing the truth of a statement to be "advanced as a defence unless the court considers that the harmful nature of the communication outweighs the truthful nature of it."[184] Phrasing the truth of the communication as a defence indicates the importance of preserving the rationale of the Defamation Act, while a balancing test leaves room for situations where the degree of harm justifies an order. To ensure that both Acts work in unison, the proposed defence should also refer to the Defamation Act defences of honest opinion, public interest and privilege. The defence of honest opinion could be seized on by many cyberbullies to excuse their actions,[185] however the defamation requirement that opinions must be supported by true facts means this defence is unlikely to be successful very frequently.[186]

---

[181] Ministerial Briefing Paper, above n 109, at [5.83].
[182] Clause 11.
[183] Clause 17(4)(c), (f) and (i).
[184] The Judges of the District Courts, above n 177, at [48].
[185] The Defamation Act, s 10(3) states that the defence is available even when the maker of a statement is motivated by malice.
[186] *APN New Zealand Ltd v Simunovich Fisheries Ltd* [2009] NZSC 93, [2010] 1 NZLR 315 at [13].

Similarly to cl 19, the District Court orders operate in relation to the harm caused to victims of harmful digital communications. However, the clauses relating to the District Court orders that deal with the requirement of harm need amendment. Clause 11(2)(b) says that the Court must not grant an order unless it is satisfied that a breach of the communications principles "has caused or is likely to cause harm to a person." However under cl 10(1)(a) individuals, parents, guardians and school principals cannot apply for an order unless the individual concerned alleges that they have *actually* suffered harm. To remedy this inconsistency, cl (10)(1)(a) should be amended to include "or is likely to suffer."

v. The new offence (Clause 19):

The new offence of "causing harm by posting a digital communication" is set out in cl 19 of the Bill. A person commits the offence if they post a communication intending to cause harm to an individual; harm would be caused to "an ordinary reasonable person in the position of the victim"; and harm is caused to the victim. 'Harm' is defined in cl 4 of the Bill as "serious emotional distress".

Clause 19(2) lists factors that the court may take into account in determining whether a post "would cause harm." The truth of a statement is merely one factor that may be considered, rather than a defence, and the public interest in a communication is not listed. However instead of adding a defence to cl 19 (as was suggested in the discussion of the District Court orders above), this dissertation will suggest that the cl 19(1)(c) requirement of actual harm be removed from the offence altogether.

The maximum penalty proposed for a conviction under cl 19 is a fine not exceeding $2000 or a maximum of three months imprisonment. This mirrors the penalties for intimidation in s 21 of the Summary Offences Act and misuse of a telecommunications device in s 112 of the Telecommunications Act, rather than the penalty of a maximum of three years imprisonment for breaches of the

intimate visual recording sections of the Crimes Act.[187] This lower penalty does not recognise the similarities that cl 19 will have with the intimate visual recording sections, and implies that publishing intimate recordings taken with consent for private purposes is less serious than making intimate recordings without consent. This implication can be challenged, as publishing pictures taken with consent for private viewing involves a violation of trust as well as a violation of privacy as a result of publication that is at least equal to the breach of privacy that occurs when images are recorded covertly.

The lower penalty may be in recognition of the fact that the new offence does target the behaviour of young people.[188] In their submission on the Bill, Youthline Otago emphasised the detrimental impact of criminal convictions on young people and the importance of imposing penalties that are proportionate to the age of the offender.[189] Considering this point, a more consistent scheme of offences and penalties would be created if cl 19 adopted the Crimes Act penalty, but included another subsection requiring the judge to consider the characteristics (especially age and maturity) of the offender.[190] This approach accords with the UK Crown Prosecution Guidelines and the calls for any new cyberbullying law in Australia to deal with offences in a way that is "appropriate to the developmental stage of the cyberbully."[191]

vi. The cl 19(1)(c) requirement of 'harm':

The cl 19(1)(c) requirement that harm be caused to the target raises two important questions: why harm is required at all, and if it is necessary, what the definition of harm in cl 4 ("serious emotional distress") means.

---

[187] Crimes Act, ss 216I and 216J. The Justice and Electoral Select Committee have recommended increasing the maximum penalty to two years imprisonment: Harmful Digital Communications Bill 2013 (168-2) (explanatory note) at 4.
[188] That the Bill targets young people is seen in the reference to parents and school principals applying for orders on behalf of children in cl 10(1).
[189] Youthline Otago "Submission to the Justice and Electoral Committee on the Harmful Digital Communications Bill 2013" at 1.
[190] See Appendix C for a revised version of cl 19.
[191] The Crown Prosecution Service, above n 154; Katz and others, above n 172, at 14.

The requirement to prove harm in cl 19 replicates the inconsistency that cl 24's amendment to the suicide provisions is designed to abolish.[192] Where no "serious emotional distress" is suffered the communication will not breach cl 19, although the same communication sent to a vulnerable person causing "serious emotional distress" would be illegal. Recognising the potential for these arbitrary results, the UK Law Commission refused to require the creation of anxiety or distress in their draft of what is now s 1 of the Malicious Communications Act 1988 (UK). The Commission thought that such a requirement "would make prosecutions impossible in cases where the recipient was sufficiently strong willed to be unaffected by this type of communication."[193] *Director of Public Prosecutions v Collins* came to the same conclusion in relation to s 127 of the Communications Act, stating that:[194]

> … the criminality of a defendant's conduct [cannot] depend on whether a message is received by A, who for any reason is deeply offended, or B, who is not. On such an approach criminal liability would turn on an unforeseeable contingency.

Ultimately, cl 19(1)(c) creates illogical distinctions between perpetrators whose targets suffer harm and those whose targets do not.

The requirement of harm also prevents the Bill from denouncing cyberbullying as unacceptable independently from the reaction of a particular victim. Considering the UK communications offences, *Director of Public Prosecutions v Collins* explained that the object of s 127 of the Communications Act (UK) is to prohibit the use of a public service to transmit communications that contravene basic societal standards.[195] In contrast s 1 of the Malicious Communications Act (UK) recognises that communications also have the potential to cause harm to their targets.[196] Like the Malicious Communications Act (UK), cl 3 states that the goal of the HDC Bill is to provide a remedy for victims. However the wider social

[192] See Chapter Two at 22.
[193] United Kingdom Law Commission, above n 151, at [4.22].
[194] *Director of Public Prosecutions v Collins* [2006] UKHL 40, [2006] 1 WLR 2223 at [8].
[195] At [7].
[196] At [26].

aims of the Bill are evident in the wide drafting of the communication principles, especially principle 10, as well as the Law Commission's emphasis on the importance of education about appropriate online behaviours.[197] The requirement that actual harm be caused fails to recognise that cyberbullying is unacceptable whether or not the individual happens to be strong enough to avoid harm.

If the requirement of harm remains in the Bill, the second important question to address is what 'harm' means. "Serious emotional distress" can be compared to the Privacy Act requirement of "significant" humiliation, loss of dignity or injury to feelings.[198] *Winter v Jans* defined "significant" as having an important, notable or considerable impact.[199] However the possibility of imprisonment resulting from a conviction under cl 19 is likely to mean that the courts will interpret 'serious' as setting a higher standard than that in the Privacy Act.[200] The courts are also likely to be wary of the chilling effect of a wide definition of harm. This concern led the UK Crown Prosecution Guidelines to repeat the statement in *Chambers v Director of Public Prosecutions* that distasteful or painful satire, rude humour and unpopular opinion should "continue at their customary level, quite undiminished by this legislation".[201] To avoid any chilling of free speech in New Zealand, the definition of "harm" needs to be amended or clarified through prosecution guidelines.

---

[197] Clause 6: principle 10 states that digital communications should not denigrate people on the basis of factors such as ethnicity and race, tying in to a wider societal belief that discrimination on those grounds is unacceptable. See also the discussion on the importance of education in the Ministerial Briefing Paper, above n 109, at [1.31]-[1.44].
[198] Section 66(1)(b)(iii).
[199] *Winter v Jans* HC Hamilton CIV-2003-419-854, 6 April 2004 at [35], [37].
[200] In particular, a conviction under cl 19 could result in a 3 month prison sentence: cl 19(3). The Select Committee has recommended this be increased to a maximum of two years imprisonment: see Harmful Digital Communications Bill 2013 (168-2) (select committee report) at 17.
[201] The Crown Prosecution Service, above n 154, citing *Chambers v Director of Public Prosecutions,* above n 149, at [28].

vii. Liability of online content hosts and the safe harbour provisions (Clause 20):

Clause 20 states that no proceedings may be brought against an online content host as long as they take reasonable steps to remove content as soon as practicable after receiving a notice of complaint from a user.[202] This protection is lost if the host fails to take these steps, fails to provide an accessible complaints mechanism or if the person providing the content complained of was acting on behalf of the host.[203]

Submitters on the Bill were concerned that cl 20 does not require authors to be notified of complaints about their content. This prevents complaints being challenged and could lead to material being removed for improper reasons. These concerns were acknowledged in the Select Committee Report on the Bill, discussed below.

viii. Enforcement

NetSafe reports that in most complaints they receive the complainant knows the perpetrator, indicating that both parties live within New Zealand's jurisdiction.[204] However international enforcement and relationships with international service providers pose more difficult questions, too complex to be discussed in detail in this research. In the Social Policy Committee report Ms Collins concluded that New Zealand would be reliant on steps taken by our "larger counterparts" in the area of international Internet regulation.[205] Currently, New Zealand is working to accede to the Budapest Convention on cyber-crime and engaging in "ongoing dialogue" with other jurisdictions including Australia.[206]

---

[202] Clause 20(2).
[203] Clauses 20(2) and (5).
[204] NetSafe "Submission", above n 21, at 9.
[205] Cabinet Social Policy Committee Paper, above n 106, at [60].
[206] At [60]. The Council of Europe Convention on Cybercrime (opened for signature 23 November 2001) [the Budapest Convention] <www.conventions.coe.int>, is the first international treaty on crimes committed via the Internet. It addresses infringements of copyright, fraud, child pornography and violations of network security.

The enforcement of the Bill currently relies on the desire of social media sites to be perceived as good corporate citizens who comply with national laws. This is shown by the requirement in cl 8 that the Approved Agency establishes and maintains "relationships with domestic and foreign service providers … to achieve the purpose of this Act."[207]

C. The Submissions: main arguments

The Bill attracted 40 submissions, many of which suggested changes to the 'safeharbour' provisions in cl 20. The Auckland District Law Society (ADLS) criticised cl 20 for failing to provide host sites with opportunities or incentives to assess the merits of the complaints they receive. Combined with the fact that the Bill includes no form of accountability for false complaints, the Society thought this created the potential for "censorship via complaint."[208] Submitters, including Google, suggested that the Bill include a counternotice procedure, a suggestion the Committee adopted.[209] Both the ADLS and the District Court Judges emphasised that the District Court orders could be more efficiently administered if the Approved Agency is given the power of referring complaints to the District Court.[210]

Submitters also commented on cl 19 and the definition of "harm." Google questioned why the more stringent *Wilkinson v Downton* standard was not used, and suggested a new test of whether harm would be caused to a reasonable person in the position of the 'intended audience' of the communication.[211] Facebook suggested linking the definition of harm to whether the defendant

---

[207] Clause 8(1)(d); also see Cabinet Social Policy Committee Paper, above n 106, at [42]. It is because NetSafe has already developed these relationships that it is likely to be appointed the Agency.
[208] Auckland District Law Society "Submission to the Justice and Electoral Committee on the Harmful Digital Communications Bill 2013" at [20].
[209] Google "Submission to the Justice and Electoral Committee on the Harmful Digital Communications Bill 2013" at 32.
[210] Auckland District Law Society at [46]; The Judges of the District Courts, above n 177, at [53]-[54].
[211] Google at 17.

intended their communication to "constitute severe bullying".[212] The Human Rights Commission argued that the requirement of demonstrable harm was too high.[213] Overall, concerns raised by submitters about the requirement of harm indicate that removing the requirement of actual harm, would simplify the section as well as make it less arbitrary.

D. The Bill as reported back from Select Committee

The Justice and Electoral Select Committee's report on the Bill was released on 27 May 2014. The Committee recommended changes to the penalties in the Bill, including increasing the maximum term of imprisonment for a conviction under cl 19 from three months to two years, aligning cl 19's penalty with that in the Harassment Act.[214] However, cl 19 would still not be consistent with the penalties in the intimate visual recordings sections of the Crimes Act, as discussed above, and would continue to imply that publishing intimate visual recordings made for private use is less serious than making intimate visual recordings without consent.

The Select Committee agreed with submitters that the safeharbour provisions needed amendment, and recommended inserting a new cl 20(3) to require online content hosts to notify authors about complaints. If the author responded with a counternotice contesting the complaint the host would have to leave the content in place and bring the complainant's attention "to other remedies," presumably including seeking help from the Approved Agency or District Court.[215]

The Committee did not recommend altering the relationship between the Approved Agency and the District Court. In fact, instead of imposing controls on

[212] Facebook "Submission to the Justice and Electoral Committee on the Harmful Digital Communications Bill 2013" at 10.
[213] Human Rights Commission "Submission to the Justice and Electoral Committee on the Harmful Digital Communications Bill 2013" at [3.8].
[214] Harmful Digital Communications Bill 2013 (168-2) (select committee report) at 17.
[215] At 20.

applications to the Court, the Committee recommended the creation of a new subclause 8(4) requiring the Agency to inform the complainant of their right to apply for an order. The Committee also did not address the problems caused by the requirement of harm throughout the Bill, or the definition of harm in cl 4.

E. Conclusion

Considering the HDC Bill from a cyberbullying perspective, creating an Approved Agency as the 'go to' source of information on cybersafety can only be beneficial. However it is concerning that the educational and monitoring roles of the Agency are not specified. The relationship between the Agency and the Court requires amendment, and the decision to award new powers to the District Court rather than create a Tribunal can be questioned, as can the relationship between the Defamation Act and the new orders proposed in the Bill. However perhaps the most significant problems with the Bill are the flaws in the new offence. Both the requirement that harm be caused to the complainant and the lack of a definition of harm are likely to cause significant problems in the application of the section in the future, and will limit the impact of the Bill on society in general.

Chapter Four: Possible alternatives to the Bill and the problem of asymmetry

A. Introduction

> Technology itself plays a critical role in shaping – and challenging – our values and concept of what is acceptable and what behaviour should be outlawed. This dynamic relationship between technology and social values has always been reflected in the law and lies at the heart of this current debate about how we respond to digital communication harms.[216]

The HDC Bill is New Zealand's response to the tension between the value of Internet freedom and the public's desire not to be subjected to harmful behaviours online. However limitations in the Bill's scope, application and enforcement create the need to examine alternatives to its proposal for the regulation of cyberspace, and to question the validity of the distinction the Bill draws between digital and non-digital communications.

B. Could amendments to existing criminal law perform the same role as cl 19?

The sections that, if amended, could possibly perform the role envisaged for cl 19 are s 112 of the Telecommunications Act and ss 123 and 124 of the Films, Videos and Publications Classification Act.

Unlike the Crimes Act intimate visual recordings sections, ss 123 and 124 do not exclude recordings made with consent, while the reference to the public good in the definition of "objectionable" avoids the distinction between resilient and vulnerable victims currently present in cl 19. However the difference between communications that are injurious to the public good and those that harm individuals could trivialise the experience of victims, especially as the definition

[216] Ministerial Briefing Paper, above n 109, at [24].

of "objectionable" would not include all cyberbullying behaviours.[217] However, the Films, Videos and Publications Classification Act is primarily a censorship tool, and the narrow definition of "objectionable" is necessary to limit how those censorship powers can be exercised.[218] In order to preserve the integrity of the Act and the safeguards within it, a better solution would be to alter cl 19 to prohibit communications that are injurious to the public good as well as communications that could cause distress to individuals.[219]

Section 112 of the Telecommunications Act is the closest section New Zealand has to the communications offences in Australia and the UK. However to effectively replace cl 19 it would need to be expanded beyond communications made using "telephone devices." It is also likely that the wide range of behaviour covered by s 112 (including using a telephone device to "disturb, annoy or irritate" someone) would need to be limited to avoid breaching the freedom of expression provisions in the New Zealand Bill of Rights Act 1990, and to reflect the UK position that a communication must be "more than simply offensive" to be illegal.[220]

Incorporating digital communications into the s 112 offence, creating an offence that deals with digital and non-digital communications, could help address the arguments made by some submitters that cl 19's focus on digital communications creates asymmetrical law.[221] Amending a pre-existing section rather than creating a new offence could also help to de-sensationalise the

---

[217] Films, Videos and Publications Classification Act, s 3.
[218] The long title of the Films, Videos and Publications Classification Act is "An Act to consolidate and amend the law relating to the censoring of films, videos, books, and other publications".
[219] See Appendix C for a revised version of cl 19.
[220] Currently s 112 criminalises a potentially wide range of language, including profane, indecent or obscene language or suggestions, using a telephone device to disturb, annoy or irritate another person; or to knowingly give a fictitious message, order or instruction. In the Ministerial Briefing Paper, above n 109, at [4.20] the Law Commission suggested that this wide range of behaviours breached s 14 of the New Zealand Bill of Rights Act 1990. For the UK position see The Crown Prosecution Service, above n 154.
[221] Tech Liberty "Submission to the Justice and Electoral Select Committee on the Harmful Digital Communications Bill 2013" at 3.

reporting of cyberbullying in the media, by avoiding the characterisation of cyberbullying as a new harm.

However, in view of the three-stage approach of the HDC Bill, separating the criminal offence from the Approved Agency and District Court orders not only presents a less coherent message to the producers of harmful digital communications, but also makes the justice system's attitude towards cyberbullying less clear to complainants. The clarity of the three-stage proposal set out in the Bill is particularly important because it the Bill involves an area of law that the general public, especially young people, are likely to have contact with. Overall, maintaining the structure of the Bill is likely to have more impact than replacing cl 19 with an amended version of s 112.

C. Is self-regulation the solution?

The HDC Bill's new civil regime relies on the cooperation of service providers at the Approved Agency and District Court levels. This raises the question of whether coordinated self-regulation (similar to the Australian Protocol) could be an alternative to the Bill's proposed civil regime.

Many service providers practise a degree of self-regulation already. Facebook and Twitter have created tools for users to report breaches of their terms and conditions and to block others from interacting with them online.[222] Internet and mobile phone connection providers like Vodafone, Spark (formerly Telecom) and 2Degrees provide information on how to deal with cyberbullying, as well as tools for parents to control their children's mobile phone usage.[223] Vodafone also created 'Vodafone Blacklist', a tool that allows users to block messages from

[222] "Facebook Help Center" Facebook <www.facebook.com>; "Twitter Help Center" Twitter <www.twitter.com>.
[223] See "Help Me" Vodafone <www.vodafone.co.nz>; "Help" Spark <www.spark.co.nz>; "Help & Support" 2Degrees <www.2degreesmobile.co.nz>.

certain phone numbers, which can prevent cyberbullying through text messages.[224]

However the terms and conditions set by social media providers can easily be circumvented, as shown by Lori Drew's involvement in the suicide of Megan Meier.[225] Any attempts at self-regulation are also constrained by "the inherent tension between the need for corporate accountability and the right of private commercial sectors to self regulate."[226] Service providers are anxious to maintain the individuality of their sites, and therefore oppose extensive regulation. As a result, service providers impose different degrees of regulation according to their view of the right balance between freedom of speech and online safety.[227]

In practice, Australia's experience of self-regulation under the Protocol (suggested by the Internet Party as an alternative to the HDC Bill) shows that it is unlikely to have the effect desired.[228] Australian Police have found that service providers are slow to respond to police requests and reluctant to remove material. Over half of all complainants were dissatisfied with the outcome of their complaint, and reported being told that it was their responsibility, not the site's, to block the bully.[229] In the UK, the House of Commons has said that it is clear that platforms like Facebook and Twitter "could do far more to signal the unacceptability of abuse and stamp it out when it arises."[230]

---

[224] Vodafone "Submission to the Justice and Electoral Select Committee on the Harmful Digital Communication Bill 2013" at [B2.2].
[225] Tokunaga, above n 13, at 277. See Chapter One at 10.
[226] Ministerial Briefing Paper, above n 109, at 104.
[227] Ministerial Briefing Paper, above n 109, at [3.15]-[3.17]. An example of social media facilitating behaviour that many people would consider unsafe is in the prevalence of 'thinspiration' pages on image sharing sites like Tumbler and Pinterest. These pages contain pictures and messages designed to encourage girls to lose weight, and are often associated with eating disorders like anorexia: Carolyn Gregoire "The Hunger Blogs: A secret world of teenage 'thinspiration'" (2 September 2012) The Huffington Post <http://www.huffingtonpost.com>.
[228] Internet Party, "Submission to the Justice and Electoral Select Committee on the Harmful Digital Communications Bill 2013" at [2].
[229] Katz and others, above n 172, at 7.
[230] House of Commons Culture, Media and Sport Committee *Online safety: Responses to the Committee's Sixth Report of Session 2013-14, First Special Report of Session 2014-15* (House of Commons, 1 July 2014) at recommendations 28, 29.

The New Zealand Police have also questioned the effectiveness of self-regulation, and report that they are receiving increasing numbers of requests for help from the public in relation to social media.[231] Similarly, NetSafe receives many complaints from people who feel "defeated and distressed by the complexity of complaints systems and the lack of direct communication channels."[232] Law Commission research found that less than a third of participants surveyed were aware of online safeguards and reporting tools, and of those the majority thought they were not effective, or were only effective some of the time.[233]

After considering the effectiveness of self-regulation currently, the experience of Australia and recommendations from the UK, it would be unwise to increase New Zealand's reliance on self-regulation. At present the efficiency of the Approved Agency and District Court will require the cooperation of service providers, but the balance that the HDC Bill strikes between cooperation and regulation should not be disturbed. This is the attitude taken by Telecom (now Spark), who acknowledge that "legislation provides a necessary escalation path for when the more informal approach does not work."[234]

D. Could education eradicate cyberbullying?

Australian research has found that young people are:[235]

> … unlikely to be impacted by a purely legal approach due to the nature of their impulsivity, their experience that few cyberbullies have been convicted, their belief in their superior knowledge and understanding of technology compared to adults, their lack of awareness of the relevant laws, and … their belief they are unlikely to be caught due to their anonymity.

---

231 Ministerial Briefing Paper, above n 109, at [3.58].
232 At [3.40].
233 At [3.44]-[3.47].
234 Telecom "Submission to the Justice and Electoral Select Committee on the Harmful Digital Communication Bill 2013" at [14].
235 Katz and others, above n 172, at 7.

This assessment of the impact of the law on the behaviour of young people indicates that for the HDC Bill to be effective, it needs to be enacted alongside attempts to address cyberbullying at a more personal level.[236] Researchers in Australia and Canada suggest that educational campaigns can have a significant effect on cyberbullying by explaining the serious impact cyberbullying can have, empowering victims and enabling professionals to prevent future incidents.[237]

Schools are currently required to provide a safe environment for students under NAG 5, and in 2011 the Ombudsman recommended that NAG 5 be amended to specifically require all schools to create and implement anti-bullying policies.[238] The New Zealand Human Rights Commission supported this recommendation, as did the Prime Minister's Chief Science Advisor.[239] However the Ministry of Education considered that an amendment to NAG 5 was not necessary, because the Ministry had clear expectations that all schools would all implement anti-bullying policies.[240] In April 2013, the Social Policy Committee paper considered that the Law Commission's concern that many schools did not have effective anti-bullying policies was being addressed in the programmes that the Ministry had in place or planned to implement.[241]

In the same month that the Social Policy Committee responded to the Commission's Ministerial Briefing Paper, a Victoria University study found that out of 1,236 school staff, 65 per cent supported including a requirement that schools create anti-bullying guidelines in the national administration guidelines. Only 60 per cent of respondents said that their school had a zero tolerance policy on bullying,[242] and less than half had received anti-bullying training or attended

---

[236] At 8.
[237] At 12; The Nova Scotia Taskforce on Bullying and Cyberbullying, above n 3, at 87.
[238] *Report of David McGee, Ombudsman on Complaints Arising out of Bullying at Hutt Valley High school in December 2007* (2011) at 39.
[239] The Prime Minister's Chief Science Advisor, above n 39, at 129; New Zealand Human Rights Commission, above n 54, at 7.
[240] Ministerial Briefing Paper, above n 109, at [6.48].
[241] Cabinet Social Policy Committee Paper, above n 106, at 26. Some of the resources available for schools include Positive Behaviour for Learning and the Wellbeing@School programme, as well as the Kia Kaha programme designed by New Zealand Police: Bullying Prevention Advisory Group, above n 53, at 65.
[242] Green and others, above n 59, at 6.

anti-bullying workshops.[243] Many participants expressed "confusion about issues of responsibility" for bullying and cyberbullying, as well as "frustration around … the issue of school staff being required and expected to deal with a problem that often arose outside of school."[244] The most recent guidelines for teachers merely state that "[t]here are no hard and fast rules about the extent of schools' responsibility for bullying that occurs off school premises" but that when it is reported, it should be acted on.[245]

Overall, the Victoria University research indicates that incorporating school's responsibilities to address bullying into NAG 5 is necessary, and would be supported by most school staff. This obligation should be linked to an obligation to provide meaningful education about bullying to teachers and parents, clarifying the role of each and enabling cooperation between parents and teachers when issues about bullying arise.

In Australia, the National Safe Schools Framework requires all schools to have a bullying policy, and provides the resources to enable this.[246] As a result in comparison to school anti-bullying policies in Victoria, New Zealand policies lack inclusive definitions of bullying behaviour, are less likely to state what students and parents should do if they or their child are being bullied, and rarely mention how the school will investigate incidents reported to it.[247] Australian research has suggested that "NZ schools may benefit from Ministry of Education provision of clear guidelines on how to develop effective polices and what the minimum standard should be for these policies".[248]

A comprehensive educational programme is likely to significantly reduce the occurrence of cyberbullying, and should be implemented alongside an

[243] At 7.
[244] At 10.
[245] Bullying Prevention Advisory Group, above n 53, at [19.4]
[246] Louise Marsh and others "Content analysis of school anti-bullying policies: a comparison between New Zealand and Victoria, Australia" (2011) 22(3) Health Promotion Journal of Australia 172 at 173.
[247] At 175-176.
[248] At 176.

amendment to NAG 5 requiring schools to create anti-bullying policies, monitor incidents and educate parents and teachers about bullying. Clarifying the educational and monitoring roles of the Approved Agency is also important to the effectiveness of an educational campaign. If the Bill makes it clear that the Agency's educational function extends beyond advising on policy, the Agency could lead anti-bullying programmes and the monitoring of bullying incidents in workplaces, and work with schools to implement the changes to NAG 5.

E. Does the Bill create inappropriately asymmetrical law?

Many submitters on the Bill questioned why cyberbullying should be criminalised while non-digital bullying is not. For example, Microsoft argued that in an offline context, a false allegation alone does not create liability, but "under communication principle 6 … a false allegation that causes "harm" … can attract sanctions."[249] One response to this argument is that the unique features of digital communications create levels of harm not present in non-digital communications. The Justice and Electoral Select Committee emphasises this reasoning in its report on the Bill, noting that "technology has made possible the rapid, anonymous distribution" of information "to a potentially huge audience."[250]

However when considering whether the unique features of digital communications justify treating them differently to non-digital communications, Tokunaga's finding that the targets of cyberbullying are also subject to traditional bullying must be acknowledged.[251] Fenaughty has also found that among young people, "nearly half of the participants who were cyberbullied … also experience face-to-face bullying from these people at school."[252] An Australian study of bullying in the workplace found that 34 per cent of

[249] Microsoft "Submission to the Justice and Electoral Select Committee on the Harmful Digital Communications Bill 2013" at 3. See communication principle 6 in Appendix B.
[250] Harmful Digital Communications Bill 2013 (168-2) (explanatory note) at 1.
[251] Tokunaga, above n 13, at 279.
[252] Fenaughty, above n 11, at 189 links this to the NAG 5 responsibility of schools to provide a safe and supportive environment, questioning whether this is being achieved.

participants reported being bullied, and those who were cyberbullied were also bullied face-to-face.[253] Finally, both Fenaughty and Ybarra et al have found that young people who are targeted by multiple forms of bullying are more likely to suffer distress than those who are just subject to cyberbullying.[254]

This research suggests that the line drawn by the Bill between digital and non-digital communications is arbitrary, as most targets will experience both forms of bullying and it is this combination that causes the most harm. Looking overseas, the Malicious Communications Act (UK) does not distinguish between online and offline communications. While s 127 of the Communications Act (UK) and s 474.17 Criminal Code Act (Australia) are confined to electronic or electromagnetic communications,[255] this is because both provisions are designed to protect society from the abuse of a specific service, while the Malicious Communications Act (UK) addresses harm caused to individuals.[256] Although the Bill does aim to protect society in general from harmful digital communications, cl 3 states that harm caused to individuals is the Bill's primary focus. This is better achieved by focusing on the content of the communication rather than the means by which it was communicated.

The most contentious aspect of extending the Bill to cover non-digital communications is extending the cl 19 offence to face-to-face verbal communications. The Malicious Communications Act (UK) does not apply to face-to-face communications, but this can be attributed to the fact that it was originally designed to criminalise poison pen letters, and has merely been updated to include their modern equivalent – written digital communications. However in Sweden, schools are held legally accountable at civil law for failing to

---

[253] Privitera and Campbell, above n 2, at 398.
[254] Fenaughty, above n 11, at 190, Ybarra, Diener-West and Leaf, above n 40, at s45.
[255] Section 127 Communications Act (UK) is confined to matter sent "by means of a public electronic communications network," while the Criminal Code Act (Australia), s 474.17 criminalises the improper use of a "carriage service," which is defined as a service that carries communications by means of electromagnetic energy: Telecommunications Act (Australia), s 7.
[256] *Director of Public Prosecutions v Collins*, above n 194, at [7].

prevent or address serious bullying, which includes face-to-face and cyberbullying.[257]

Practically, if the Bill were extended this far, a large percentage of face-to-face bullying would not create the degree of harm required to trigger the application of the offence. Including verbal communications in the Bill would simply formally recognise the impact that such communications can have, and encourage people to seek mediation from the Approved Agency. However, if the required level of harm can be proved, research shows that there is no reason why the offence should be confined to the digital sphere.

[257] Act Prohibiting Discrimination and Other Degrading Treatment of Children and School Students (2006:67) (Sweden), s 15. See also "Swedish student settles bullying with city" (2 July 2014) The Local <www.thelocal.se>.

Conclusion

The aim of this dissertation was to assess first, whether cyberbullying is currently illegal, second, the effect and effectiveness of the Harmful Digital Communications Bill, and third, whether there are alternatives to criminalising cyberbullying. After considering New Zealand's current civil and criminal law, it is clear that some aspects of cyberbullying are already illegal. However there are currently no orders that can require material that is not private or defamatory to be removed from the Internet, and Acts like the Privacy Act and Harassment Act are an uncomfortable fit with the characteristics of digital communications. New Zealand also has no provisions criminalising the unauthorised publication of private pictures taken with the consent of the subject, or communications that do not threaten violence or involve indecency, intimidation or blackmail, but nonetheless cause their recipients harm.

The HDC Bill's three-stage proposal to address these gaps in the law has the advantage of a clear structure, but the content of the Bill requires amendment. The monitoring and educational functions of the Approved Agency need to be specifically identified. Although the choice of the District Court, rather than a Tribunal, to administer the orders is questionable, to enable the efficient administration of the orders in the District Court the Agency should be given a stronger 'gatekeeper' role. The District Court orders themselves require amendment to achieve consistency between cl 10 and cl 11, and also need defences that coordinate with those in the Defamation Act to prevent the orders being used to censor material that the Defamation Act would allow to be published. The Bill also proposes a new criminal offence in cl 19 of "causing harm by posting digital communication." Significant flaws in offence require it to be redrafted, including the requirement in cl 19(1)(c) that the victim suffer actual harm and the vague definition of "harm" in cl 4 on which cl 19 relies.

Taking a wider view, the Bill's assumption that digital communications cause more harm than non-digital communications is not supported by evidence. Rather, research indicates that the most severe distress occurs when digital and

non-digital bullying behaviours are combined. This suggests that the scope of the Bill should be widened to include *all* forms of harmful communications. It is also clear that the Bill's attempts to reduce cyberbullying will be greatly aided by an amendment to NAG 5 requiring schools to implement an effective education campaign that involves teachers, students and parents. Clarification of the Approved Agency's educational role would allow the Agency to work in cooperation with schools and to promote education about bullying in society in general.

The third aspect of my research was directed towards whether cyberbullying should be criminalised. Bullying and cyberbullying cause significant problems in society, affecting the mental and physical health of targets, creating barriers to learning and impacting the productivity and reputation of workplaces. Although service providers argue self-regulation can resolve these problems, the Australian experience of working with service providers under the Protocol indicates self-regulation cannot be relied on to the exclusion of a legislative solution. The most effective means of reducing all forms of bullying will be to use the Approved Agency proposed in the HDC Bill to coordinate self-regulation and an effective anti-bullying education campaign, while retaining the District Court orders and new offence as tools to use in the most serious cases.

The HDC Bill in its current form is likely to encounter numerous problems, particularly in relation to the District Court orders and the new offence of "causing harm by posting a digital communication" in cl 19. However if the Bill is amended as I have suggested above and implemented alongside changes to NAG 5, it has the potential to reduce not only cyberbullying, but also bullying in general. In a context where we are gaining insight into the severe consequences of bullying, and where as a society we are increasingly intolerant of all kinds of violence, the HDC Bill provides an opportunity for lawmakers to make a positive change to New Zealand's culture.

Bibliography

A. Cases

i. New Zealand

APN New Zealand Ltd v Simunovich Fisheries Ltd [2009] NZSC 93, [2010] 1 NZLR 315.

Attorney-General v Gilbert [2002] 2 NZLR 342 (CA).

Brown v Sperling [2012] DCR 753 (DC).

C v Holland [2012] NZHC 2155, [2012] 3 NZLR 672.

Fenandos v Police HC Auckland CRI-2010-404-280, 12 November 2010.

George v Police [2014] NZHC 1725.

Hosking v Runting [2005] 1 NZLR 1 (CA).

Karam v Parker [2014] NZHC 737.

L v G [2002] DCR 234 (DC).

McLachlan v Police HC Auckland CRI-2010-404-106, 29 June 2010.

MJF v Sperling [2013] NZFLR 715.

New Zealand Police v Beange DC Dunedin CRI-2012-012-003856, 3 May 2013.

R v Bailey [2012] NZHC 1276.

R v Broekman [2012] NZCA 213.

R v D [2000] 2 NZLR 641 (CA).

R v Hutton HC Hamilton CRI-2005-419-379, 20 May 2005.

R v Pengelly [2013] NZHC 527.

Simunovich Fisheries Ltd v Television New Zealand Ltd [2008] NZCA 350.

T (CA662/2012) v R [2013] NZCA 550.

Trower v R [2011] NZCA 653.

Winter v Jans HC Hamilton CIV-2003-419-854, 6 April 2004.

Wishart v Murray [2013] NZHC 540, [2013] 3 NZLR 246.

ii. Australia

Agostino v Cleaves [2010] ACTSC 19.

iii. United Kingdom

Blunt v Tilley [2006] EWHC 407 (QB), [2007] 1 WLR 1243.

Byrne v Deane [1937] 1 KB 818.

Chambers v Director of Public Prosecutions [2012] EWHC 2157 (Admin), [2013] 1 WLR 1833.

Director of Public Prosecutions v Collins [2006] UKHL 40, [2006] 1 WLR 2223.

Metropolitan International Schools Ltd v Designtechnica Corporation [2009] EWHC 1765 (QB), [2011] 1 WLR 1743.

Wainwright v Home Office [2003] UKHL 53, [2004] 2 AC 406.

Wilkinson v Downton [1897] 2 QB 57.

B. Legislation

i. New Zealand

Broadcasting Act 1989.

Children, Young Persons and Their Families Act 1989.

Crimes Act 1961.

Crimes (Substituted Section 59) Amendment Act 2007.

Defamation Act 1992.

Education Act 1989.

Films, Videos and Publications Classification Act 1993.

Harassment Act 1997.

Health and Safety in Employment Act 1992.

New Zealand Bill Of Rights Act 1990.

Privacy Act 1993.

Telecommunications Act 2001.

Harmful Digital Communications Bill 2013 (168-1).

Harmful Digital Communications Bill 2013 (168-2).

ii. Australia

Criminal Code Act 1995.

Telecommunications Act 1997.

iii. Sweden

Act Prohibiting Discrimination and Other Degrading Treatment of Children and School Students (2006:67).

iv. United Kingdom

Communications Act 2003.

Malicious Communications Act 1988.

School Standards and Framework Act 1998.
Telecommunications Act 1984.

C. International Conventions

United Nations Convention on the Rights of the Child (opened for signature 20 November 1989, entered into force 2 September 1990).

The Council of Europe Convention on Cybercrime (opened for signature 23 November 2001) [The Budapest Convention].

D. Journal articles

Sally Adams "Cyberbullying: An emerging form of student aggression for the 'always-on' generation" (2007) 2 The Australian Educational Leader 16.

Sally Boyd *"Wellbeing@School: Building a safe and caring school climate that deters bullying. Overview paper"* (2012) New Zealand Council for Educational Research.

Des Butler, Sally Kift and Marilyn Campbell "Cyber Bullying In Schools and the Law: Is There an Effective Means of Addressing the Power Imbalance?" (2009) 16(1) Murdoch University Electronic Journal of Law 84.

Marilyn A Campbell "Cyberbullying: An Old Problem in a New Guise?" (2005) 15(1) Australian Journal of Guidance and Counselling 68.

Carolyn Coggan, Sara Bennett, Rhonda Hooper and Pauline Dickinson "Association between Bullying and Mental Health Status in New Zealand Adolescents" (2003) 5(1) International Journal of Mental Health Promotion 16.

Sameer Hinduja and Justin W. Patchin "Bullying, Cyberbullying and Suicide" (2010) 14(3) Archives of Suicide Research 206.

Magdalena Marczak and Iain Coyne "Cyberbullying at School: Good Practice and Legal Aspects in the United Kingdom" (2010) 20(2) Australian Journal of Guidance & Counselling 182.

Louise Marsh, Rob McGee, Sheryl A Hemphill and Sheila Williams "Content analysis of school anti-bullying policies: a comparison between New Zealand and Victoria, Australia" (2011) 22(3) Health Promotion Journal of Australia 172.

Justin W. Patchin and Sameer Hinduja "Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying" (2006) 4 Youth Violence and Juvenile Justice 148.

Carmel Privitera and Marilyn Anne Campbell "Cyberbullying: The New Face of Workplace Bullying" (2009) 12(4) CyberPsychology & Behaviour 395.

Paul Roth "Data Protection Meets Web 2.0: Two Ships Passing in the Night" (2010) 33(2) UNSW Law Journal 532.

Russell A. Sabella, Justin W. Patchin and Sameer Hinduja "Cyberbullying myths and realities" (2013) 29 Computers in Human Behaviour 2703.

Robert Slonje, Peter K. Smith and Ann Frisén "The nature of cyberbullying, and strategies for prevention" (2013) 29 Computers in Human Behaviour 26.

Robert S. Tokunaga "Following you home from school: A critical review and synthesis of research on cyberbullying victimization" (2010) 26 Computers in Human Behaviour 277.

Michele L. Ybarra, Marie Diener-West and Philip J. Leaf "Examining the Overlap in Internet Harassment and School Bullying: Implications for School Intervention (2007) 41 Journal of Adolescent Health s42.

E. Parliamentary, Law Commission and government materials

i. New Zealand

Bullying Prevention Advisory Group "Bullying prevention and response: A guide for schools" (Ministry of Education, 2014).

Cabinet Social Policy Committee Paper "Harmful Digital Communications" (April 2013).

Clare Curran MP, First Reading of the Harmful Digital Communications Bill 2013 (3 December 2013) 695 NZPD 15164.

Gareth Hughes MP, First Reading of the Harmful Digital Communications Bill 2013 (3 December 2013) 695 NZPD 15164.

Law Commission *Harmful Digital Communications: The adequacy of the current sanctions and remedies* (Ministerial Briefing Paper, 2012).

Law Commission *The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age* (NZLC IP27, 2011).

Submission by the New Zealand Human Rights Commission: Consideration of New Zealand's third periodic report on the implementation of the International Covenant on Economic, Social and Cultural Rights (New Zealand Human Rights, March 2012).

ii. UK

House of Commons Culture, Media and Sport Committee *Online safety: Responses to the Committee's Sixth Report of Session 2013-14, First Special Report of Session 2014-15* (House of Commons, 1 July 2014).

House of Lords Select Committee on Communications *Social media and criminal offences* (House of Lords, HL Paper 37, July 2014).

United Kingdom Law Commission *Report on Poison Pen Letters* (Law Com. No. 147, 1985).

F. Submissions

i. New Zealand

Auckland District Law Society "Submission to the Justice and Electoral Committee on the Harmful Digital communications Bill 2013."

Facebook "Submission to the Justice and Electoral Committee on the Harmful Digital Communications Bill 2013."

Google "Submission to the Justice and Electoral Committee on the Harmful Digital Communications Bill 2013."

Human Rights Commission "Submission to the Justice and Electoral Committee on the Harmful Digital Communications Bill 2013."

Internet Party, "Submission to the Justice and Electoral Select Committee on the Harmful Digital Communications Bill 2013."

Microsoft "Submission to the Justice and Electoral Select Committee on the Harmful Digital Communications Bill 2013."

NetSafe "Submission to the Justice and Electoral Select Committee on the Harmful Digital Communications Bill 2013."

New Zealand Police "Submission to the Justice and Electoral Select Committee on the Harmful Digital Communications Bill 2013."

Tech Liberty "Submission to the Justice and Electoral Select Committee on the Harmful Digital Communications Bill 2013."

Telecom "Submission to the Justice and Electoral Select Committee on the Harmful Digital Communication Bill 2013."

The Judges of the District Courts "Submission to the Justice and Electoral Committee on the Harmful Digital Communications Bill 2013."

Vodafone "Submission to the Justice and Electoral Select Committee on the Harmful Digital Communication Bill 2013."

Youthline Otago "Submission to the Justice and Electoral Committee on the Harmful Digital Communications Bill 2013."

ii. Australia

Australian Federal Police "Submission to the Government's Discussion Paper on Enhancing Online Safety for Children 2014."

Australian Law Council "Submission to the Government's Discussion Paper on Enhancing Online Safety for Children 2014."

G. Reports and theses

i. New Zealand

John Fenaughty "Challenging Risk: NZ High-school Students' Activity, Challenge, Distress, and Resiliency, within Cyberspace" (PhD Thesis, University of Auckland, 2010).

Vanessa A. Green, Susan Harcourt, Loreto Mattioni and Tessa Prior "Bullying in New Zealand Schools: A Final Report" (Victoria University of Wellington, 2013).

Report of David McGee, Ombudsman on Complaints Arising out of Bullying at Hutt Valley High school in December 2007 (2011).

The Prime Minister's Chief Science Advisor *Improving the Transition: Reducing Social and Psychological Morbidity During Adolescence* (Office of the Prime Minister's Science Advisory Committee, May 2011).

ii. Australia

Enhancing Online Safety for Children: Public consultation on key election commitments (Australian Government Department of Communications, January 2014).

Ilan Katz, Matthew Keeley, Barbara Spears, Carmel Taddeo, Teresa Swirski and Shona Bates *Research on youth exposure to, and management of, cyberbullying incidents in Australia: Synthesis report* (Australian Government Department of Communications, June 2014).

Matthew Keeley, Ilan Katz, Shona Bates and Melissa Wong *Research on youth exposure to, and management of, cyberbullying incidents in Australia. Part B: cyberbullying incidents involving Australian minors, the nature of the incidents and how they are currently being dealt with (SPRC Report 10/2014)* (Australian Government Department of Communications, June 2014).

Barbara Spears, Matthew Keeley, Tony Daly, Carmel Taddeo, Ilan Katz, Teresa Swirski, Philippa Collin and Shona Bates *Research on youth exposure to, and management of, cyberbullying incidents in Australia. Part C: An evidence-based assessment of deterrents to you cyberbullying - Appendix A (SPRC report 12/2014)* (Australian Government Department of Communications, June 2014).

iii. Canada

The Nova Scotia Task Force on Bullying and Cyberbullying *Respectful and Responsible Relationships: There's No App for That*. *The Report of the Nova Scotia Task Force on Bullying and Cyberbullying* (February 29 2012).

H. Newspaper articles

David Clarkson "Man in court over naked pic threats" *The Press* (online ed, Christchurch, 31 May 2012).

David Clarkson "Woman feared nude pics posted online" *The Press* (online ed, Christchurch, 25 August 2014).

"Man in BNP expose sent abusive text messages" *The Guardian* (online ed, London, 26 August 2004).

Myles Hume "Explicit page done 'out of respect'" *The Press* (online ed, Christchurch, 8 October 2014).

Rob Kidd "Man gets home detention for blackmailing partner into cleaning" *The New Zealand Herald* (online ed, Auckland, 30 September 2014).

Henry McDonald "Man charged over Ronan Kerr social network comments" *The Guardian* (online ed, London, 30 June 2011).

Simon O'Rourke "Teenage bullies hound 12-year-old to death" *New Zealand Herald* (online ed, Auckland, 11 March 2006).

Andrea Vance and Jody O'Callaghan "'Time's up' for cyber tormentors" *The Press* (online ed, Christchurch, 5 November 2013).

I. Internet resources

"Help & Support" 2Degrees <www.2degreesmobile.co.nz>.

Australian Government Department of Communications "Online Safety" <www.communications.gov.au>.

Lilian Edwards "Section 127 of the Communication Act 2003: Threat or Menace?" (September 2012) panGloss <www.blogscript.blogspot.co.uk>.

"Facebook Help Center" Facebook <www.facebook.com>.

Carolyn Gregoire "The Hunger Blogs: A secret world of teenage 'thinspiration'" (2 September 2012) The Huffington Post <http://www.huffingtonpost.com>.

Matthew Manarino "'Star Wars Kid' Ghyslain Raza Breaks 10-Year Silence In New Magazine Interview" (9 May 2013) New Media Rockstars <www.newmediarockstars.com>.

Ministry of Education "Positive behaviour for learning" <www.pb4l.tki.org.nz>.

Ministry of Education "Understanding bullying behaviours" <www.pb4l.tki.org.nz>.

Ministry of Education "Programmes and initiatives" <www.pb4l.tki.org.nz>.

NetSafe "About NetSafe" <www.netsafe.org.nz>.

Talia Shadwell "Top cop fronts over Roast Busters case" (11 December 2013) Stuff <www.stuff.co.nz>.

"Help" Spark <www.spark.co.nz>.

"Charlotte Dawson found dead" (22 February 2014) Stuff <www.stuff.co.nz>.

"Naked photo sends jilted lover to jail" (13 November 2010) Stuff <www.stuff.co.nz>.

The Crown Prosecution Service "Guidelines on prosecuting cases involving communications sent via social media" <www.cps.gov.uk>.

"Swedish student settles bullying with city" (2 July 2014) The Local <www.thelocal.se>.

"Twitter Help Center" Twitter <www.twitter.com>.

"Help Me" Vodafone <www.vodafone.co.nz>.

Appendix A: International legislation

A. UK legislation

Malicious Communications Act 1988

Section 1: Offence of sending letters etc with intent to cause distress or anxiety

(1) Any person who sends to another person—

(a) a letter, electronic communication or article of any description which conveys—

(i) a message which is indecent or grossly offensive;

(ii) a threat; or

(iii) information which is false and known or believed to be false by the sender; or

(b) any article or electronic communication which is, in whole or part, of an indecent or grossly offensive nature,

is guilty of an offence if his purpose, or one of his purposes, in sending it is that it should, so far as falling within paragraph (a) or (b) above, cause distress or anxiety to the recipient or to any other person to whom he intends that it or its contents or nature should be communicated.

(2) A person is not guilty of an offence by virtue of subsection (1)(a)(ii) above if he shows—

(a) that the threat was used to reinforce a demand made by him on reasonable grounds; and

(b) that he believed, and had reasonable grounds for believing, that the use of the threat was a proper means of reinforcing the demand.

(2A) In this section "electronic communication" includes—

(a) any oral or other communication by means of a telecommunication system (within the meaning of the Telecommunications Act 1984 (c. 12)); and

(b) any communication (however sent) that is in electronic form.

(2) In this section references to sending include references to delivering or transmitting and causing to be sent, delivered or transmitted and "sender" shall be construed accordingly.

(3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale, or to both.[258]

[258] Level 5 on the standard scale of fines is £5 000: s 37(2) Criminal Justice Act 1982 (UK)

Communications Act 2003

Section 127: Improper use of public electronic communications network

(1) A person is guilty of an offence if he—
   (a) sends by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or
   (b) causes any such message or matter to be so sent.

(2) A person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he—
   (a) sends by means of a public electronic communications network, a message that he knows to be false,
   (b) causes such a message to be sent; or
   (c) persistently makes use of a public electronic communications network.

(3) A person guilty of an offence under this section shall be liable, on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale, or to both.

(4) Subsections (1) and (2) do not apply to anything done in the course of providing a programme service (within the meaning of the Broadcasting Act 1990 (c. 42)).

B. Australian legislation

Criminal Code Act 1995

Section 474.17: Using a carriage service to menace, harass or cause offence

(1) A person is guilty of an offence if:
   (a) the person uses a carriage service; and
   (b) the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive.

   Penalty: Imprisonment for 3 years.

(2) Without limiting subsection (1), that subsection applies to menacing, harassing or causing offence to:
   (a) an employee of the NRS provider; or
   (b) an emergency call person; or
   (c) an employee of an emergency service organisation; or
   (d) an APS employee in the Attorney-General's Department acting as a National Security Hotline call taker.

Appendix B: Selected sections from the Harmful Digital Communications Bill

3 Purpose

The Purpose of this Act is to mitigate harm caused to individuals by digital communications and to provide victims of harmful digital communications with a quick and efficient means of redress.

4 Interpretation

In this Act, unless the context otherwise requires, -

…

harm means serious emotional distress

6 Communication principles

(1) The communication principles are –

Principle 1

A digital communication should not disclose sensitive personal facts about an individual.

Principle 2

A digital communication should not be threatening, intimidating, or menacing.

Principle 3

A digital communication should not be grossly offensive to a reasonable person in the complainant's position.

Principle 4

A digital communication should not be indecent or obscene.

Principle 5

A digital communication should not be part of a pattern of conduct that constitutes harassment.

Principle 6

A digital communication should not make false allegations.

Principle 7

A digital communication should not contain a matter that is published in breach of confidence.

Principle 8

A digital communication should not incite or encourage anyone to send a message to a person with the intention of causing harm to that person.

Principle 9
A digital communication should not incite or encourage another person to commit suicide.

Principle 10
A digital communication should not denigrate a person by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation, or disability.

(2) In performing functions or exercising powers under this Act, the Approved Agency and courts must –
- (a) take account of the communication principles; and
- (b) act consistently with the rights and freedoms contained in the New Zealand Bill of Rights Act 1990.

8 Functions and powers of Approved Agency

(1) The functions of the Approved Agency are –
- (a) to receive and assess complaints about harm caused to persons by digital communications:
- (b) to use negotiation, mediation, and persuasion (as appropriate) to resolve complaints:
- (c) to investigate complaints, unless the Agency considers that –
  - (i) the complaint is trivial, frivolous, or vexatious; or
  - (ii) the subject matter or nature of the complaint is unlikely to cause harm to any individual; or
  - (iii) investigating the subject matter or nature of the complaint is unlikely to uphold or enhance the communication principles:
- (d) to establish and maintain relationships with domestic and foreign service providers, online content hosts, and agencies (as appropriate) to achieve the purpose of this Act:
- (e) to provide education and advice on policies for online safety and conduct on the internet:
- (f) to perform other functions conferred on it by or under this Act, including functions prescribed by Order in Council made under **section 7.**

(2) The Agency may seek and receive any information that the Agency considers will assist it in the performance of its functions.

(3) The Agency may decide not to take any further action on a complain if, in the course of assessing or investigating the complaint, it appears to the Agency that, having regard to all the circumstances of the case, any further action is unnecessary or inappropriate.

10 Who may bring proceedings

(1) Any of the following may apply to a District Court for an order under **section 16 or 17**:
- (a) an individual who alleges that he or she has suffered harm as a result of a harmful digital communication:
- (b) a parent or guardian on behalf of a person described in **paragraph (a):**

(c) the principal of an educational establishment, if a student of that establishment is a person described in **paragraph (a)** and the student consents to the principal bringing the proceedings:
(d) the Police, if the digital communication constitutes a threat to the safety of any person.

(2) The chief coroner may apply for an order under **section 16 or 17(1)(a) or (b)** in respect of a digital communication that contravenes a provision of the Coroners Act 2006.

11 Threshold for proceedings

(1) A person to whom **section 10(1)(a), (b), or (c)** applies may not apply for an order under **section 16 or 17** in respect of a digital communication unless the Approved Agency has first considered a complaint about the communication and had a reasonable opportunity to consider and decide what action (if any) to take.

(2) In any case, a District Court must not grant an application from a person referred to in **section 19(1)(a) to (c)** for an order under **section 16 or 17** unless it is satisfied that –
(a) there has been a serious or repeated breach of 1 or more communication principles; and
(b) the breach has caused or is likely to cause harm to a person.

(3) The court may, on its own initiative, dismiss an application from a person to whom **section 10(1)(a), (b), or (c)** applies without a hearing if it considers that the application is frivolous or vexatious, or for any other reason does not meet the threshold in **subsection (2).**

19 Causing serious distress by posting a communication

(1) Any person commits an offence if –
(a) the person posts a communication with the intention that it cause harm to a victim; and
(b) posting the communication would cause harm to an ordinary reasonable person in the position of the victim; and
(c) posting the communication causes harm to the victim.

(2) In determining whether a post would cause harm, the court may take into account any factors it considers relevant, including -
(a) the extremity of the language used:
(b) the age and characteristics of the victim:
(c) whether the digital communication was anonymous:
(d) whether the digital communication was repeated:
(e) the extent of circulation of the digital communication:
(f) whether the digital communication is true or false:
(g) the context in which the digital communication appeared.

(3) A person who commits an offence against this section is liable to imprisonment for a term not exceeding 3 months or a fine not exceeding $2,000.

(4) In this section, -
intimate visual recording -
(a) means a visual recording (for example, a photograph, videotape, or digital image) that is made in any medium using any device with or

without the knowledge or consent of the person who is the subject of the recording, and that is of –

(i) a person who is in a place which, in the circumstances, would reasonably be expected to provide privacy, and that person is –

(A) naked or has his or her genitals, public area, buttocks, or female breasts exposed, partially exposed, or clad solely in undergarments; or

(B) engaged in an intimate sexual activity; or

(C) engaging in showering, toileting, or other personal bodily activity that involves dressing or undressing; or

(ii) a person's naked or undergarment-clad genitals, pubic area, buttocks, or female breasts which is made –

(A) from beneath or under a person's clothing; or

(B) through a person's outer clothing in circumstances where it is unreasonable to do so.

(b) includes an intimate visual recording that is made and transmitted in real time without retention or storage in -

(i) a physical form; or

(ii) an electronic form from which the recording is capable of being reproduced with or without the aid of any device or thing

posts a digital communication -

(a) means transfers, sends, posts, publishes, disseminates or otherwise communicates by means of a digital communication any information, whether truthful or untruthful, about the victim; and

(b) includes publishing an intimate visual recording of another person; and

(c) includes an attempt to do anything referred to in **paragraph (a) or (b)**

victim means the person who is the target of the conduct elicited by the posted digital communication.

20 Liability of online content host for content posted by user

(1) This section applies to the liability of an online content host for the content of a digital communication posted by a person and hosted by the online content host.

(2) No civil or criminal proceedings may be brought against the online content host in respect of the content complained of (the **specific content**) unless –

(a) the person who provides the specific content does so on behalf, or at the direction, of the online content host; or

(b) the online content host –

(i) receives a notice of complaint about the specific content; and

(ii) does not take reasonable steps as soon as is reasonably practicable to remove or disable access to the specific content.

(3) A notice of complaint must –

(a) specify the complainant's name; and

(b) set out the specific content, and explain why the complainant considers that –
  (i) the specific content is unlawful; or
  (ii) the specific content ought to be taken down or access to it be disabled because it is harmful or otherwise objectionable; and
(c) sufficiently enable the specific content to be readily located; and
(d) contain any other information that the complainant considers relevant.

(4) The Approved Agency may lodge a notice of complaint on behalf of a complainant and provide advice and assistance to the complainant in relation to the complaint.

(5) The protection conferred on an online content host by **subsection (2)** does not apply if the host does not provide an easily accessible mechanism that enables a user to contact the host about specific content as provided in **subsection 3**.

(6) Nothing in **subsection (2)** affects
(a) section 211 of the Criminal Procedure Act 2011; or
(b) section 19 of the Bail Act 2000; or
(c) copyright liability, or any proceedings, under the Copyright Act 1994; or
(d) any enactment that expressly overrides **subsection (2)**.

Appendix C: A draft new communications offence

19 Causing serious distress by transmitting a communication

(1) Any person commits an offence if –

(a) the person -

(i) transmits a communication with the intention that it cause serious distress to the recipient or any other person to whom he intends it be communicated; and

(ii) the communication would cause serious distress to a reasonable person in the position of the recipient or other person to whom he intends it be communicated; or

(b) the communication is injurious to the public good.

(2) In considering whether **subsection (1)(a)(ii)** is satisfied, the court must consider the following factors -

(a) the nature of the language used and the content of the communication (including but not limited to whether the language or content was obscene, indecent, grossly offensive, harassing, threatening, intimidating or menacing);

(b) whether the communication breaches general societal standards of acceptable communications;

(c) the age and characteristics of the sender and the recipient or people to whom the sender intended to communication to be communicated.

(d) whether the communication was anonymous or repeated;

(e) the extent of circulation of the communication;

(f) whether the communication was true or false;

(g) the context in which the communication appeared.

(3) A person who commits an offence against this section is liable to imprisonment for a term not exceeding 3 years.

(a) When determining the sentence to be imposed for a conviction under this section the court must take into account the characteristics of the offender, including their age and emotional maturity as well as their involvement either as a target or perpetrator of similar communications.

(4) In this section, "communication" includes but is not limited to written messages, video recordings, face-to-face conversations, pictures and intimate visual recordings.

(5) "Intimate visual recordings" are defined as:

(a) visual recordings (for example a photograph, videotape or digital image) that is made in any medium using any device with or without the knowledge or consent of the subject of the recording, and that is of –

(i) a person who is in a place which, in the circumstances, would reasonably be expected to provide privacy, and that person is –

(A) naked or has his or her genitals, public area, buttocks or female breasts exposed, partially exposed, or clad solely in undergarments; or
(B) engaged in an intimate sexual activity; or
(C) engaging in showering, toileting, or other personal bodily activity that involves dressing or undressing; or

(ii) a person's naked or undergarment-clad genitals, public area, buttocks or female breasts which is made –
(A) from beneath or under a person's clothing; or
(B) through a person's outer clothing in circumstances where it is unreasonable to do so.

(b) includes an intimate visual recording that is made and transmitted in real time without retention or storage in
(i) a physical form; or
(ii) an electronic form from which the recording is capable of being reproduced with or without the aid of any device or thing.

(6) "Transmits a communication"
(a) means transfers, sends, posts, publishes, disseminates, speaks or otherwise communicates any information on the internet, by post, by means of a digital communications service or through any other means, including face to face verbal communications;
(b) includes an attempt to do anything referred to in (a).

(7) A communication that would cause serious distress -
(a) does not include a communication that is merely in bad taste, is controversial or unpopular, or that may cause offence to certain individuals or communities; and
(b) does not include satire or rude humour.