CYBERSPACE, CYBERBULLYING, DUTY OF CARE: LEGAL AND EDUCATIONAL RESPONSES

CYBERSPACE, CYBERBULLYING, DUTY OF CARE: LEGAL AND EDUCATIONAL RESPONSES

Elizabeth Grierson
RMIT University
Australia & New Zealand[1]

The creative economies of information technologies open a new spatial runway for bullies to proliferate. The advent of social media brings unheralded opportunities for creative communications between parties in agreement, or about third parties without agreement. It is commonly understood that cyberbullying may have deleterious effects on victims, yet perpetrators are often emboldened in their behaviours by creative potentials of cyberspace.

'Cyberbullying' is the object of analysis in this paper. Attention is given to definitions and contexts of cyberbullying and its space of occurrence, the Internet and cyberspace. The paper then undertakes a jurisprudential analysis of cyberbullying laws in a range of locations, and considers institutional duty of care in an Australian example. Giving specific attention to cyberbullying in Australia and New Zealand, the paper concludes with some recommendations.

1 INTRODUCTION

1.1 The Paper

This paper considers the expanding opportunities for creative communications in the digital age, the corresponding opportunities for cyberbullying, and legal responses to it. So great is the open potential of cyber-communications through the creative impetus of text, sound and image-sharing networks and blogging platforms that cyberbullies are often encouraged by the anonymity cyberspace affords them.

This paper considers specific characteristics of cyberbullying in relation to an understanding of cyberspace and the Internet. It undertakes a jurisprudential analysis of cyberbullying legislation and case law, then turns to the overarching duty of care an institution owes its employees in cyber abuse situations.

The overall aim is to raise awareness of the current legal landscape regarding cyberbullying, particularly in Australia and New Zealand. The paper concludes with findings and recommendations.

1.2 Focus and Background

In presenting this paper, my focus comes from experience in education and law. My specialist area of university education is in the creative arts field, which brings a focus to philosophies, politics and practices of creativity and culture. The advent of Internet has brought unheralded opportunities for creativity—and cyberbullying—to flourish.

[1] Contacts: <griersonlaw@gmail.com> <elizabeth.grierson@rmit.edu.au> Professor, RMIT University Melbourne Australia, Adjunct Professor, AUT University NZ.

1.3 Building on Research

This paper grows out of research focusing on cyberspace and issues of identity in 2001;[2] and legal approaches to cyberstalking for the 2012 ANZELA Conference.[3] In 2015, the research was extended in a project on policy and legal responses to cyberbullying and cyberstalking in Australia and New Zealand; updated in 2016 for this present paper.

2 CONTEXT: THE INTERNET

2.1 The Internet

The advent of the Internet has brought new offences to the table of law and education.

Through the Internet the digital economy is transforming the everyday, social, educational, economic and political lives of pre-1980s 'digital immigrants',[4] while furnishing a new world order for post-1980s 'digital natives'.[5] The latter have in hand a lifelong use of the Internet as a normal part of everyday lives; they use the Internet for learning in schools, communicating with friends, playing games, inventing ideas, and social networking.

As 'the worldwide interconnection of individual networks'[6] the Internet derives from *inter*-connected *net*-works.[7] It has a relatively short life in historical time; cyberbullying even shorter. The Internet's speed of growth is a magnet for economic and social interests; it offers a scale of connectivity unparalleled in human endeavour.[8] Cyberbullying is growing at a corresponding rate.

A discernment of this economy assists in understanding the ubiquitous operations of online communications, and the ever-expanding opportunities for creative enterprise, and for online offences.

2.2 Growth of Capacity

(1) Globally, in 2016, there are approximately 3.9billion Internet users (a 33% increase since 2015), profoundly changing the way we live, learn and do business.[9]

(2) In was only 27-years ago, in 1989, that the IP-based network was established in Australia and New Zealand.

---

2 Elizabeth Grierson, 'From Cemeteries to Cyberspace: Cartographies of Identity in a Technologised Age' (2001) 20 *ACCESS Critical Perspectives on Communication, Cultural & Policy Studies* 2, 11.

3 Elizabeth Grierson, 'Cyberspace, Cyberbullying, Cyberstalking: New Challenges in Law and Education' in Alan Knowsley (ed) *Proceedings of the 21st Annual ANZELA Conference 2012 - Woteva nxt! Legal and Social Challenges in Education* (Wellington, New Zealand 3-5 October 2012) 1.

4 'Digital immigrants' includes 'Generation X' and their parents known as 'Baby Boomers' born at end of World War II; descriptors from popular usage are not scientifically determined.

5 'Digital natives' are known by the interchangeable terms 'Net Generation' or 'Generation Y'. Marc Prensky, 'Digital Natives, Digital Immigrants' (2001) 9 *On the Horizon* 1.

6 'Internet World Stats', <http://www.internetworldstats.com/emarketing.htm >. Accessed 9 December 2014.

7 Bela Bonita Chatterjee, 'The Last of the Rainmacs: Thinking about Pornography in Cyberspace' in David S Wall (ed), *Crime and the Internet* (Routledge, 2004) 74.

8 For history and growth of Internet see: Merriam-Webster Dictionary; Internet Society <http://www.internetsociety.org >; K Hafner and M Lyon, *Where Wizards Stay up Late* (Simon and Schuster, 1996); Nicholas Negroponte, *Being Digital* (Vintage Books, 1995); Stein Schjølberg, *The History of Cybercrime: 1976-2014* (Kindle e-book, 2014).

9 Internet Live Stats, 'Internet Users', < http://www.internetlivestats.com/internet-users/ >. Accessed 1 September 2016.

(3) In 1991, the advent of 'pull' technology appeared as the World Wide Web,[10] followed by other network browsers. This opened a vast potential for information gathering. From this moment on, there was an exponential growth in capacity and opportunity for creative enterprise and commercial interests.

(4) 14-years ago, in 2002, second-generation interactivity, known as Web 2.0, opened up social networking possibilities of content sharing in user-generated sites. This gave unheralded creative opportunities for interactive conversations and communications.

(5) In 2004, with the launch of Facebook,[11] individuals and groups could network as never before by posting messages, videos and images.[12] Other social networking sites soon flourished: Bebo, Blogs, Flickr, Instagram, Instant Messages (IM), LinkedIn, Multimedia Messages (MMS), Myspace, Smart-phones, Snapchat, Snapfish, Streetchat, Text messaging (SMS), Tinder, Tumblr, Twitter, YouTube, WhatsApp, with more appearing almost by the day.[13] Information sharing became almost instantaneous as virtual, self-forming communities took effect.

(6) Web-3.0 is heralded as a Web culture of heightened intelligence. With capacities for data-mining, convergence, cryptography and automated reasoning, the semantic-Web is transforming human communication, thought and reason. Here lies the theatre for enactment of intentional, harmful, digital communications, known as cyberbullying.

2.3 Internet Usage and Cyberbullying

The global statistics show uneven distribution in the usage and rates of Internet growth and occurrence of cyber offences.[14]

(1) *New Zealand* Internet usage: there are over 4million Internet users in a population of 4.7million, with 89.4% penetration of population, and a plan to bring broadband to 97.8% of the population by 2019. *Cyberbullying* occurrence: research shows two in five children have been victims of online bullies, three in five teenagers, women aged 18 to 19 reporting the highest incidence, and one in 10 people between 30 to 59.[15]

(2) *Australia* Internet usage: an 85% penetration with 20million users, similar percentages to *NZ* and *USA*. *Cyberbullying* occurrence similar to New Zealand; although for children results vary, from one in 10 children, to one in five, and as high as one in two in some studies.[16]

---

10 WWW is one of many services via Internet; pages of information are written in HTML code.

11 Founded by Mark Zuckerburg and fellow students at Harvard University, in 2004.

12 'Internet access can now be gained via radio signals, cable-television lines, satellites, and fibre-optic connections, though most traffic still uses a part of the public telecommunications (telephone) network'. Merriam-Webster Dictionary and Encyclopedia online, <http://www.merriam-webster.com/dictionary/internet >. Accessed 1 February 2015.

13 For legal issues in social networking sites, Margaret Jackson and Marita Shelly, *Electronic Information and the Law* (Thomson Reuters, 2012).

14 The percentage figures in this section come from Internet Live Stats, 'Internet users by Country 2016', < http://www.internetlivestats.com/internet-users-by-country/>. Accessed 6 September 2016.

15 Jamie Morton, 'Rates of cyberbullying in New Zealand alarming', in *New Zealand Herald* Monday (28 March 2016) <http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11612551>. Accessed 1 September 2016.

16 NoBullying.com, 'Cyberbullying Statistics Australia, the Ultimate Guide' (22 December 2015) <https://nobullying.com/cyber-bullying-statistics-australia-the-ultimate-guide/>. Accessed 1 September 2015.

(3) *European countries* reveal similar percentages as Australia, NZ and USA, and similar patterns of cyber abuse; although Scandinavian countries evidence a higher percentage of Internet penetration, 92% to 98%.

(4) *Japan* and *UK* Internet usage: a 91% penetration of 115million users for Japan, and 92.6% for UK, with 60million users; *Russia* 72.0% penetration.

(5) *China*: 52.2% penetration with 721million users in 1.4billion population. *India* has low penetration at 34.8% of 1.3billion population; *Singapore* high usage at 82.5%. *Cyberbullying* occurrence is high in each of these countries according to a survey by Microsoft Corporation.[17]

(6) *South America* reveals Internet usage to be between 40% (Peru) and 77.8% (Chile). *Cyberbullying* occurrence varies accordingly.

(7) *Africa*: Not unsurprising, statistics for Internet usage and *cyberbullying* vary considerably. One research (by Vodafone) found South Africa was the fourth highest for cyberbullying after New Zealand, USA and Ireland.[18] For countries such as Democratic Republic of Congo with 3.9% penetration, Sierra Leone with 2.4%, or Somalia 1.7%, cyberbullying statistics are rarely reported.[19]

3 CYBERBULLYING

3.1 Cyberbullying Defined

The term *cyberbullying* is relatively new and definitions vary. One of the key problems in definitional terms is whether cyberbullying is simply an extension of offline bullying, or whether it has its own characteristics from networked communications in cyberspace.

(1) *The OECD* defines cyberbullying as an extension of offline bullying, but draws attention to its *endless spatial capacity*. 'It is a lot meaner and more vindictive that traditional forms of bullying … Cyberbullies are able to enter the homes of victims, the one safe ground where victims were able to shelter in the past'.[20]

(2) *The US Department of Human Services* defines cyberbullying as 'bullying that takes place using electronic technology…'. It can happen 24-hours, 7-days a week; 'messages and images can be posted anonymously and distributed quickly to a very wide audience. It can be difficult and sometimes impossible to trace the source' and 'deleting inappropriate or harassing messages, texts, and pictures is extremely difficult after they have been posted or sent'. [21]

[17] End to Cyberbullying Organization, 'India Ranks Third on Global Cyber Bullying list', <http://www.endcyberbullying.org/india-ranks-third-on-global-cyber-bullying-list/>. Accessed 7 September 2016.

[18] Paula Gilbert, 'One in five SA teens cyber bullied', Web Wireless (23 September 2015) < http://www.itweb.co.za/index.php?option=com_content&view=article&id=146442>. Accessed 3 September 2016.

[19] Internet Live Stats, above n 14, Accessed 28 August 2016.

[20] OECD Centre for Educational Research and Innovation CERI, New Millenium Learners Blog 'Cyber bullying', <https://www.oecd.org/edu/ceri/centreforeducationalresearchandinnovationceri-thenewmilleniumlearnersblog.htm>. Accessed 4 September 2016.

[21] US Department of Human Services, 'What is Bullying', < http://www.stopbullying.gov/what-is-bullying/definition/index.html >. Accessed 7 September 2016.

(3) *The US legal definition* online extends from technologies to types of posting: 'Communications technology is used to intentionally harm others through hostile behavior such as sending text messages and *posting ugly comments* on the internet'.[22]

(4) The *US National Crime Prevention Council* defines cyberbullying as sending messages or images that are mean, threatening, embarrassing, cruel, untrue.[23]

(5) *The Australian Human Rights Commission* includes effects of cyberbullying, as 'bullying that is done through the use of technology … It can be *shared widely with a lot of people quickly*, which is why it is so *dangerous and hurtful*'.[24]

(6) *New Zealand NetSafe* definition is similar to the Australian, with emphasis on the spatial and temporal reach, *attacking victims at any time of day or night*.[25]

(7) *Sexting*: sending nude or sexual images through mobile phones or Internet may be classed as a form of cyberbullying, if non-consensual. The considerable problem for those under 18-years, is that it attracts criminal offences and penalties.[26]

3.2 What Differences from Bullying?

(1) No Differences

(i) Dan Olweus,[27] one of the foremost US experts on bullying from a psychological perspective argues that there is no specific difference between bullying and cyberbullying.[28] He positions bullying as repeated harmful acts with imbalance of power, conducted with malice and with intent to inflict harm. It becomes cyberbullying when electronic means of communication are used intentionally and repeatedly to aggress a victim.

(ii) The *Australian National Safe Schools Framework* positions cyberbullying in schools as bullying through the Internet or mobile devices.[29] The multiplication effect of cyberbullying is not included, yet it is a crucial characteristic.

---

22 US Legal Definitions, < http://definitions.uslegal.com/c/cyber-bullying/>. Accessed 3 September 2016.

23 NCPC 2016, 'What is Cyberbullying?' <http://www.ncpc.org/topics/cyberbullying/what-is-cyberbullying>. Accessed 7 September 2016.

24 Australian Human Rights Commission, 'Cyberbullying: what is it and how to get help. Violence, Harassment and Bullying Fact sheet, <https://www.humanrights.gov.au/cyberbullying-what-it-and-how-get-help-violence-harassment-and-bullying-fact-sheet>. Accessed 5 September 2016.

25 Netsafe Cyberbullying, <http://www.cyberbullying.org.nz/>. Accessed 5 September 2016.

26 FindLaw Team, 'Sexting' and Australian Law, FindLaw Australia, <http://www.findlaw.com.au/articles/4720/sexting-and-australian-law.aspx>. Accessed 3 September 2016; Parliament of Victoria, Law Reform Committee, Inquiry into Sexting, Final Report May 2013 <http://www.parliament.vic.gov.au/lawreform/article/944 >. Accessed 8 September 2016.

27 Known for empirical research on bullying; the Olweus Bullying Prevention Program for Schools.

28 Dan Olweus, 'Cyberbullying: An Overrated Phenomenon?' (2012) 9 *European Journal of Developmental Psychology* 5, 1; Dan Olweus, 'Comments on Cyberbullying Article: A Rejoinder' (2012) 9 *European Journal of Developmental Psychology* 5, 559; Dan Olweus and Susan P Limber, 'Bullying in School: Evaluation and Dissemination of the Olweus Bullying Prevention Program' (2010) 80 *American Journal of Orthpsychiatry* 1, 124.

29 Australian Standing Council on School Education and Early Childhood Development (SCSEEC), *National Safe Schools Framework* 2011, Emphasis added. <http://www.safeschoolshub.edu.au/documents/nationalsafeschoolsframework.pdf >. Accessed 6 September 2016.

(2) Differences

(i) *New Zealand Law Commission* Ministerial Briefing Paper positions cyberbullying as a specific variant.[30] It details harmful communications or cyberbullying as taking a variety of forms and occurring in a range of *digital mediums with a viral nature*; they may be used to intimidate, damage reputations, spread rumours, publish distressing images, and harass others. They are persistent and offer anonymity; content is easy to create and difficult to remove.[31]

The Commission differentiates cyberbullying by its *capacity* and *effect*. 'The distinguishing feature of electronic communication is that it has the *capacity to spread beyond the original sender and recipient*, and *envelop the recipient* in an environment that is *pervasive, insidious and distressing*'.[32]

(ii) Julian Dooley from an Australian law research centre takes account of the specific nature of online bullying.[33] Just *one instance* may comprise cyberbullying as, by the very nature of cyberspace postings, one message has the *potential to multiply in time and place* with online viewing by multiple networked viewers: the harmful effects on the victim multiply accordingly.

The multiplication effect was referred to in the judgement of *Police v Ravshan Usmanov*.[34] This may indicate Australian courts are working towards differentiating cyberbullying from offline bullying.

(iii) The Australian policy to combat cybercrime references judicial approaches: '[P]rosecutors and judges will increasingly be required to present and understand highly technical details in order to effectively administer the law'.[35]

Such understanding requires knowledge of advancement of electronic technologies, the Internet's capacities, and particular characteristics of data-sharing and networked communications in cyberspace.

From the above, it seems there is more weight to the argument that cyberbullying does have specific characteristics, which differentiate it from face-to-face bullying.

---

30 New Zealand Law Commission, Ministerial Briefing Paper, *Harmful Digital Communications: The Adequacy of the Current Sanctions and Remedies* (August 2012).

31 Ibid.

32 Ibid 17. Emphasis added.

33 Sellenger Centre for Research in Law, Justice, and Social Change, Edith Cowan University, Australia, < http://www.ecu.edu.au/research/research-showcase/>. Accessed 1 February 2015.

34 *Police v Ravshan Usmanov* [2011] NSWLC 40. (See further discussion in Case Law, this paper).

35 Australia Government, Attorney-General's Department, *National Plan to Combat Cybercrime* (Commonwealth of Australia, 2013) 21.

3.3 Effects of Cyberbullying

Cyberbullying can have devastating effects. The National Children and Youth Law Centre (NCYLC) project finds, 'Victims of cyber bullying are more likely than non-victims to experience impaired social and emotional adjustment, poor academic achievement, poor physical health, low self esteem, anxiety and depression'.[36]

Advocating for law change, New Zealand Judge Neil MacLean said in 2012, 'bullying by mobile phone texting or on social media such as Facebook is "often a background factor" in suicides coming before the coroners'.[37]

The media makes frequent links between cyberbullying and suicide. For example, in 2012, news from Sydney told of abusive and unrelenting Twitter-tweets to well-known media personality, Charlotte Dawson, who spoke out publicly against cyberbullying before her death by suicide.[38] A 2016 news item from New Zealand reports the suicide of 12-year old, Kyana Vergara, a victim of social media attacks.[39]

Such accounts may serve as demonstrations of the mordant nature of online bullying. Where does cyberbullying happen? What space?

4 CYBERSPACE

4.1 Open and Creative Space

Cyberspace furnishes the stage for cyberbullying scripts and actions. Understanding the specific characteristics of this environment is crucial for understanding differences between offline and online offences.

(1) The term *cyberspace* is a blend of *cybernetics* (based in information theory) and *space*.[40] Cyberspace is an informational environment unlike Euclidean geometry or relativistic space.[41] A coded, stratified, dynamic, virtual space, cyberspace is the 'fifth common space, after land, sea, air and outer space'.[42]

---

36 Kelly Tallon, Ahram Choi, Matthew Keeley, Julianne Elliott and Debra Maher, 'New Voices / New Laws: School-age young people in New South Wales speak out about the criminal laws that apply to their online behaviour' (National Children's and Youth Law Centre and Legal Aid NSW, 2012) <http://www.lawstuff.org.au/__data/assets/pdf_file/0009/15030/New-Voices-Law-Reform-Report.pdf> 30.

37 Simon Collins, 'Suicide link in cyberbullying', *New Zealand Herald*, 7 May 2012, <http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10803980>. Accessed 6 September 2016.

38 Andrew Horney and Bianca Hall, 'Top Model judge in hospital after Twitter attacks' (*The Age* Melbourne, 30 August 2012) <http://www.theage.com.au>; 3News online, 'Charlotte Dawson speaks out about cyber bullying' (3News New Zealand, 3 September 2012) <http://www.3news.co.nz>.

39 Bevan Hurley, '12yo girl dies after bullying', *Sunday Star Times*, 13 March 2016, p.1.

40 William Gibson, science fiction writer, coined the term cyberspace as a dystopian virtual world of human habitation in *Burning Chrome* (Victor Gollancz 1986; first published by Omni, 1982) and popularised through his novel *Neuromancer* (1984). Online Etymology Dictionary, <http://www.etymonline.com/index.php?term=cyberspace >. Accessed 1 February 2016.

41 Margaret Wertheim, *The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet* (Doubleday, 2000).

42 Stein Schjølberg, *The History of Cybercrime: 1976-2014* (Kindle e-book, 2014).

(2) Cyberspace is a spatial depiction of computer data. It is an immaterial world of the mind, free of physical laws of gravity and the body's corporeal demarcations.[43] It offers a life beyond this life, a *virtual* reality.[44]

(3) Early commentators on cyberspace advocated a lawless cyber world.[45] Some early 'libertarian theorists' saw its potential for an 'unregulated social sphere',[46] advocating freedom of speech for users. Cyberspace offered a creative and utopian world of anonymity and pseudonymity,[47] a 'moral holiday'[48] in a borderless frontier land, released not only from corporeal restrictions, but legal interventions as well.

(4) However, cyberspace, for all the freedom it offers is not free of regulatory intervention. Cyberspace offers a creative space, yes, but it is also a coded and malleable environment designed as a three-dimensional matrix capable of being mapped and regulated.[49]

Everything in cyberspace is human-made; it is not beyond positive laws and regulations, and is already shaped by its technological codes of governance.[50] Cyberspace is not beyond governability.

4.2 Jurisdiction

The regulation of offences in this space raises issues for justice systems.

(1) Territorial jurisdiction emanates from national or state sovereignty, whereas cyberspace activities are globally fluid.[51] Cyberspace differs from geographical space in which one cannot be in two places at once. Cyberspace rejects such limitations.[52]

(2) With the advent of trans-border Internet technologies, offences involving anti-social or harmful conduct may give rise to a complainant in one location with a perpetrator in another. '[I]f a stalker in California uses an international service provider in Nevada to connect to an anonymiser in Latvia to target a victim in Australia, which jurisdiction has responsibility for regulating the cyberstalking?'.[53] This question applies equally to cyberbullying.

---

43 Elizabeth Grierson, above n 2.

44 'Virtual reality' (VR) has a specific definition within the broader category 'cyberspace', as an immersive environment created by computer data. Users wear sense-active technological headpieces or other devices to create characters or avatars as incarnations of humans, and to navigate the space via auditory, tactile and other sensory data as though their bodies inhabited real space. Multi-user domains (MUDS) or Second Life are interactive databases in which virtual environments can be constructed for group participation.

45 Nicholas Negroponte, *Being Digital* (Vintage Books, 1995).

46 Andrew D Murray, *The Regulation of Cyberspace, Control in the Online Environment* (Routledge-Cavendish, 2008), 5.

47 Pseudonymity: online digital persona and forged identities in email and cyberspace, minus face-to-face social clues, gestures, expressions. Louise Ellison, 'Cyberstalking, Tackling Harassment on the Internet' in David S Wall, *Crime and the Internet* (Routledge, 2004) 141; David Harvey J, and Internet Harassment: What the law can do' (Paper presented at NetSafe II Conference *Society, Safety and the Internet*, NZ Internet Safety Group, 2003) 3.

48 David S Wall, 'Maintaining Order and Law on the Internet' *Crime and the Internet*, above n 48, 167.

49 Andrew D Murray, above n 47, 53-4.

50 Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 2006); Andrew D Murray, above nn 47, 50.

51 Susan W Brenner, 'Cybercrime Jurisdiction' (2006) 46 *Crime Law Social Change* 189; Bert-Jaap Koops and Susan W Brenner (eds), *Cybercrime and Jurisdiction, A Global Survey* (Cambridge University Press, 2006); Uta Kohl, *Jurisdiction and the Internet, Regulatory Competence over Online Activity* (Cambridge University Press, 2007); Kim Soukieh, 'Cybercrime – the Shifting Doctrine of Jurisdiction' (2011) 10 *Canberra Law Review* 221.

52 Lawrence Lessig, above n 51.

53 E Ogilvie (2000) *Cyberstalking, Trends and Issues in Crime and Criminal Justice*, 166 <http://www.aic.gov.au>. Accessed 30 January 2015.

(3) In the Australian federal system, 'State and Territory agencies have primary responsibility for cybercrime that targets individuals, businesses and government systems in their jurisdictions'.[54] As with international jurisdictions, potential difficulties arise. Variable investigation powers for police and prosecutors exist under different criminal justice frameworks.[55]

(4) The US *Jake Baker* case[56] advances concerns apposite to this point. Baker was charged with five counts of transmitting threats by email across state borders,[57] by posting violent stories to a Sex Usenet group,[58] and corresponding by email about plans with a Canadian friend who transmitted emails via an Ontario based computer. Based on an FBI agent's affidavit, Michigan-based Baker was charged under *18 US Code* s 875(c) for sending threats via interstate commerce.[59]

Notwithstanding issues raised by conduct elements regarding what constitutes a 'threat', the case demonstrates challenges of finding appropriate jurisdiction for an action.

5 LEGAL AND POLICY RESPONSES

5.1 Global Legal Landscape

Globally, there is a wide variance to hold cyber bullies legally accountable.

(1) *United Kingdom*: cyberbullying is not legally identified as an offence. Several existing laws may apply, such as *Protection from Harassment Act*, *Criminal Justice and Public Order Act*, *Malicious Communications Act*, *Communications Act*.[60]

(2) *United States*: a range of state laws for cyberbullying offences exist in criminal and civil jurisdictions albeit with different methods of enforcement and adjudication on violations.[61] As of January 2016, bullying laws exist in every state, with cyberbullying specifically named in about 50% of them.[62]

(3) *European Union*: approaches to cyber abuse vary. For example, *Germany* relies on the Penal Code; *Sweden* enacted legislation against cyberbullying in 1993, the first European country to do so, and evidences the lowest rate of bullying in school-age children; *France* added consequences of cyberbullying into the French Labour Code in 2002; *Austria*, which has the highest cyberbullying rate in the EU, enacted legislation in January 2016 to criminalise cyber abuse.[63]

---

54 Australian Government, above n 36, 5.

55 Bert-Jaap Koops and Susan W Brenner, above n 52; Australian Government, above nn 36, 55.

56 *United States of America v Abraham Jacob Alkhabaz (Jake Baker)* (1997) 104 F.3d 1492.

57 Pursuant to *18 US Code* §875(c) Interstate Communications; relevantly interstate communication contains threat to kidnap or injure a person.

58 Alt.sex.stories Usenet group.

59 *18 US Code*, above n 58.

60 *Protection from Harassment Act 1997* (UK), *Criminal Justice and Public Order Act 1994* (UK), *Malicious Communications Act 1988* (UK), *Communications Act 2003* (UK). The Crown Prosecution Service provides guidelines for application of these laws to cyberbullying.

61 US Federal laws provide a civil rights defence to vitiate charges of bullying or cyberbullying: US Department of Education's Office for Civil Rights <http://www2.ed.gov/about/offices/list/ocr/index.html> and US Department of Justice, Civil Rights Division < https://www.justice.gov/crt>. Accessed 9 September 2016.

62 Cyberbullying Research Center, 'Analysis and Implications of Laws' <http://cyberbullying.org/cyberbullying-laws>. Accessed 4 September 2016.

63 The Local, 'Austria Cracks down on cyber abuse' (4 January 2016) <http://www.thelocal.at/20160104/austria-cracks-down-on-cyber-abuse>. Accessed 4 September 2016.

(4) Canada: victims of cyberbullying rely on police or civil remedies. The first legal protection against cyberbullying, the Cyber Safety Act, 64 was enacted in Nova Scotia in 2013, only to be struck down in late 2015, by the Supreme Court of Nova Scotia. It was adjudged that the Charter of Human Rights and Freedoms, section 2,65 trumped the legislative rights of the provincial Act.[66]

(5) *Africa*: legislation in *South Africa* targets online abuse by requiring ISPs to divulge contact details of those found harassing another.[67] In *other African* countries, a weakness of legislation persists and victims frequently do not report online abuse because of systemic corruption and protection of abusers' reputations.[68]

(6) *Asia*: legal responses vary. In brief, *China* tracks individual users, censors Internet content, controls news transmission, and blocks Facebook and access to Google (although permitted in Hong Kong). *Taiwan* has no specific anti-cyberbullying laws and relies on a self-regulatory system. In 2008, *South Korea* introduced the Korea Communication Standards Commission (KCSC) to combat cyberbullyting.

In *Japan*, legislation was enacted in 2013 to regulate cyberbullying. In *Malaysia*, there is no specific law to regulate cyberbullying. In 2013, *Phillippines* put legal responsibility onto schools. *Singapore* introduced legislation in 2014, to criminalise cyberbullying with hefty penalties, to the concern of journalists who consider freedom of speech may be hampered.[69] *India* has a 'legal vacuum' regarding cyberbullying.[70]

(7) *Russia* has a high rate of cyberbullying, but no laws to regulate it. *Saudi Arabia's* cybercrime laws rely on naming and shaming. *Turkey* puts responsibility onto education institutions. In *UAE* cyberbullying is a criminal offence.

(8) In *South America* legal responses vary. In 2008 *Argentina* introduced information technology offences into existing criminal legislation. In 2011, *Chile* put legal responsibility for cyberbullying onto schools. *Brazil* introduced a new law in 2015 to establish a national programme to regulate and educate against cyberbullying.

5.2 Australia and New Zealand

Over the past four years, *Australia* and *New Zealand* have been active in responding to cyberbullying. Both countries provide resources for educational institutions to support the institution's duty of care role in providing a safe educational environment.

Legal and policy responses will be addressed shortly, but first some attention to issues of duty of care, as raised by a cyber event in an Australian university.

---

64 *Cyber-Safety Act 2013* (Nova Scotia).

65 *Canadian Charter of Human Rights and Freedoms*, section 2, of the *Constitution Act* 1982.

66 Andrew Vaughan, *The Canadian Press*, 26 July 2016, 'Canadian Provinces in urgent need of anti-cyberbullying laws, expert says' < https://www.thestar.com/news/canada/2016/07/26/canadian-provinces-in-urgent-need-of-anti-cyberbullying-laws-expert-says.html>. Accessed 4 September 2016.

67 Henry Carus Associates, 'A Guide to Worldwide Bullying Laws' <https://www.hcalawyers.com.au/blog/bullying-laws-around-the-world/>. Accessed 4 September 2016.

68 K. Lyons, T. Phillips, S. Walker, J. Henley, P. Farrell, M. Carpentier, 'Online Abuse: How different countries deal with it', *The Guardian* (12 April 2016) <https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrassment-revenge-pornography-different-countries-deal-with-it>. Accessed 4 September 2016.

69 Mong Palatino, 'Singapore Criminalizes Cyberbullying and Stalking', *The Diplomat* (24 March 2014) < http://thediplomat.com/2014/03/singapore-criminalizes-cyber-bullying-and-stalking/>. Accessed 4 September 2016.

70 Deccan Herald, 'Cyber bullying rampant in India, legal vacuum persists', (19 April 2015) <http://www.deccanherald.com/content/472554/cyber-bullying-rampant-india-legal.html>. Accessed 9 September 2016.

6 DUTY OF CARE

6.1 Raising Problems

The following account addresses the duty of care owed by an educational institution in cyber abuse situations. It raises problems of how far the duty of care extends, and of how to address cyber harm. Problems are identified for both the institution and the judiciary.

6.2 Educational Change and Court Action

(1) As head of a school of art in an Australian university for seven years, I was immersed in the opportunities afforded by the creative potentials of cyberspace. Students and academics maximised the capacity of the Internet for communications, creative productions and pedagogies. Some used it for nefarious purposes.

In 2011, I led an educational change project. The thought of change attracted the wrath of a teacher in the same school who took to social media to vent his spleen. His unrelenting actions went well beyond the regulatory codes of the university, and this employee was dismissed ultimately through the university disciplinary process. His venting became more acrimonious when he was no longer an employee of the institution, and therefore no longer subject to its regulatory codes. He was however still subject to the laws of the State. There were no bullying provisions in the *Fair Work Act* at the time. The university took a stalking action under the *Crimes Act*.[71]

(2) The entire process brought to light the deleterious effects of cyberbullying—and cyberstalking—in the institutional context and the fundamental requirements of duty of care vested in an educational institution. Difficulties of distinguishing between cyberbullying and cyberstalking were also raised.

(3) On the day of the contested hearing at the Magistrates' Court,[72] the matter was resolved by negotiation, with the respondent agreeing to remove certain particularly offensive and targeted postings that were causing the greatest level of distress for the complainant.

A Court Order was handed down to prevent the respondent from posting anything about the complainant, by name, title or past relationship to her, with malice, or for any purpose other than fair comment on matters of public affairs, or cause another to do so, for 20-years.[73]

Curiously, the Court Order stipulated 20-years for the complainant not to access the respondent's social media pages. This suggests that by not seeing any postings one is protected from harm. This is quite illogical.

(4) The Court Order gave rise to an impossible if not illogical situation in three ways: (i) to order a victim to not look at a public Facebook or other social media site does not stop the continuation of any deleterious conduct; and

(ii) knowing the victim is prohibited from looking at cyber sites could well be an open invitation for a perpetrator to continue posting with alacrity;

---

71 Discussed in E.M. Grierson, above n 3.
72 13 April 2011, Magistrates Court of Victoria, Melbourne.
73 Court Order Magistrates' Court of Victoria, Melbourne, Court Order B10510315, 13 April 2011.

(iii) if one is prohibited from viewing the social media sites, then how could further abuse be identified and how could further action be taken against a perpetrator?

(5) As the contested hearing did not proceed the legal provisions were not tested in relation to stalking on Facebook and other cyber sites. Thus an opportunity was lost to test evidence and advance the jurisprudence of laws in respect of cyberstalking and/or cyberbullying.

Notwithstanding any loss to jurisprudence, the entire event raises a number of significant issues regarding duty of care by the education institution.

6.3 What is the Duty of Care?

(1) Firstly, an educational institution has a duty of care to its employees to ensure their health and safety at work. To fulfill this duty appropriately it is incumbent upon an institution to be fully informed about the inherent nature of cyberspace, to understand how malicious words and images multiply in social media attracting other people into their orbit, and to recognize deleterious effects upon victims.

In this case, the advice of the university media and communications executive to 'let sleeping blogs lie' evidences a lack of awareness and knowledge of the multiplication effect. The chain of abuse holds endless capacity for corrosive and far-reaching damage. Blogs do not sleep, nor do they lie down; their nerve systems and life-blood draw from their networked circulations.

(2) Secondly, a university has a duty to its employees, if not to external stakeholders, to be at the forefront of anticipating and managing media interest around events of cyber abuse, if and when they occur in employment situations.

This case evidenced a serious underestimation of media interest by the university. The university was unprepared. No statement had been given to the media, no protection for the complainant. The half page article complete with photographs on the front page of *The Age* the next morning,[74] and the fanning of media fires in newspapers, radios, and online sites for many weeks to follow attested to that deficiency.

The respondent took to the media with alacrity, turning his defence to the public gaze, making it a freedom of speech issue, and seeking public sympathy.

(3) Thirdly, a university's fiduciary duty must extend past one event in time. Where would be a cut off point? Harm to the victim continued. Harm from cyber abuse is not born of being offended; it is a psychological harm caused by conduct with continuous corrosive effects, its orbit increasing in ever-multiplying networks.

(4) Fourthly, does the university's fiduciary duty extend to protect employees from defamation? The university's advice in this case was to take a private action, but they would not assist. The fiduciary duty to the employee appeared to end there.

[74] Karl Quinn, 'Art school altercation puts new spin on cyberstalking' (*The Age* Melbourne, Thursday 14 April 2011) 1.

(5) Had the amendments for workplace bullying in the *Fair Work Act*[75] been in place at the time the action may have taken a different turn. From 2013, a worker who alleges bullying at work may apply to the Fair Work Commission for orders to stop the bullying,[76] to be dealt with in 14 days.[77] The Commissioner has jurisdiction to order employers to take action.

7 LEGAL RESPONSES IN AUSTRALIA

There is no overarching cyberbullying legislation in Australia. Each state and territory has laws on bullying; legal responses to regulate cyber abuse vary.[78]

7.1 Commonwealth Responses

(1) Successive governments in Australia have responded in policy to the escalating problem of cyberbullying.[79] In recommending 'an effective complaints system, backed by legislation, to get harmful material down fast from large social media sites',[80] the opposition Coalition policy advised consideration of the New Zealand approach to the enactment of a 'new, simplified cyberbullying offence'.[81]

(2) Redress for cyberbullying may be found under the Commonwealth *Criminal Code Act*:[82] it is an offence to misuse telecommunications services in a way that is 'menacing, harassing or offensive'.[83] This may involve explicit taunts or threats to a receiver or an implicit threat by multiple cyber-postings. The objective reasonable person test applies. The Act also provides for threats to cause serious harm or to kill.[84]

(3) In 2015 the *Enhancing Online Safety for Children's Act*[85] established a Children's e-Safety Commissioner and Office of the Children's e-Safety Commissioner. The Act provides an effective means of regulating social media usage with mechanisms for reporting abuses, assistance to stakeholders for online safety, and removal of cyberbullying material targeting an Australian child.[86] The Commission is partnered with social media sites, Facebook, Flickr, Twitter, Google, Instagram and YouTube.

---

75 *Fair Work Act 2009* (Cth).
76 *Fair Work Act 2009* (Cth) ss 789FC(1), 789(FF).
77 *Fair Work Act 2009* s 789FE.
78 Information is found on Australian Human Rights Commission, 'Cyberbullying: what is it and how to get help. Violence, harassment and bullying fact sheet <https://www.humanrights.gov.au/cyberbullying-what-it-and-how-get-help-violence-harassment-and-bullying-fact-sheet>. Accessed 3 September 2016.
79 For example, the Gillard Labour Government in Australia launched *Cybersmart. The Easy Guide to Socialising Online* <http://www.cybersmart.gov.au>. The opposition Coalition Policy to Enhance Online Safety for Children (September 2013) recommended establishment of a Children's e-Safety Commissioner to work with the National Safe Schools Framework so that all schools 'plan, implement and monitor online safety initiatives', <http://lpaweb-static.s3.amazonaws.com/Coalition%202013%20Election%20Policy%20-%20Enhance%20Online%20Safety%20for%20Children.pdf> 8. Accessed 15 January 2015.
80 Ibid 2.
81 Ibid.
82 *Criminal Code Act 1995* (Cth).
83 *Criminal Code Act 1995* (Cth) s 474.17.
84 *Criminal Code Act1995* (Cth) s 474.15.
85 *Enhancing Online Safety for Children's Act 2015* (Cth).
86 Australian Government Office of the Children's e-Safety Commissioner <https://www.esafety.gov.au/> Accessed 3 September 2016.

7.2 States and Territories

Legal responses to cyberbullying vary with each jurisdiction. In brief:

(1) *Victoria*. Following the tragic suicide of Brodie Rae Constance Panlock who was bullied mercilessly at work, legal reforms in Victoria brought bullying into criminal jurisdiction in 2011. Online conduct is included.[87] The reform expanded s 21A(2)(d) of the *Crimes Act* to 'making threats', 'using offensive or abusive words', 'directing abusive or offensive acts',[88] causing 'self-harm' to a victim (physical or mental).[89]

(2) *New South Wales*. The *Crimes Act* makes it an offence to 'assault, stalk, harass or intimidate any school student or member of staff … *while attending school'*.[90] Attending school means bullying on school grounds or entering or leaving school premises in connection with school-related work, duty or care.[91] Because of the borderless nature of cyberspace, difficulty may arise in such situations of cyberbullying.[92]

(3) *Queensland*. Provisions applying to unlawful stalking in the *Criminal Code Act*,[93] 'engaged in on any 1 occasion if the conduct is protracted'.[94] This provision may arguably apply to the multiplier effect of online bullying. *South Australia*. The bullying conduct occurring 'on at least two separate occasions',[95] may cover the multiplier effect of cyberbullying.

(4) *Tasmania*. The conduct requirement, 'using the internet or any other form of electronic communication in a way that could reasonably be expected to cause the other person to be apprehensive or fearful',[96] may extend to cyberbullying. In *Western Australia*,[97] as with New South Wales, 'place' is not defined with regard to cyber-offences.[98]

(5) In *Northern Territory* and *Australian Capital Territory*, cyberbullying can be a crime when the abuse is menacing, harassing, threatening or offensive.

8 CASE LAW

8.1 Shane Philip Gerada

Australia's first successful prosecution for a cyberbullying offence was in 2011, *Shane Philip Gerada*.**[99]** The offender sent over-300 hateful and threatening messages by text, out of revenge, over a few months to 17-year-old, Allem Halkic, and made false comments about Halkic on MySpace. This resulted in Halkic's suicide in 2009.

87 *Crimes Act 1958* (Vic).
88 *Crimes Act1958* (Vic) ss 21A(2)(da)-(dd).
89 *Crimes Act 1958* (Vic) s 21A(2)(g)(i); ss 21A(2)-(3).
90 *Crimes Act 1900* (NSW) s 60E. Emphasis added.
91 *Crimes Act 1900* (NSW) s 60D(2).
92 Makinson and d'Apice Lawyers, 'Cyberbullying: Where does a school's duty of care end?' (2011) *Education Law Today* 3.
93 *Criminal Code Act 1899* (Qld).
94 *Criminal Code Act 1899* (Qld) s 359B(b); s 359B(c)(i)-(vii).
95 *Criminal Law Consolidation Act 1935* (SA) s 19AA(1)(a).
96 *Criminal Code Act 1924* (Tas) s 192(1)(h).
97 *Criminal Code Act Compilation Act 1913* (WA) s 338(D)-(E).
98 *Criminal Code Act Compilation Act 1913* (WA) s 338D; *Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 8(1).
99 *VPOL v Shane Gerada* (Y03370432) [2011] Magistrates Court of Victoria, Melbourne.

Magistrate Peter Reardon declared, 'It just demonstrates SMS messages or internet communication may have severe consequences on intended victims whether it was meant to or not'.[100]

The sentence was light, 18-month community based order and 200 hours of unpaid community work.

This case activated public outcry against insufficient legal avenues and penalties for conviction of online bullies.

8.2 Police v Ravshan Usmanov

Police v Ravshan Usmanov[101] concerned publishing an indecent article pursuant to s 578C of the *Crimes Act*.[102] A conviction was upheld.

This case was the first action in New South Wales to demonstrate the court's response to offensive publications in cyberspace. The offender had uploaded onto Facebook six nude photographs of the complainant, his ex-girlfriend, without her consent, and invited a person known to her to be a friend on the Facebook site.[103]

Mottley J stated, 'no NSW reported decisions could be located that assist with the approach to be taken in a matter such as this where the material has been published on Facebook or the Internet'.[104]

His Honour then turned to '[t]he only decision found', from Judge Becroft in the Wellington District Court of New Zealand, *Police v Joshua Ashby*.[105] 'Mr Ashby had posted a nude photograph of his ex girlfriend on Facebook … [It] remained online for a period of 12 hours before the police and Facebook authorities shut down the account'.[106] Mr Ashby had also logged into the victim's account, 'unlocked her privacy settings and changed her password'.

In sentencing the offender to four months imprisonment, Judge Becroft considered the appropriate starting point to be prison as a deterrent in the use of technology.

In *Usmanov,* Mottley J found no extenuating circumstances. 'The nature of this offence could not be regarded as trivial. The offence was executed with planning and characterised by a clear intent'.[107]

---

100 Ibid [Peter Reardon Magistrate].
101 *Police v Ravshan Usmanov* (*Usmano*v) [2011] NSWLC 40; *Usmanov v R* [2012] NSWDC 290.
102 *Crimes Act 1900* (NSW) s 578C.
103 *Police v Ravshan Usmanov* [2011] NSWLC 40, 3-8 [Mottley J].
104 Ibid 10 [Mottley J].
105 *Police v Joshua Ashby* (2010) District Court of Wellington, NZ.
106 As outlined by Mottley J in *Police v Ravshan Usmanov* [2011] NSWLC 40, 11 [Mottley J].
107 *Police v Ravshan Usmanov* [2011] NSWLC 40, 17 (Mottley J).

In handing down a six-month term of imprisonment, Mottley J took care to account for the specific nature of social networking sites and the importance of deterrence for the offender and the community:

> This is a particularly relevant consideration in a matter such as this where new age technology through Facebook gives instant access to the world. Facebook as a social networking site has limited boundaries. Incalculable damage can be done to a person's reputation by the irresponsible posting of information through that medium. With its popularity and potential for real harm, there is a genuine need to ensure the use of this medium to commit offences of this type is deterred.[108]

This judicial approach to the law shows a willing engagement with the new challenges posed by the specific characteristics of cyberspace offences.

8.3 Sentencing

Case precedent for conviction and sentencing is limited. Notwithstanding that the magistrates in both the *Gerada* and *Usmanov* cases emphasised the seriousness of online bullying, both offenders received lenient sentences, one a community based order, the other a term of imprisonment, which was suspended on appeal.[109]

8.4 Separate Cyberbullying Laws

Following the lenient sentencing in *Gerada*, Chair of *National Centre Against Bullying*, the Honourable Alastair Nicholson stated, 'There is a very strong argument that [cyberbullying] should be considered a specific offence'.[110]

His Honour pointed out that with the lack of specific cyberbullying laws perpetrators are being charged with the wrong offences: 'You tend to get it in the stalking area, and with some of the sexually explicit communications get into breaches of pornography laws'.[111]

The above analysis supports the growing contention in this research that separate cyberbullying laws are needed with specific offences for cyberbullying in Australia; accompanied by robust educational programs.[112]

9 NEW ZEALAND APPROACHES

9.1 Legislative Change

In 2015, New Zealand enacted the *Harmful Digital Communications Act*,[113] making it an offence to send or publish offensive or threatening material or messages. This includes sending images, or harassing, intimidating, or spreading rumours of a degrading or damaging kind.

---

108 Ibid 19.

109 *Usmanov v R* [2012] NSWDC 290.

110 Alastair Nicholson, former CJ of Family Court, cited in Cyber-bullying in Australia, 'Australian Cases, Cyberbullying in Australia' (2013) <https://cybercrime2013.wordpress.com/findings-and-research/australian-cases/>.

111 Ibid.

112 See also recommendations, National Centre Against Byllying, 'Bullying Young People and the Law Symposium' (Victoria University Melbourne, 18-19 July 2013) <https://www.ncab.org.au/other/bullying-young-people-and-the-law-symposium-recommendations/>. Accessed 9 September 2016.

113 *Harmful Digital Communications Act 2015* (NZ).

Since this enactment, there have been eight charges, and two people convicted, one sentenced to four-months imprisonment, another to three-month's community detention and 200-hours community work.

9.2 NZ Law Commission Review

(1) In December 2011, the New Zealand Law Commission[114] commenced a review of harmful digital communications. The Commission examined the effectiveness or otherwise of 'existing criminal and civil remedies for wrongs' in the new media environment, and 'whether alternative remedies may be available'.[115]

(2) The Commission called for submissions on its Issues Paper,[116] focusing on rights and responsibilities towards 'harmful speech in the digital age' and making recommendations for reform.[117]

Published responses variously claimed threats to freedom of speech,[118] effects on social networking users,[119] concern for a single regulator,[120] and approval for naming and shaming.[121]

(3) The Bill stated that the proposed legislation 'creates a precedent, not only in New Zealand, but internationally, for establishing criminal offences which only apply to the digital environment'.[122]

Microsoft was reported to be against the legislative changes claiming the standard for online abuse in New Zealand would be different from other jurisdictions.[123]

---

[114] The Law Commission Te Aka Matua O Te Ture is an independent Crown agency under the *Crown Entities Act 2004* (NZ) to review laws, recommend need for reform or development, and make recommendations to Parliament <http://www.lawcom.govt.nz/about>. Accessed 15 January 2015

[115] Simon Power, 'Review of Regulatory Gaps and the New Media', The New Zealand Law Commission Issues Paper 27 Summary and preliminary proposals (Law Commission Te Aka Matua O Te Ture, December 2011).

[116] New Zealand Law Commission Te Aka Matua O Te Ture, *The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age* (submissions closed 30 March 2012) <http://www.lawcom.govt.nz>. Accessed 15 January 2015.

[117] New Zealand Law Commission (submissions published, 4 May 2012), ibid.

[118] Editor, 'Centuries of press freedom under threat' *New Zealand Herald*, New Zealand (12 May 2012) <http://www.nzherald.co.nz>. Accessed 15 January 2015.

[119] William Akel and Tracey Walker, 'Bloggers, Tweeters and Facebook: New Media or News Media' (Simpson Grierson, Auckland, 22 December 2011) <http://www.simpsongrierson.com/litigation>.

[120] Editor, 'Slings and arrows of a single regulator' (*Dominion Post* Wellington, 19 January 2012) <http://www.stuff.co.nz/dominion-post>. Accessed 15 January 2015.

[121] Alanah Eriksen, 'Name, shame plan to fight cyber-bullies' (*NZ Herald*, 15 August 2012), A1.

[122] *Harmful Digital Communications Bill 2014* (NZ), Commentary Introduction (Justice and Electoral Committee, House of Representatives New Zealand, 2014). Accessed 15 January 2015.

[123] Su Reissa, 'Microsoft Against Proposed Changes to New Zealands Cyberbullying Law' (*International Business Times*, 27 March 2014) < http://au.ibtimes.com/microsoft-against-proposed-changes-new-zealands-cyberbullying-law-1336164>. Accessed 15 January 2015.

(4) A ministerial briefing paper[124] followed publication of the review submissions.[125] This process resulted in the *Harmful Digital Communications Bill NZ*,[126] seeking 'to mitigate harm caused to individuals by electronic communications and to provide victims of harmful digital communications with a quick and effective means of redress'; and to 'create a new civil enforcement regime and new criminal offences to deal with the most seriously harmful digital communications'.[127]

9.3 The Act

The *Harmful Digital Communications Act* provides new civil and criminal remedies for harmful digital communications—including public and private postings.[128]

> (1) The new criminal offence is 'causing harm by posting a digital communication'.[129] Elements include intention to cause harm, and it would cause harm by the ordinary reasonable person test, and it causes harm to the victim. It carries a term of imprisonment of up to two years, up to $50,000 fine for an individual, $200,00 for a body corporate
>
> (2) The Court has powers to require the author of content, to
>
> (i) remove content; (ii) cease from conduct; (iii) not encourage others to engage in similar communication to the affected person; (iv) order a right of reply for the affected person; (v) publish an apology or correction.
>
> The Court may require the online host, to
>
> (i) take down or disable public access to material already sent; (ii) publish a correction; (iii) provide right of reply for affected person; (iv) release identity of the author to the Court; or require an IPAP to do so.[130]
>
> (3) Ten Communications Principles[131] guide the 'Approved Agency or courts' in 'performing functions or exercising powers under this Act'.[132]
>
> Digital communications should not,
>
> (i) disclose sensitive personal facts about an individual;
>
> (ii) be threatening, intimidating, or menacing;
>
> (iii) be grossly offensive to a reasonable person in the position of the affected individual;
>
> (iv) be indecent or obscene;
>
> (v) be used to harass an individual;
>
> (vi) make a false allegation;
>
> (vii) contain a matter that is published in breach of confidence;

---

124 New Zealand Law Commission, Te Aka Matua O Te Ture, *Harmful Digital Communications: The adequacy of the current sanctions and remedies* (Law Commission Ministerial Briefing Paper, 2012).

125 New Zealand Law Commission, above n 118.

126 *Harmful Digital Communications Bill 2014* (NZ) (Justice and Electoral Committee, House of Representatives New Zealand, 2014). Consideration is given to tensions between regulation of speech in digital communications via the *Harmful Digital Communications Bill* and rights to freedom of speech consistent with *New Zealand Bill of Rights Act 1990* (NZ).

127 *Harmful Digital Communications Bill 2014* (NZ) Commentary Introduction.

128 *Harmful Digital Communications Act 2015* (NZ).

129 *Harmful Digital Communications Act 2015* (NZ) s 22 Causing harm by posting digital communication.

130 IPAP: Internet Protocol Address Provider.

131 *Harmful Digital Communications Act 2015* (NZ) s 6(1).

132 *Harmful Digital Communications Act 2015* (NZ) s 6(2).

(viii) incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual;

(ix) incite or encourage an individual to commit suicide;

(x) denigrate an individual by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation or disability.[133]

(4) The Act amends a number of existing statutes;[134] and makes consequential amendments of other Acts to which the Approved Agency is subject.[135]

10 FINDINGS AND RECOMMENDATIONS

10.1 Findings

In summary this research finds that:

(1) Cyberbullying has different characteristics from offline bullying. The footprints of words, images and messages in cyberspace have the potential to multiply in space and time affecting continuing harm for victims.

(2) Understanding the nature of the digital economy and cyberspace enhances institutional and judicial approaches to cyberbullying and other forms of harm through digital communications.

(3) As the penetration percentage of Internet usage increases, so cyberbullying occurrence increases.

(4) Legal responses to cyberbullying present significant global variations.

(5) An educational institution has a continuing duty of care for employees in cyber harm situations.

(6) From 2015, New Zealand has an overarching law to regulate harmful digital communications.

(7) Australia has in place an overarching *National Plan to Combat Cybercrime* with the key priority of 'ensuring the criminal justice framework is effective'.[136]

(8) Whilst Australia has enacted legislation for children's online safety, there is no uniform or stand-alone law to combat cyberbullying for adults. The question of whether or not there ought to be remains open.

[133] Principles from *Harmful Digital Communications Act* s 6, outlined by Simpson Grierson, 'Harmful Digital Communications Act: what you need to know', <http://www.simpsongrierson.com/articles/2015/harmful-digital-communications-act>. Accessed 9 September 2016.

[134] *Crimes Act 1961* (NZ); *Harassment Act 1997* (NZ); *Human Rights Act 1993* (NZ); *Privacy Act 1993* (NZ).

[135] *Ombudsmen Act 1975* (NZ); *Public Records Act 2005* (NZ); *Official Information Act 1982* (NZ).

[136] Australia Government, above nn 36, 55, 20-21. The *National Plan* provides four policy principles for a national response to cybercrime: 'Understanding the problem'; 'Partnerships and shared responsibility'; 'Focusing on prevention'; and 'Balancing security, freedom and privacy'. *National Plan*, 7.

10.2 Recommendations

The research submits the following recommendations:

(1) The specific characteristics of the Internet and cyberspace, and the harmful conduct that occurs in this 'faceless space', be better understood by the three arms of government, and this understanding is reflected in policy, legislation and the administration of justice.

(2) In Australia, a cohesive approach is established to regulate cyber-related offences; a robust cyberbullying statute at Commonwealth level would be reflected by a uniform approach in State and Territory jurisdictions.

(3) There is effective coordination between the justice system, education, social and other agencies to better respond to harmful online communications, in Australia and elsewhere.

(4) In formulating new legislation tailored specifically for digital communications, Australia makes a close examination of the New Zealand approach to this serious public issue.

(5) To deal with the escalating problem of cyberbullying, as a global issue, the implementation and consolidation of effective justice frameworks is prioritised globally, in order to protect people's wellbeing and safety.

(6) Finally, as the New Zealand approach shows, cohesive statutory regulations of harmful conduct in cyberspace provide assurance for public and private protection, and positive outcomes for the justice system.

REFERENCES

A *Articles/Books/Reports*

3News New Zealand, 3News online, 'Charlotte Dawson speaks out about cyber bullying' (3 September 2012) <http://www.3news.co.nz>

Akel, William and Tracey Walker, 'Bloggers, Tweeters and Facebook: New Media or News Media' (Simpson Grierson, Auckland, 22 December 2011) <http://www.simpsongrierson.com/litigation>

Australian Government, Attorney-General's Department, *National Plan to Combat Cybercrime* (Commonwealth of Australia, 2013)

Brenner, Susan W, 'Cybercrime Jurisdiction' (2006) 46 *Crime Law Social Change*, 189

Brenner, Susan W, *Cybercrime and the Law: Challenges, Issues, and Outcomes* (Northeastern University Press, 2012)

Chatterjee, Bela Bonita, 'The Last of the Rainmacs: Thinking about Pornography in Cyberspace' in David S Wall (ed), *Crime and the Internet* (Routledge, 2004) 74

Collins, Simon, 'Suicide link in cyberbullying', *New Zealand Herald*, 7 May 2012, <http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10803980>

Deccan Herald, 'Cyber bullying rampant in India, legal vacuum persists' (19 April 2015) <http://www.deccanherald.com/content/472554/cyber-bullying-rampant-india-legal.html>

Editor, 'Centuries of press freedom under threat', *New Zealand Herald*, New Zealand (12 May 2012) <http://www.nzherald.co.nz>

Editor, 'Slings and arrows of a single regulator', *Dominion Post* Wellington (19 January 2012) <http://www.stuff.co.nz/dominion-post>

Ellison, Louise, 'Cyberstalking, Tackling Harassment on the Internet' in David S Wall, *Crime and the Internet* (Routledge, 2004)

Eriksen, Alanah, 'Name, shame plan to fight cyber-bullies', *New Zealand Herald* New Zealand (15 August 2012)

Gibson, William, *Burning Chrome and Other Short Stories* (Victor Gollancz 1986, first published by Omni, 1982)

Gibson, William, *Neuromancer* (London Grafton Books, 1984)

Gilbert, Paula, 'One in five SA teens cyber bullied', Web Wireless (23 September 2015) <http://www.itweb.co.za/index.php?option=com_content&view=article&id=146442>

Grierson, E M, 'From Cemeteries to Cyberspace: Cartographies of Identity in a Technologised Age' (2001) 20 *ACCESS Critical Perspectives on Communication, Cultural and Policy Studies* 2, 11

Grierson, E M, 'Cyberspace, Cyberbullying, Cyberstalking: New challenges in law and education' in Alan Knowsley (ed) *Proceedings of the 21st Annual ANZELA Conference 2012 - Woteva nxt! Legal and social challenges in education* (Wellington, New Zealand 3-5 October 2012) 1-13

Hafner, K and M Lyon, *Where Wizards Stay up Late* (Simon and Schuster 1996)

Harvey J David, 'Cyberstalking and Internet Harassment: What the law can do' (Paper presented at NetSafe II Conference *Society, Safety and the Internet,* New Zealand Internet Safety Group, 2003)

Horney, Andrew and Bianca Hall, 'Top Model judge in hospital after Twitter attacks' (*The Age* Melbourne, 30 August 2012) <http://www.theage.com.au>

Hurley, Bevan, '12yo girl dies after bullying', *Sunday Star Times,* 13 March 2016

Jackson, Margaret and Marita Shelly, *Electronic Information and the Law* (Thomson Reuters 2012)

Kohl, Uta, *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (Cambridge University Press, 2007)

Koops, Bert-Jaap and Susan W Brenner (eds), *Cybercrime and Jurisdiction, A Global Survey* (Cambridge University Press, 2006)

Lessig, Lawrence, *Code and Other Laws of Cyberspace (*Basic Books, 2006)

The Local, 'Austria Cracks down on cyber abuse' (4 January 2016) <http://www.thelocal.at/20160104/austria-cracks-down-on-cyber-abuse>

Lyons, K, T Phillips, S Walker, J Henley, P Farrell, and M Carpentier, 'Online Abuse: How different countries deal with it', *The Guardian* (12 April 2016) <https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrassment-revenge-pornography-different-countries-deal-with-it>

Makinson and d'Apice Lawyers, 'Cyberbullying: Where does a school's duty of care end?' (2011) *Education Law Today* 3

Merriam-Webster Dictionary and Encyclopedia online < http://www.merriam-webster.com/dictionary/internet >

Morton, Jamie, 'Rates of cyberbullying in New Zealand alarming', in *New Zealand Herald* Monday (28 March 2016) <http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11612551>.

Murray, Andrew D, *The Regulation of Cyberspace, Control in the Online Environment* (Routledge-Cavendish, 2008)

Negroponte, Nicholas, *Being Digital* (Vintage Books, 1995)

New Zealand Law Commission Te Aka Matua O Te Ture, *The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age* (NZ Government 2011) <http://www.lawcom.govt.nz >

Ogilvie, E (2000) *Cyberstalking, Trends and Issues in Crime and Criminal Justice*, 166 <http://www.aic.gov.au>

Olweus, Dan, 'Cyberbullying: An Overrated Phenomenon?' (2012) 9 *European Journal of Developmental Psychology* 5, 1

Olweus, Dan, 'Comments on Cyberbullying Article: A Rejoinder' (2012) 9 *European Journal of Developmental Psychology* 5, 559

Olweus, Dan and Susan P Limber, 'Bullying in School: Evaluation and Dissemination of the Olweus Bullying Prevention Program' (2010) 80 *American Journal of Orthpsychiatry* 1, 124

Palatino, Mong, 'Singapore Criminalizes Cyberbullying and Stalking', *The Diplomat* (24 March 2014) < http://thediplomat.com/2014/03/singapore-criminalizes-cyber-bullying-and-stalking/>

Parliament of Victoria, Law Reform Committee, Inquiry into Sexting, Final Report May 2013 <http://www.parliament.vic.gov.au/lawreform/article/944>

Prensky, Marc, 'Digital Natives, Digital Immigrants' (2001) 9 *On the Horizon* 1

Quinn, Karl, 'Art school altercation puts new spin on cyberstalking' (*The Age* Melbourne, Thursday 14 April 2011) 1

Schjølberg, Stein, *The History of Cybercrime: 1976-2014* (Kindle e-book, 2014)

Soukieh, Kim, 'Cybercrime – the Shifting Doctrine of Jurisdiction' (2011) 10 *Canberra Law Review* 221

Su, Reissa, 'Microsoft Against Proposed Changes to New Zealand's Cyberbullying Law', *International Business Times* (27 March 2014) <http://au.ibtimes.com/microsoft-against-proposed-changes-new-zealands-cyberbullying-law-1336164>

Tallon, Kelly, Ahram Choi, Matthew Keeley, Julianne Elliott and Debra Maher, '*New Voices / New Laws*: School-age young people in New South Wales speak out about the criminal laws that apply to their online behaviour' (National Children's and Youth Law Centre and Legal Aid NSW, 2012) <http://www.lawstuff.org.au/__data/assets/pdf_file/0009/15030/New-Voices-Law-Reform-Report.pdf>

Vaughan, Andrew, *The Canadian Press*, 26 July 2016, 'Canadian Provinces in urgent need of anti-cyberbullying laws, expert says' <https://www.thestar.com/news/canada/2016/07/26/canadian-provinces-in-urgent-need-of-anti-cyberbullying-laws-expert-says.html>

Wall, David S (ed), *Crime on the Internet* (Routledge 2004)

Wall, David S, 'Maintaining Order and Law on the Internet' in *Crime and the Internet* (Routledge, 2004)

Wertheim, Margaret, *The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet* (Doubleday, 2000)

B *Cases*

Police v Ashby (2010) District Court of Wellington NZ

Police v Ravshan Usmanov [2011] NSWLC 40

United States of America v Abraham Jacob Alkhabaz (Jake Baker) (1997) 104 F.3d 1492

Usmanov v R [2012] NSWDC 290

VPOL v Shane Gerada (Y03370432) [2011] Magistrates Court of Victoria, Melbourne

C *Legislation*

18 US Code (United States)

Canadian Charter of Human Rights and Freedoms (Canada)

Communications Act 2003 (UK)

Constitution Act 1982 (Canada)

Copyright Act 1968 (Cth)

Copyright Act 1994 (NZ)

Crimes Act 1990 (NSW)

Crimes Act 1961 (NZ)

Crimes Act 1958 (Vic)

Crimes (Domestic and Personal Violence) Act 2007 (NSW)

Criminal Code 1985 (Canada)

Criminal Code Act 1995 (Cth)

Criminal Code Act 1899 (Qld)

Criminal Code Act 1924 (Tas)

Criminal Code Act Compilation Act 1913 (WA)

Criminal Justice and Public Order Act 1994 (UK)

Criminal Law Consolidation Act 1935 (SA)

Crown Entities Act 2004 (NZ)

Cyber-Safety Act 2013 (Nova Scotia)

Enhancing Online Safety for Children's Act 2015 (Cth)

Fair Work Act 2009 (Cth)

Harassment Act 1997 (NZ)

Harmful Digital Communications Act 2015 (NZ)

Harmful Digital Communications Bill 2014 (NZ)

Human Rights Act 1993 (NZ)

Malicious Communications Act 1998 (UK)

New Zealand Bill of Rights Act 1990 (NZ)

Official Information Act 1982 (NZ)

Ombudsmen Act 1975 (NZ)

Privacy Act 1993 (NZ)

Protection from Harassment Act 1997 (UK)

Public Records Act 2005 (NZ)

D *Other*

3News online, 'Charlotte Dawson speaks out about cyber bullying' (3News New Zealand, 3 September 2012) <http://www.3news.co.nz>

Australian Government, *Coalition's Policy to Enhance Online Safety for Children* (September 2013) < http://lpaweb-static.s3.amazonaws.com/Coalition%202013%20Election%20Policy%20-%20Enhance%20Online%20Safety%20for%20Children.pdf>

Australian Government, *Cybersmart. The Easy Guide to Socialising Online* <http://www.cybersmart.gov.au>

Australian Government Office of the Children's e-Safety Commissioner <https://www.esafety.gov.au/>

Australian Human Rights Commission, 'Cyberbullying: what is it and how to get help. Violence, Harassment and Bullying Fact sheet <https://www.humanrights.gov.au/cyberbullying-what-it-and-how-get-help-violence-harassment-and-bullying-fact-sheet>

Australian Standing Council on School Education and Early Childhood Development (SCSEEC), *National Safe Schools Framework* (2011) <http://www.safeschoolshub.edu.au/documents/nationalsafeschoolsframework.pdf >

Bullying Around the World, 30 August 2016, 'Bullying in Japan' <https://nobullying.com/bullying-in-japan-2/>

Cyber-bullying in Australia, 'Australian Cases, Cyberbullying in Australia', 2013 <https://cybercrime2013.wordpress.com/findings-and-research/australian-cases/>

Cyberbullying Research Center, 'Analysis and Implications of Laws' <http://cyberbullying.org/cyberbullying-laws>

End to Cyberbullying Organization, 'India Ranks Third on Global Cyber Bullying list', <http://www.endcyberbullying.org/india-ranks-third-on-global-cyber-bullying-list/>

Etymology Dictionary Online <http://www.etymonline.com/index.php?term=cyberspace >

FindLaw Team, 'Sexting' and Australian Law, FindLaw Australia, <http://www.findlaw.com.au/articles/4720/sexting-and-australian-law.aspx>

Henry Carus Associates, 'A Guide to Worldwide Bullying Laws' <https://www.hcalawyers.com.au/blog/bullying-laws-around-the-world/>

Internet Live Stats, 'Internet Users' < http://www.internetlivestats.com/internet-users/ >

Internet Live Stats, 'Internet users by Country 2016' <http://www.internetlivestats.com/internet-users-by-country/>

Internet Society <http://www.internetsociety.org >

Internet World Stats <http://www.internetworldstats.com/emarketing.htm >

Law Reform Committee, Inquiry into Sexting, Final Report (Parliament of Victoria, May 2013) <http://www.parliament.vic.gov.au/lawreform/article/944>

Magistrates' Court of Victoria Melbourne, Court Order B10510315, 13 April 2011

National Centre Against Bullying, 'Bullying Young People and the Law Symposium' (Victoria University Melbourne, 18-19 July 2013) <https://www.ncab.org.au/other/bullying-young-people-and-the-law-symposium-recommendations/>

Netsafe Cyberbullying New Zealand <http://www.cyberbullying.org.nz/>

New Zealand Law Commission Te Aka Matua O Te Ture <http://www.lawcom.govt.nz/about>

New Zealand Law Commission Te Aka Matua O Te Ture, *Harmful Digital Communications: The adequacy of the current sanctions and remedies* (Ministerial Briefing Paper, 2012)

New Zealand Law Commission Te Aka Matua O Te Ture*, The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age* <http://www.lawcom.govt.nz>

NCPC, National Crime Prevention Council, 'What is Cyberbullying?' (2016) <http://www.ncpc.org/topics/cyberbullying/what-is-cyberbullying>

NoBullying.com, 'Cyberbullying Statistics Australia, the Ultimate Guide' (22 December 2015) < https://nobullying.com/cyber-bullying-statistics-australia-the-ultimate-guide/>

NSPCC, 'Bullying and Cyberbulllying Facts and Statistics' (2016) <https://www.nspcc.org.uk>

OECD Centre for Educational Research and Innovation CERI, 'Cyber bullying' New Millenium Learners Blog <https://www.oecd.org/edu/ceri/centreforeducationalresearchandinnovationceri-thenewmilleniumlearnersblog.htm>

Power, Simon, New Zealand Law Commission Te Aka Matua O Te Ture, 'Review of Regulatory Gaps and the New Media', New Zealand Law Commission Issues Paper 27 (December 2011) <http://www.lawcom.govt.nz>

Sellenger Centre for Research in Law, Justice, and Social Change, Edith Cowan University, Australia < http://www.ecu.edu.au/research/research-showcase/>

US Department of Education's Office for Civil Rights <http://www2.ed.gov/about/offices/list/ocr/index.html>

US Department of Human Services, 'What is Bullying' <http://www.stopbullying.gov/what-is-bullying/definition/index.html >

US Department of Justice, Civil Rights Division < https://www.justice.gov/crt>

US Legal Definitions < http://definitions.uslegal.com/c/cyber-bullying/>

Victorian Law Reform, Law Reform Process < http://www.lawreform.vic.gov.au/our-approach/law-reform-process >