# Harmful online speech: An analysis of New Zealand's Harmful Digital Communications Act 2015 to combat cyberbullying

Myra E.J.B. Williamson[1]

*...there is a real, significant harm that can be caused through digital means. It is a new threat, and it is a very real, very serious threat that Parliament has to respond to...*[2]

## Introduction

In 2013, a schoolgirl in Auckland, New Zealand was hospitalized after she attempted to commit suicide.[3] Whilst at the hospital, the girl's mother picked up her daughter's phone and for the first time read some very nasty messages that her daughter had been receiving from other school students. The online communications had become so vicious that the girl had tried to end her own life. This is an example of the increasingly common real-life effect of harmful digital communications. This particular schoolgirl survived, others have not. In 2006, a 12 year-old teenage girl committed suicide in New Zealand. Her death was directly linked to an orchestrated campaign of email and text-bullying.[4] In Australia earlier this year, 14-year-old Amy 'Dolly' Everett—the Akubra hat girl—committed suicide after suffering from ongoing cyberbullying.[5] But it does not only affect children and young adults.[6] In April 2016, an American female firefighter, 31-year-old Nicole Mittendorff, committed suicide after suffering months of online harassment.[7] In the aftermath of her suicide, it became apparent that Mittendorff had been subjected to months of 'lurid, sexist comments' via



[1] BA, LL (Hons), LLM (Hons), PhD; Associate Professor of Law. The author can be contacted at drmyrawilliamson@gmail.com.

[2] This comment was made by the Minister responsible for the Harmful Digital Communications Act 2015, the Honourable Amy Adams, in the House of Representatives, prior to the bill's passing: (25 June 2015) 706 NZPD 4830 (Hon Amy Adams).

[3] Simon Collins, '13-year-old girl hospitalized after vicious cyber bullying' *New Zealand Herald* (10 September 2015) <http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11510529> accessed 27 February 2018.

[4] Simon O'Rourke, 'Teenage bullies hound 12-year-old to death' *New Zealand Herald* (13 March 2006) <http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10372137> accessed 4 March 2018. The girl lived in a small, rural NZ town called Putaruru. She had been receiving text messages threatening to 'beat her up' and saying things such as, 'You'd better not come to school because nobody likes you.'

[5] (no author), 'Cyberbullying blamed for Australian child model's suicide' *Associated Press* (12 January 2018) <https://wtop.com/australia/2018/01/cyberbullying-blamed-for-australian-child-models-suicide/> accessed 27 March 2018.

[6] In a 2016 New Zealand survey, it was found that three in five women in their late teens had been hurt or embarrassed online. Moreover, one in 10 people aged 30-59 have experienced it: Jamie Morton 'Rates of cyberbullying in New Zealand alarming' *NZ Herald* (28 March 2016) <http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11612551> accessed 28 March 2018.

[7] Cole Kazdin, 'Female Firefighter who Committed Suicide was a Target for Cyberbullies' *Broadly* (27 April 2016) <https://broadly.vice.com/en_us/article/ezjyze/female-firefighter-who-committed-suicide-was-a-target-for-cyberbullies> accessed 27 February 2018. Her body was found in the Shenendoah National Park in Virginia.

an anonymous, online gossip forum called the 'Fairfax Underground'.[8] The gossip was allegedly posted by her work colleagues (male firefighters).[9] Online harassment may have played a significant part in her decision to take her own life.[10]

The emotional harm caused by cyberbullying/online harassment is a relatively new problem brought about by almost universal access to the Internet[11] and to all forms of information and computer technology (ICT). Its increasing prevalence forces schools, universities, non-governmental organizations and governments to find effective ways to combat it.

*Structure of this paper*

This paper outlines New Zealand's experience with harmful digital communications and the legislative solutions that New Zealand has adopted. Part 1 explains the nature of the problem, definitional issues, and the NZ Law Commission's work. Part 2 describes NZ's main legal response, the Harmful Digital Communications Act 2015 (HDCA 2015). It also discusses the fear that a new law would stifle freedom of expression. Part 3 discusses some of the most important criminal cases decided in New Zealand under the HDCA 2015.[12] Part 4 contains a comparative analysis of legal responses in some other jurisdictions. Part 5 concludes with a summary of trends and a set of recommendations.

*About this paper: context and scope*

The scope of this paper is limited to the issue of harmful online speech, with a particular focus on New Zealand's response. Yet the constraint of online speech necessarily involves larger human rights questions, especially the rights to privacy and



[8] Peggy Fox, 'Mittendorff may have been the subject of cyber-bullying' *WASA-9* (25 April 2016) <http://www.wusa9.com/article/news/local/virginia/nicole-mittendorff-may-have-been-victim-of-cyberbullying/65-149881285> accessed 27 February 2018.

[9] *Ibid*. Forum users are anonymous so the authors of the posts cannot be confirmed.

[10] This has been a controversial aspect of the story. The Fairfax County Professional Firefighters and Paramedics, where Mitendorff worked, carried out an investigation after her death. At its completion, the Fire Chief released a statement (http://fairfaxfirefighters.org/news/415-response-to-anonymous-complaints-of-bullying-and-harassment) claiming that Mittendorff's suicide was not a result of any type of workplace harassment or cyberbullying. That statement was criticised by some members of Mitendorff's family: see Fox, *supra* n 8.

[11] Note: 'Internet' will be used when referring to the internet-working infrastructure while the adjective 'internet' will be used when describing technology and services relating to the Internet: see Chris Reed, *Internet Law – Text and Materials* (2nd ed. Cambridge University Press, 2004) at 7 n 3.

[12] "'Netsafe' was established in 1998 as an independent non-profit organization committed to improving community understanding of the internet and how to enhance safety and security online. It works with governmental and non-governmental organizations…': IP 27 n 222. Netsafe is funded by grants from government departments and private organizations. It is discussed in Part 2 below because it was given a new, expanded role under the HDCA 2015.

freedom of expression.[13] New Zealand regards free speech as the 'cornerstone of all other freedoms'.[14] Free speech is protected by statute: section 14 of the New Zealand Bill of Rights Act 1990 guarantees that every New Zealander has the right to freedom of expression, including the freedom to seek, receive and impart information and opinions of any kind, in any form.[15] That freedom is subject only to such 'reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society'.[16] Most countries have an equivalent provision in their constitutions. Although New Zealand protects this right in a normal statute (rather than in a written constitution), freedom of expression is taken seriously.[17]

New Zealand has a free and independent press. In the 2017 'Corruption Perceptions Index' New Zealand ranks number one – it is apparently the least corrupt country in the world.[18] In 2017, Reporters Without Borders ranked New Zealand 13th in the World Press Freedom Index.[19] There is a direct link between a free press and lack of corruption: countries with the least protection of the press tend to have the worst rates of corruption:[20]

> *We [Transparency International] found evidence to suggest that those countries that respect press freedom, encourage open dialogue, and allow for full participation of CSOs [civil society organisations] in the public arena tend to be more successful at controlling corruption. Conversely, countries that repress journalists, restrict civil liberties and seek to stifle civil society organisations typically score lower on the CPI.*



[13] For an excellent discussion of these wider issues see Saul and Martha C Nussbaum (eds) *The Offensive Internet – Speech, Privacy and Reputation* (Harvard University Press, 2010). For an Australian perspective, see Margaret Jackson and Gordon Hughes *Private Life in a Digital World* (Thomson Reuters, 2015). For a UK perspective, see Ian Lloyd *Cyber Law in the United Kingdom* (Wolters Kluwer, 2010).
[14] NZLC Issues Paper, para 7.60.
[15] New Zealand Bill of Rights Act 1990, s 14 <www.legislation.govt.nz/act/public/1990/0109/latest/DLM225513.html> accessed 1 March 2018.
[16] NZ Bill of Rights Act 1990, s 5.
[17] See discussion in Part 1 about concerns that the HDCA 2015 would stifle media freedom.
[18] Transparency International, 'Corruption Perceptions Index 2017' <https://www.transparency.org/news/feature/corruption_perceptions_index_2017> accessed 1 March 2018. New Zealand is ranked at the top ahead of Denmark, Finland and Norway. The best-ranked Arab country was the UAE at 21, followed by Qatar at 29, Saudi Arabia at 57, Jordan at 59, Oman at 69, Tunisia at 74, Morocco at 81, Kuwait at 85, Bahrain at 103, Algeria at 112, Egypt at 117, Lebanon at 143, Iraq at 169, Yemen at 175 and Syria at 178. A total of 180 countries were ranked.
[19] Reporters Without Borders, '2017 World Press Freedom Index' <https://rsf.org/en/ranking> accessed 1 March 2018. The top three places were occupied by Norway, Sweden and Finland in 2017. The best-ranked Arab country was Tunisia at 97, followed by Lebanon at 99, Kuwait at 104, UAE at 114, Qatar at 123, Oman at 126, Morocco at 133, Algeria at 134, Palestine at 135, Jordan at 138, Iraq at 158, Egypt at 161, Bahrain at 164, Iran at 165, Yemen at 166, Saudi Arabia at 168 and Syria at 177. A total of 180 countries were ranked.
[20] Transparency International, 'Digging Deeper into Corruption, Violence Against Journalists and Active Civil Society' (21 February 2018) <www.transparency.org/news/feature/digging_deeper_into_corruption_violence_against_journalists> accessed 4 March 2018.

As discussed in Part 1, the HDCA 2015, which was passed to address harmful online speech, did not seek to stifle journalists' freedom and, despite the initial fears, it does not seem to have any negative effect on freedom of expression.[21] Some countries do have cybercrime laws that specifically target the expression of political opinions online.[22] Typically, those countries rank poorly on measures of press freedom and have higher levels of public corruption.[23] Since freedom of the press was not the focus of the HDCA it is also not the focus of this paper, but it is highly relevant: any law that limits digital speech is a potential encroachment on that freedom. The narrow focus of this research is individuals' protection from harmful digital communications in the read/write web age.

## *PART 1 THE PROBLEM AND THE RESPONSE: A NEW ZEALAND PERSPECTIVE*

Cyber-bullying is one aspect of a much broader area of activity called 'cybercrime'. The umbrella term 'cybercrime' refers to 'any criminal activity that involves the Internet, a computer or other electronic device'.[24] 'Cybercrime' is a wide-ranging term and definitions vary.[25] It includes distributing malware, hacking, email-based fraud, online scams, online copyright breaches, stealing money, goods, information or data, as well as the possession of objectionable material. Cybercrime is also connected with traditional criminal activity (theft, drug smuggling, fraud, etc). Cybercrime is a major global problem. In 2017 alone, hackers stole $US172 billion from 978 million consumers in 20 countries.[26] From Millennials to baby-boomers, almost everyone is affected or knows someone affected, by cybercrime.[27] Kuwait apparently experienced

[21] See discussion in Part 1. Before it was passed into law, concerns were expressed that HDC bill would impinge on media freedom. The author has not found any articles since it was passed that would suggest journalists have felt compelled to change their reporting practices since it was passed.
[22] See discussion in Part 4.
[23] The correlation between high corruption and a lack of freedom of expression has been observed elsewhere including by Transparency International, *supra* n 20.
[24] New Zealand Police 'Electronic crime: what it is and how to report it' (no date) <www.police.govt.nz/advice/email-and-internet-safety/electronic-crime> accessed 28 February 2018.
[25] Symantech defines a cybercrime as, but not limited to, a number of specific actions, including identity theft, credit card fraud or having your account password compromised: Symantec Corporation, '2017 Norton Cyber Security Insights Report' 2017, 4 <http://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-US.pdf> accessed 3 March 2018, 29. The UK divides 'cybercrime' into two broad categories: **cyber-dependent** crimes and **cyber-enabled** crimes: Crown Prosecution Service 'Cybercrime – prosecution guideline' (no date) <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance> accessed 28 February 2018. Cyber-dependent crimes are 'crimes that can be committed only though the use of ICT devices' whereas cyber-enabled crimes are 'traditional crimes which can be increased in scale or reach by the use of computers' such as cyber-enabled theft.
[26] Symantec, *supra* n 25 at 4. On average, consumers globally have reported an average loss of $142 per victim and nearly 24 hours (or three full work days) dealing with the aftermath.
[27] *Ibid,* at 6. Symantec reports that although Millennials are the most technologically savvy, owning the most devices (four on average) and adopting advanced security practices (32%) like pattern matching, face recognition and two-factor authentication, one in four (26%) uses the same password for all accounts. Bad password management is one of the biggest mistakes made by victims of cybercrime.

a 170% increase in cybercrime from 2015 to 2016.[28] Cyberbullying or online harassment is just one subset of cybercrime - here the harm is mainly emotional, rather than economic. The 'harm' caused by cyberbullying is harder to measure and thus it may be over-looked by lawmakers.

*1.1 Definition*

Cyberbullying is bullying that takes place over digital devices such as phones, computers and tablets. It can occur through text messages, apps, online in social media, forums or gaming.[29] Some definitions[30] use age to draw a distinction between cyberbullying and online harassment; others do not.[31] The definition used in *this* paper is the definition used by the New Zealand non-governmental organization, Netsafe:[32]

> *Online bullying (also known as cyberbullying) is when a person uses digital technology to send, post or publish content with the intention to harm another person or a group. This behavior is often aggressive, repeated and involves some kind of power imbalance between the people involved (emphasis added)*

Cyberbullying can affect anyone and it can take many different forms: 'name calling online, repeated unwanted online messages, spreading rumours or lies, [setting up] fake accounts used to harass people, excluding people from social activities, [posting] embarrassing pictures, videos, websites or fake profiles.'[33] New Zealand has experienced all of these. Although the focus in this paper is New Zealand, the problem of cyberbullying is a global problem. It affects people of all ages, and in many different settings, including schools and universities. Reputations can be damaged permanently by material posted online (whether true or not).[34] Personal relationships,



[28] According to the Undersecretary of the Ministry of Interior of Kuwait, Cybercrime increased by 170% in 2016 and a 15% decrease in traffic accidents': *Al Anbaa* (2017) [in Arabic] <www.alanba.com.kw/ar/kuwait-news/incidents-issues/> accessed 28 February 2018.

[29] See Stopbullying.gov 'What is cyberbullying' <www.stopbullying.gov/cyberbullying/what-is-it/index.html> accessed 24 March 2018. This is an official website of the US Government.

[30] For example, Judge David Harvey defines cyberbullying as 'when a child, pre-teen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, pre-teen or teen using the Internet, interactive and digital technologies or mobile phones. It has a minor on both sides.' Once an adult is involved, he terms it 'cyberharassment' or 'cyberstalking'. He discusses the definitional lines in much more detail than is warranted in this paper. See David Harvey *Internet.law.nz - Selected Issues* (4th edn LexisNexis, 2015) 112-15.

[31] The US Department of Health and Human Services defines cyberbullying as the sending, posting or sharing of negative, harmful, false or mean content about someone else. No mention is made of age: see Stopbullying.gov, *supra* n 29.

[32] Netsafe, 'Online bullying advice' (21 February 2017) <https://www.netsafe.org.nz/online-bullying/> accessed 28 February 2018.

[33] *Ibid.*

[34] Examples abound of students harming the reputations of other students, instructors and professors in universities in the US. For instance, at Syracuse University, sixteen students joined a Facebook group solely devoted to criticizing an English doctoral student teaching a writing class. Four of the students were expelled and placed under 'disciplinary reprimand' for crude comments: Rob Capriccioso, 'Facebook Face Off' *Inside Higher Ed* (14 February 2006) <https://www.insidehighered.com/news/2006/02/14/facebook> accessed 27 March 2018, as cited in Karen M Bradshaw

emotional well-being and future employment opportunities can be irreparably damaged by postings on online discussion groups and message boards.[35]

*1.2 The New Zealand Law Commission's review of harmful digital communications*

In October 2010, the New Zealand Law Commission (NZLC) was asked to 'review the adequacy of the regulatory environment in which New Zealand's news media is operating in the digital era'.[36] In December 2011, it released an 'Issues Paper' (IP 27) with two parts. Part 1, 'The News Media Meets "New Media"', examined the issues of fundamental importance to the future of news media and the rights, responsibilities, protections and privileges that should be afforded to digital journalists (e.g. bloggers). Part 2, 'Speech Harms: The Adequacy of the Current Legal Sanctions and Remedies', is directly relevant to this paper. The NZLC observed that:

> *The vast majority of New Zealanders publishing on the Internet will not be within the regulatory system we have proposed for the news media…they will be able to exercise complete freedom of speech…they can, without fear of a regulator, be inaccurate in their facts, unbalanced in their coverage and extreme in their opinions…but…they will remain subject to the law.*

The NZLC stated that 'before the advent of the web the risk of causing harm to others through the exercise of free speech was most commonly a question that concerned the media rather than ordinary citizens.'[37] Now that 'everyone has the power to publish, these risks – and potential harms – are much more widely shared.'[38] The Internet creates a tension between free speech rights and the need for some restraint of those rights.[39] The NZLC also noted that 'those who exercise their free speech to intimidate, bully, denigrate and harass others on the Internet lessen the credibility of free speech arguments.'[40] Although people harmed by abusive speech on the web have the opportunity to exercise their right of reply, 'not all have the courage or the standing to

---

and Souvik Saha 'Academic Administrators and the Challenge of Social-Networking Websites' in Levmore and Nussbaum, *supra* n 13 at 144 and 148.

[35] Capriccioso, *ibid*, recalls that the Syracuse students had created an online discussion group devoted to discussing one particular Teaching Assistant, and they called the group 'Clearly, Rachel doesn't know what she's doing, ever'. They posted a picture of the Teaching Assistant (an English doctoral student at the university) with comments such as, 'Rachel, I'm sorry, you really suck.' Some academics criticized Syracuse for the 'disciplinary reprimand' handed out to the students, stating that the speech was 'juvenile, stupid and distasteful but fully protected [by the First Amendment to the US Constitution].'

[36] The New Zealand Law Commission, 'The News Media Meets "New Media": Rights, Responsibilities and Regulation in the Digital Age' Issues Paper 27 (December 2011) <www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20IP27.pdf> accessed 28 February 2018 [hereinafter IP 27].

[37] IP 27, para 7.3.

[38] IP 27, para 7.3.

[39] IP 27, para 7.4

[40] IP 27para 7.5.

exercise it. In effect, those who exercise their free speech rights to cause harm may inhibit others from participating freely in this vital new public domain.'[41]

Although existing laws imposed constraints on certain types of speech, most of those laws were drafted in the pre-digital era. The NZLC posed the question: are the existing criminal and civil remedies for wrongs such as defamation, harassment, breach of confidence and privacy effective in the new media environment and if not, what are the alternative remedies?[42] The overall answer to that question was 'no'. The NZLC provided many insightful observations.[43] First, with regard to '[h]arassment, defamation, hate speech and invasions of privacy – all these abuses of free speech predated the internet'.[44] However, the Internet has introduced new dimensions to these harms and amplified their harmful consequences.[45] Secondly, the fact that anything written on the Internet can be manipulated and disseminated so easily and so quickly is a new challenge. And this power is available to anyone who has access to the Internet: 'social media sites do more than simply replicate the dynamics of the school playground or the workplace lunchroom. They provide an **unprecedented vehicle for the distribution of gossip and information,** enabling malevolent uses to target a victim's social network simultaneously.'[46] Thirdly, damaging content can be difficult, if not impossible, to completely remove.[47] Harmful content can continue to cause damage long after the original publication. Fourthly, practical anonymity can encourage abusive speech and it can shelter the abuser from any consequences for their actions.[48]

*1.3 Quantifying the harm: how many people are affected? To whom do they complain?*
In 2011, the NZLC acknowledged that it was probably impossible to quantify how many New Zealanders had been significantly affected by abusive publishing.[49] That is because the breadth of harm is so wide, it encompasses so many different forms, and because there is no 'central repository' for recording adverse events.[50] People who have suffered harm have complained to different entities including the NZ Police, the

[41] IP 27 para 7.5.
[42] IP 27 para 7.6.
[43] In the course of preparing IP 27, the NZLC consulted the NZ Police, the Solicitor-General's Office, the Privacy Commissioner, the Human Rights Commission, Netsafe, Facebook, Google and Trade Me (a New Zealand website for buying and selling goods, advertising property and jobs, New Zealand's most visited website).
[44] IP 27, para 7.10.
[45] IP 27 para 7.11.
[46] IP 27 para 7.12 (emphasis added).
[47] IP 27 para 7.12.
[48] IP 27 para 7.15.
[49] IP 27 para 7.18.
[50] IP 27para 7.18.

Privacy Commissioner, the Human Rights Commissioner and Netsafe. Other countries, such as Kuwait, have a similar problem in not having accurate measures of the problem, in part because 'no official monitoring bodies produce independent, reliable statistics on a regular basis.'[51]

Many different studies and statistics are available. In 2008, an Australian researcher claimed that 'one in three children are affected by online bullying'.[52] Another report stated that one in five New Zealanders aged 13-30 have experienced harmful communication on the Internet.[53] In the UK, a 2017 study reported that in the previous year, 17% of 12-20 year olds had experienced cyberbullying.[54] For those who *had* experienced it, the incidents were often repetitive: 29% of those who had suffered cyberbullying in the UK reported experiencing it at least once a month.[55] More than a third had a nasty comment posted about their profile or about a photo and 68% had received a nasty message. Cyberbullying has a negative impact on victims' health: anxiety, depression and suicidal feelings were mentioned by more than a third.[56] Many countries might not have carried out such research: they may have a similar problem that is as yet under-reported.

Incidents of cyberbullying/online harassment have often come to the attention of the **NZ Police.** In 2007, police protection was provided to government workers who were named in threatening and derogatory posts on a website.[57] In 2010, NZ Police investigated a man who posted death threats on Facebook.[58] The **NZ Privacy**



[51] Joyce Hakmeh 'Cybercrime and the Digital Economy in the GCC Countries' *Chatham House* (June 2017) <www.chathamhouse.org/sites/files/chathamhouse/publications/research/2017-06-30-cybercrime-digital-economy-gcc-hakmeh.pdf> accessed 22 March 2018, at 5.

[52] James Ihaka, 'Online bullying affects 1 in 3 children' *NZ Herald* (10 July 2008) <www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10520847> accessed 7 March 2018. Ihaka was referring to a study by Dr Martin Wild, a cyber-safety expert from Australia who found that 35% of children surfing the web had been bullied, are bullies, or both.

[53] Amy Adams, Minister of Justice 'Digital Communications Bill will safeguard free speech, not curtail it' *Stuff* (2 July 2015) <www.stuff.co.nz/the-press/opinion/69873428/digital-communications-bill-will-safeguard-free-speech-not-curtail-it> accessed 7 March 2018.

[54] Ditch the Label, 'The Annual Bullying Survey 2017' (July 2017) <www.ditchthelabel.org/wp-content/uploads/2017/07/The-Annual-Bullying-Survey-2017-1.pdf> accessed 20 March 2018, 23.

[55] *Ibid,* 24.

[56] *Ibid,* 25.

[57] IP 27, para 7.22. The government social workers were personally identified on a website called 'CYFSWatch'. The name of the website refers to the government department that was previously called 'Children, Young Persons and Their Families' or CYFS'. According to the NZLC, the Ministry of Social Development complained to Google about the site and it was closed, but the content was then posted on mirror sites. Currently, a blog is being used for the same purpose. Its raison detra, as stated on the blog, is that "its better to NAME and SHAME the bad social workers rather than tarring all social workers with the same brush": Watching CYFSWatch <https://watchingcyfs.wordpress.com/cyfswatch-hall-of-shame/> accessed 2 March 2018. Note that although individuals' names are visible on the blog, the site's hosting expired on 1 March 2018 so none of the links to the blog posts are currently working.

[58] IP 27 para 7.22. See Rachel Taylor, 'Dunedin arrest after Facebook death threats' *Otago Daily Times* (23 June 2010) <www.odt.co.nz/news/dunedin/dunedin-arrest-after-facebook-death-threats> accessed 3 March 2018.

**Commissioner** has also received many complaints involving the misuse of 'personal information in the context of family or personal relationship conflicts, including for example the posting of incriminating photographs on social networking sites.'[59] The **Human Rights Commissioner** has received complaints: between January 2008 and June 2011 it received 110 complaints relating to potentially discriminatory content on websites. Of those, 30 related to content hosted on NZ sites and the remainder were posted on overseas sites - predominantly on Facebook.[60] If the content was posted on an overseas site, the Human Rights Commission declined jurisdiction. **Netsafe,** an independent non-governmental NZ organization, is the fourth and final recipient of complaints concerning online abuse. It logged 1,279 inquiries between April 2009 and June 2011:[61]

> *Text and cyber-bullying accounted for a significant portion of these, together with incidents involving the misuse of social networking site to victimise, harass, defame or intimidate individuals. Cyber-bullying and harassment took a number of forms including emails, texts, phone messages, blog sites and forums.*

Netsafe found that sites were often used to launch attacks on people's reputation, spreading damaging rumours and publishing invasive or distressing photos or videos. Netsafe had received a number of complaints from parents and schools about the proliferation of Facebook sites used to publish 'derogatory and often sexually explicit rumours about students…ultimately these were thought to have played some parts in the suicide of a young girl.[62] The establishment of fake Facebook pages for malicious purposes featured prominently in complaints dealt with by Netsafe, which was sometimes successful in having the pages taken down. On other occasions, neither Netsafe nor the complainant, were able to have the site/content removed.[63] Overall, looking at the information provided by Netsafe, the NZLC noted some disturbing trends. Many of the incidents—including online impersonation and smear campaigns—were specifically designed to intimidate and cause psychological distress.



[59] IP 27, para 7.25ff. In many cases, the Privacy Commissioner could not intervene because s 56 of the Privacy Act 1993 (pre-2015) exempted any information held in connection with *personal affairs* from the Act. The NZLC recommended that the Privacy Act 1993 be amended. That recommendation was adopted by Parliament and subsection 2 was added to s 56 of the Privacy Act 1993.
[60] IP 27 para 7.30-7.33.
[61] IP 27para 7.38.
[62] IP 27para 7.40-41.
[63] For example, a secondary school principal fought a year long battle, unsuccessfully, to have a fake Facebook page taken down which purportedly belonged to a teacher. The original site contained lewd comments, which were both distressing and damaging to the teacher concerned. Despite repeated reports to Facebook, the page remained: IP 27, para 7.41.

It also noted that female students were frequently targeted in a sexually derogatory manner.[64]

*1.4 Legal and non-legal remedies for allegedly harmful online speech*

The NZLC reviewed all existing avenues of legal redress including criminal remedies (eg. offences against the Crimes Act, contempt of court, harassment) and civil remedies (eg. defamation and breach of privacy). It also looked at non-legal remedies such as approaching the content owner (for example, a person who has posted a video to Youtube) to take down the offensive publication, community moderating and reporting, and using the self-regulatory systems that already exist within large tech companies, such as Facebook and Google, to take-down content.[65] Governments make 'take-down requests' from such companies for many reasons.[66] A government may allege that content is defamatory of its citizens, or that content violates local laws which prohibit hate speech or adult content (for example, pornography), or that the content violates court orders (for example, the content identifies a person who cannot be identified).[67] The number of 'take-down requests' made by governments to tech companies is growing.[68] Private individuals sometimes request take-downs too; many of these are collected and are accessible (with redactions) from sites such as Lumen.[69] For example, on 6 October 2016 a Kuwaiti individual asked Google to remove a page from 'Arabian Business' – the allegation was that the online business news article was defamatory.[70] The article referred to two high-profile Kuwaiti families (the Al Roumis



[64] IP 27 7.59. This point is mentioned again in this paper, *infra,* at n 191.

[65] Since 2009, Google has voluntarily posted 6-monthly 'transparency reports' which indicate how many requests it has received from law enforcement agencies worldwide. Many of these requests are to assist governments in their own law enforcement efforts. However, since December 2017 Google has been releasing data on requests from governments to *remove content* from services like YouTube and Blogger: Google, 'Google Transparency Report – Recent Updates' 7 December 2017 <https://transparencyreport.google.com/about> accessed 3 March 2018.

[66] A 'take-down request', also called a notice and take down request, is a procedure for asking Internet Service Providers (ISPs) or search engines to remove or disable access to illegal, irrelevant or outdated information: see Margaret Rouse, 'Definition take-down request' *Techtarget.com* (no date) <http://searchcontentmanagement.techtarget.com/definition/take-down-request> accessed 27 March 2018.

[67] Google, 'Transparency Report – Government requests to remove content', 7 December 2019 <https://transparencyreport.google.com/government-removals/overview> accessed 3 March 2018. Note that the Google Transparency Report's data only includes requests from governments.

[68] From January to June 2017 Google received 19,176 requests from governments around the world to remove 76,714 pieces of content. That was a 20% increase in removals over the second half of 2016: Richard Salgado, 'New government removals and National Security Letter data' Google blog, 7 December 2017 <www.blog.google/topics/public-policy/new-government-removals-and-national-security-letter-data/> accessed 3 March 2018.

[69] The Lumen database includes takedown request from individuals and governments to a variety of websites including Google. Lumen's 'The Takedown Project' is a collaborative research project housed at the US-Berkeley School of Law and the American Assembly to study notice and takedown procedures. Researchers in the US, Europe and other countries are working collaboratively to understand this fundamental regulatory system for global online speech': The Takedown project, <http://takedownproject.org/> accessed 3 March 2018.

[70] Lumen database, complaint from 'Unknown' re allegedly defamatory material <www.lumendatabase.org/notices/13143847> accessed 4 March 2018.

and the Al Humaidhis) who were being sued in the UK because of their default on a $60 million loan. Google received the take-down request and the URL, but decided it was not defamatory (no court judgment was attached) and Google chose not to remove the URL.[71]

The Google Transparency Report allows users to search by country to see the take-down requests made by individual countries – and the reasons for those requests.[72] Any user can search the data on any country.[73] This data is enormously interesting: the reasons why governments make requests from Google to take down content tells a story in itself. However, for the purposes of this paper, this data shows that non-legal remedies—such as asking a site to take-down content from its products—can be a fast and effective solution *if* that site has a sound process in place for considering removals. However, success might involve the judicial process to first obtain a court order, or it might involve a government agency, such as the police, writing a letter on official letterhead.[74] On the downside, the requestor is at the mercy of the site. There is a lot of discretion on the company's part in framing their removals policy and making decisions on individual requests.[75] Whether a post violates 'community standards' is a decision made by the individual tech company. Before moving on, it is noteworthy that Google has been followed by other consumer tech companies such as Twitter and



[71] The URL which the Kuwaiti complainant wanted removed refers to a news story in Arabian Business which is still accessible: Beatrice Thomas 'Wealthy Kuwaiti families embroiled in UK lawsuit over $60 m loan' 30 June 2014 <www.arabianbusiness.com/wealthy-kuwaiti-families-embroiled-in-uk-lawsuit-over-60m-loan-555830.html> accessed 4 March 2018.

[72] For example, the New Zealand government has made 64 requests since 2009 for the removal of 277 items. One request may involve a number of different items across different services such as YouTube, web searches, blogs and others. The first three are the products with the most frequent government requests to remove content: Google, 'Transparency Report - Government requests to remove content' December 2017 <https://transparencyreport.google.com/government-removals/overview?authority_search=country:new%20zealand&lu=authority_search> accessed 3 March 2017. As a point of comparison, Kuwait made 3 requests for 4 items to removed in that same period: Google, 'Transparency Report – Kuwait' December 2017 <https://transparencyreport.google.com/government-removals/by-country/KW> accessed 3 March 2018. One request for removal was made in 2013 for a copyright infringement, one was made in the first 6 months of 2016 for government criticism and one in the second half of 2016 for privacy and security. The 2013 copyright request was granted. The 2016 government criticism request was not granted. The 2016 privacy and security request was granted. All requests were made by Kuwait's executive branch of government.

[73] Google, 'Transparency Report – Government request to remove content' 7 December 2018 <https://transparencyreport.google.com/government-removals/by-country> accessed 3 March 2018.

[74] Google, 'Transparency Report - Government request to remove content' 7 December 2018 <https://transparencyreport.google.com/government-removals/overview?removal_reasons=reason:8&lu=removal_reasons> accessed 3 March 2018. Google says that they 'always assess the legitimacy and completeness of a government request…it must be in writing, as specific as possible about the content to be removed and clear in its explanation of how the content is illegal.' They note that 'sometimes written letters from agencies aren't sufficient and a court order is necessary…but from time to time we receive forged court orders…[court orders] often do not compel Google to take any action.'

[75] Facebook has come under a lot of criticism for its decisions to both take down legal content and for its refusals to take down offensive content: see for instance the controversy involving Anas Modamani in Germany

Facebook in providing transparency over take-down requests.[76] The data on take-down requests is very informative to any freedom of expression analysis involving the Internet.[77] It is submitted that take-down procedures and policies are likely to be a growth area for both lawyers and legal research as different jurisdictions' and different companies' interpretations of free speech clash.[78]

*1.5 The NZLC recommendations – gaps and remedies*

The NZLC's comprehensive review of New Zealand laws resulted in many findings, including that:[79]

- Significant harms are experienced as a result of the abusive and sometimes malicious use of the Internet as a publishing platform.
- Young people are particularly susceptible but the problems are not confined to the young.
- The various forms of cyber harassment can have an immensely debilitating effect on people's well-being and may impact their professional lives.
- Existing criminal and civil law is capable of dealing with many of the types of harmful communication but the current law is not always capable of addressing the new and potentially more damaging ways of using communication to harm others.
- The public can experience difficulties accessing the law.
- Legal remedies are important but many social media sites rely on a combination of internal controls, backed by community monitoring and reporting systems, to deal with harmful speech.
- Empirical information is lacking about the effectiveness of the self-regulatory systems.
- There 'really needs to be a way for people to get faster takedowns across the board.'[80]

[76] See Twitter, 'Transparency Report - Removal requests' (January-June 2017) <https://transparency.twitter.com/en/removal-requests.html#removal-requests-jan-jun-2017> accessed 3 March 2018.

[77] For instance, see the OpenNet Initiative <https://opennet.net/>, which provides data and reports on governmental attempts at controlling and filtering the internet. See also the Lumen database <www.lumendatabase.org/>. Lumen is an independent 3rd party research project studying 'cease and desist' letters concerning online content. It collects and analyses legal complaints and requests for removal of online materials helping Internet users to know their rights and understand the law': see Lumen 'About Us'<www.lumendatabase.org/pages/about> accessed 3 March 2018. The Lumen database contains 'millions of notices, some of them with valid legal basis, some of them without, and some on the murky border.' Lumen is a unique collaboration among law school clinics and the Electronic Frontier Foundation.

[78] For example, on 1 October 2017, a new law came into effect in Germany (the 'NetzDG' law),which forces social-media platforms such as Google and Facebook to takedown 'obviously illegal' material within 24 hours of being notified (and 7 days if it is less obviously illegal). Failure to comply can result in fines of up to 50 million euros. Facebook opposes the law and the US First Amendment right to free speech looks headed for confrontation with Germany's more restrictive interpretation of free speech rights: see Geoffrey Smith 'Germany's New Law is a Milestone for Social Media Regulation in Europe' *Fortune* (30 June 2017) <http://fortune.com/2017/06/30/germany-law-social-media-hate/> accessed 25 March 2018.

[79] These points paraphrase the analysis at NZLC IP 27 paras 7.172-7.177.

In response to those problems the NZLC made recommendations including amending several existing laws.[81] It suggested a new criminal offence to cover the problem of intimate photographs because the NZLC said there was a 'gap' in the law. It said a new criminal offence should cover situations where a former partner posts intimate pictures of the other on the Internet (whether or not the images were taken with permission) without permission. It also recommended that incitement to commit suicide should be a crime even if the person does not attempt to do so. Those changes have been enacted. The NZLC also said that a court or tribunal should be empowered to issue 'takedown orders' against ISPs and website hosts, irrespective of their legal responsibility for the content.[82] A swift and reasonably effective remedy needs to be available. This remedy would not be readily available to the Crown. Any order should require the ISP or website host to take reasonable steps to remove the item. Other suggestions included considering whether a Communications Tribunal is needed;[83] creating a single 'one stop shop' for complaints;[84] and possibly establishing an independent commissioner to whom members of the public can turn to for information and assistance (if a tribunal is not established).[85] That is a very brief summary of the detailed recommendations made by the NZLC in its Issues Paper 27 of 2011. Part 2 below describes Parliament's legislative response.

## *PART 2 – THE NEW NZ LEGISLATIVE FRAMEWORK FOR COMBATTING CYBERBULLYING*

### *2.1 Outcome of the law reform process*

After the publication of the Issues Paper, the public was invited to make submissions on the proposals. There was a 4-month consultation period (December 2011 - March



[80] IP 27, para 8.49.

[81] It recommended amending the Harassment Act 1997. It was amended, so that 'making contact' with a person includes making *electronic* contact. Also, placing offensive material where it can be found now includes placing it on electronic media. Section 4(1)(d) was amended and s 4(1)(ea) was inserted by the HDCA 2015 s 33(1) and s33(2) <www.legislation.govt.nz/act/public/1997/0092/28.0/DLM417726.html> accessed 4 March 2018. See the recommendations made the NZLC IP 27 at paras 8.15-8.16. The NZLC also recommended amending the Human Rights Act in IP 27, para 8.23. The recommendation was implemented by the HDCA 2015, s63(2)(k) (racial harassment) and s63(2)(k) (sexual harassment). It also recommended amending the Defamation Act 1992 in IP 27, para 8.34. 'Internet Service Provides' (ISPs) are now included as 'distributors' in s2(1) of the Defamation Act.

[82] IP 27, para 8.35

[83] A 'Communications Tribunal' could be placed at a lower level than the court system to administer speedy, efficient and relatively cheap justice to those who have been significantly damaged by communications in media of all kinds. It would not become a censorship body. It could make orders only when the law had been broken and demonstrable harm had been caused (financial, psychological harm such as distress, intimidation, humiliation or fear for safety). The tribunal's purpose would be to redress harm to individuals in their personal capacity: IP 27, paras 8.44-8.57.

[84] IP 27, para 8.49-50.

[85] Neither a Communications Tribunal nor an independent commissioner were established, but Netsafe was appointed as the Approved Agency and given wide-ranging powers to receive complaints and act on them.

2012). The Law Commission received 72 submissions.[86] A list of the submitters is publicly available with links to their submissions.[87] During the consultation period, Coroners, Police and the Post Primary Teachers Association all expressed concern 'about the ways in which the abuse of communication technologies was contributing to truancy, school failure and a range of adolescent problems including depression, self-harm and suicide.' [88] There was significant public support for the recommendations concerning harmful online speech. [89] Therefore, the Minister responsible for the Law Commission asked the Law Commission to fast-track the part of its project dealing with harmful digital communications. The final set of recommendations were set forth in a Ministerial Briefing Paper accompanied by a Draft Bill.[90] The Ministerial Briefing Paper proposed many solutions, including the creation of a new electronic communications offence, which is the focus here.[91]

*2.2 From bill to law*

On 5 November 2013, the Harmful Digital Communications Bill was introduced to the New Zealand Parliament.[92] It passed its First Reading on 3 December 2013. It was then sent to the Justice and Electoral Select Committee. At its First Reading, MP Hon Chester Burrows (Acting Minister of Justice) noted that:[93]

> *A digital age has meant that tormentors can harass their target anywhere, at any time, and the trails of abuse remain in cyberspace forever. Research suggests that as many as one in 10*

[86] NZLC 'Regulatory Gaps and the New Media' <www.lawcom.govt.nz/our-projects/regulatory-gaps-and-new-media> accessed 4 March 2018.
[87] Submissions on IP 27, <www.lawcom.govt.nz/sites/default/files/submissionAttachments/0%20Website%20list%20of%20submitters%20final_0.pdf> accessed 4 March 2018.
[88] NZLC 'The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age' 22 March 2013 <www.lawcom.govt.nz/our-projects/regulatory-gaps-and-new-media> accessed 5 March 2018 [hereinafter NZLC R128] para 1.15.
[89] The NZLC subsequently prepared a full report setting out its recommendations, published in March 2013. However, most of that report focused solely on concerns over the new media. The Law Commission made 32 recommendations regarding how to regulate the new media, but none of them were taken up by the government: 'The Government response thanks the Law Commission for the Report and notes that the Government's preference is not to make any statutory or institutional changes at this time and to continue to observe how issues of technological convergence are dealt with by the news media.': Government response to the Law Commission Report on the News Media Meets "New Media": Rights, Responsibilities and Regulation in the Digital Age' <www.lawcom.govt.nz/sites/default/files/governmentResponseAttachments/News-media-meets-new-media-government-response-to-law-commission-report%20%28D-0503423%29.PDF> accessed 5 March 2018.
[90] NZLC 'Regulatory Gaps and the New Media' 15 August 2012 <www.lawcom.govt.nz/our-projects/regulatory-gaps-and-new-media> accessed 5 March 2018.
[91] NZLC, R128, *supra* n 88, para 1.18.
[92] Harmful Digital Communications Bill, Government Bill 168-3, www.legislation.govt.nz/bill/government/2013/0168/latest/DLM5711810.html accessed 5 March 2018 [hereinafter the HDC Bill].
[93] HDC Bill, First Reading, Chester Borrows, *Hansard,* Vol 694, p14747 <www.parliament.nz/en/pb/hansard-debates/rhr/document/50HansD_20131114_00000024/harmful-digital-communications-bill-first-reading> accessed 5 March 2018.

> *New Zealanders has personal experience of harmful communications on the internet. In 2007…one in five adolescents experienced some form of cyber-bullying or harassment that year.*

The Committee produced its report on 27 May 2014 and then the Bill returned to Parliament for its Second Reading on 24 March 2015. It was read in the Committee of the Whole House on 23 June 2016, passed its Third Reading (a formality) on 30 June 2015 and was signed by the Governor-General on 2 July 2015.[94] It became law the day after gaining Royal Assent, on 3 July 2015, but different parts came into effect at different times. The civil enforcement regime came into effect in November 2016.

*2.3 The new HDCA Act – the key provisions*

**2.3.1 Purpose**

The Harmful Digital Communications Act 2015 (HDCA 2015) was passed with two objectives: (a) to deter, prevent and mitigate harm caused to individuals by digital communications; and (b) provide victims of harmful digital communications with a quick and efficient means of redress.[95]

**2.3.2 Definitions**

The Act provides a definition of a **digital communication.** It means 'any form of electronic communication'. It includes 'any text message, writing, photograph, picture, recording, or other matter that is communicated electronically.'[96]

The meaning of 'harm' is defined as 'serious emotional distress'.[97] How the NZ courts have interpreted this term is discussed below in Part 3.

An 'intimate visual recording' is separately defined in the HDCA. It means any visual recording (a photograph, videotape or digital image) in any medium using any device *with or without the knowledge or consent of the individual* who is the subject of the recording, in a place where there would reasonably be expected to be privacy. There



[94] The progression of the HDC Bill together with the *Hansard* debates, Supplementary Order Papers, submissions and Final Report of the Select Committee and videos of the Parliamentary debate can all be accessed here: <www.parliament.nz/en/pb/bills-and-laws/bills-proposed-laws/document/00DBHOH_BILL12843_1/tab/hansard> accessed 5 March 2018.
[95] Harmful Digital Communications Act 2015 http://www.legislation.govt.nz/act/public/2015/0063/latest/DLM5711810.html accessed 5 March 2018, s 3 'Purpose'.
[96] HDCA 2015, s 4 'digital communication'.
[97] HDCA 2015, s 4 ' 'harm'.

are further qualifying attributes, which need not be detailed at this point.[98] Retention or storage is not required to satisfy the definition.

### 2.3.3 The 10 "Communication principles"

The HDCA 2015 contains 10 communication principles.[99] Digital communications should not breach any of them. Netsafe and the District Court **must** take these principles into account when determining if the Act has been breached.[100] The 10 communications 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 position of the affected individual.
- Principle 4: A digital communication should not be indecent or obscene.
- Principle 5: A digital communication should not be used to harass an individual.
- Principle 6: A digital communication should not make a false allegation.
- Principle 7: A digital communication should not contain matter that is published in breach of confidence.
- Principle 8 A digital communication should not incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual.
- Principle 9: A digital communication should not incite or encourage an individual to commit suicide.
- Principle 10: A digital communication should not denigrate an individual by reason or his or her colour, race, ethnic or national origins, religion, gender, sexual orientation, or disability.

The principles were derived from existing criminal and civil laws. They are an attempt to make it easier for the public to grasp the legal rights and responsibilities that attach to the use of digital communications.[101]

### 2.3.4 The role of Netsafe

[98] See the full definition of an 'intimate visual recording' in the HDCA 2015, s 4, <www.legislation.govt.nz/act/public/2015/0063/latest/whole.html#DLM5711818> accessed 22 March 2018.
[99] HDCA 2015, s 6(1).
[100] HDCA 2015, s 6(2) mandates that the Approved Agency and the courts must take the communication principles into account when performing functions or exercising powers under the Act.
[101] Sally Carter 'The Harmful Digital Communications Act 2015- Two Years On' in NZLS CLE *Cyber Law – Applying Cyber to the Real World* (April 2017)

Although there needs to be the option to go to court, for most people, using court processes is time-consuming, expensive and intimidating. A faster, cheaper solution was devised to deal with the vast majority of complaints. The HDCA 2015 provided for the future appointment of an 'Approved Agency' and Netsafe was subsequently appointed.[102] Netsafe is an independent, not-for-profit and non-governmental organisation that has existed since 1998.[103] It aims to educate New Zealanders about using information and communications technology safely, securely, and responsibly.[104] Netsafe now has a key statutory role in preventing and addressing online harassment in New Zealand with the power:[105]

> *(a) To receive and assess complaints about harm caused to individuals by digital communications;*
> *(b) To investigate complaints;*
> *(c) To use advice, negotiation, mediation and persuasion (as appropriate) to resolve complaints;*
> *(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) ...*

Netsafe is a free-to-use 'triage' service, which assesses what should happen with any complaint.[106] Netsafe has the power to *refuse* or *cease* investigating any complaint if the complaint is trivial, frivolous or vexatious, if the subject matter of the complaint is unlikely to cause harm to an individual, or if the complaint does not contravene the communication principles.[107] It might not take any further action if it appears that any further action is unnecessary or inappropriate.[108] No one can apply for a court order without having first made a complaint to Netsafe.[109] If Netsafe decides to take no further action, it has to tell the complainant that they can still apply to the District Court for a court order.[110] Netsafe sometimes refers a complainant to the Police if they think that criminal prosecution is a possibility.[111] Netsafe has reported that they are receiving a greater number of complaints now than in the years before the Act was

[102] Netsafe's current expanded role under the HDCA was announced on 31 May 2016 and it began its new role in November 2016.
[103] Netsafe, 'About Netsafe' <www.netsafe.org.nz/aboutnetsafe/> accessed 24 March 2018.
[104] Netsafe's submission to the NZLC on NZLC IP27 (24 February 2012) <http://www.lawcom.govt.nz/sites/default/files/submissionAttachments/39%20NetSafe.pdf> accessed 24 March 2018.
[105] HDCA 2015 s 8 sets out the powers and functions of the Approved Agency.
[106] Netsafe advocated for such an agency in its submission to the Select Committee on IP27 when it suggested that there needed to be a pre-tribunal triaging process to contact alleged offenders and explore what other measures are available to address the speech abuses: see Netsafe, submission to the NZLC on IP27, 24 February 2012, <www.lawcom.govt.nz/sites/default/files/submissionAttachments/39%20NetSafe.pdf> accessed 6 March 2018.
[107] HDCA 2015 s 8(3).
[108] HDCA 2015 s 8(4).
[109] HDCA 2015 s 12(1).
[110] HDCA 2015 s 8(5).
[111] Email from Sean Lyons, Director of Technology and Partnerships at Netsafe, to author (16 March 2018).

passed.[112] The most common complaint 'involves sexual content including what is described as 'revenge pornography' being put online when a relationship between two people has broken down.[113]

### 2.3.5 The District Court's powers

In addition to the role played by Netsafe, the District Court has been given a wide range of civil and criminal powers. Section 18 (interim orders) and section 19 contain the main civil enforcement provisions. The criminal offences are created by sections 21 and 22. Both civil and criminal regimes are discussed briefly below.

#### 2.3.5.1 Civil remedies under the HDCA 2015

The following may apply to the District Court for a court order:

- An individual who alleges that they have suffered or will suffer harm as a result of a digital communication (the 'affected individual');[114]
- A parent or guardian of an affected individual;[115]
- The professional leader of a registered school if the affected individual is a student of that school **and** consents to that professional leader bringing proceedings;[116]
- The Police, if the digital communication constitutes a threat to the safety of an individual.[117]

The District Court has the power under s 11(2) of the HDCA 2015 to grant an order if it satisfied that: (a) there has been a threatened serious breach, a serious breach or a repeated breach of one or more communication principles;[118] **and** (b) the breach has caused or is likely to cause harm to an individual.[119] This is a two-step test: both elements must be satisfied. The Court must also consider whether an attempt has been made to resolve the complaint, through mediation or otherwise.[120]

The 'heart' of the District Court's role in enforcing the HDCA is contained in s 19. The list of orders that may be made by the Court is extensive. They include an order: to take down or disable material; that the defendant cease or refrain from the conduct

[112] *Ibid.*
[113] New Zealand Law Society, 'Cyber Law two years on, not without controversy' (6 April 2017) <www.lawsociety.org.nz/news-and-communications/latest-news/news/cyber-law-two-years-on,-not-without-controversy> accessed 22 March 2018, quoting Ben Thomas of Netsafe.
[114] HDCA s 11(1)(a).
[115] HDCA s 11(1)(b).
[116] HDCA s 11(1)(c).
[117] HDCA s 11(1)(d). Also, the chief coroner can bring proceedings by virtue of s 11(2).
[118] HDCA 2015, s 12(2)(a).
[119] HDCA 2015, s 12(2)(b).
[120] HDCA 2015 s 13(2). The Court can adjourn the proceeding and refer the matter back to Netsafe.

concerned; that the defendant not encourage any other persons to engage in similar communications towards them; that a correction be published; that a right of reply be given to the affected individual; and that an apology be published.[121]

In addition, the District Court can also make any of the following orders against an online content host (eg. Google, YouTube, Twitter, Facebook): take down or disable public access to material that has been posted or sent; release the identity of the author of an anonymous or pseudonymous communication to the court; publish a correction; or give a right of reply to the affected individual.[122]

In exercising its powers the court **must** take into account a number of things including:[123]

- The content of the communication and the level of harm caused or likely to be caused;
- The purpose of the communicator and whether it was intended to cause harm;
- The occasion, context and subject matter of the communication;
- The extent to which the communication has spread beyond the original parties;
- The age and vulnerability of the affected individual;
- The truth or falsity of the statement; and
- Whether the communication is in the **public interest**.

The court must act consistently with the rights and freedoms contained in the NZ Bill of Rights Act 1990.[124] The 'public interest' consideration ought to help the Courts distinguish between speech that is political and 'useful' and speech that is genuinely harmful.[125] It is hard to know how these provisions will be interpreted by the courts. No civil decisions are currently available.[126] That may be a sign of Netsafe's effectiveness at resolving complaints without the need to resort to the courts.

#### 2.3.5.2 Criminal prosecutions for harmful online speech under the HDCA 2015

The Act is important not only for the civil remedies it creates, but because for the first time, it makes it a criminal offence in New Zealand to post or send harmful digital

[121] HDCA 2015, s 19(1)(a)-(f).
[122] HDCA 2015, s 19(2)(a)-(d).
[123] HDCA 2015, s 19(5) sets out the whole list, only the items mentioned at s 19(4)(a)-(g) are listed above.
[124] HDCA 2015, s 19(6).
[125] This point refers to John Stuart Mill's arguments in favour of free speech. He argued that the main point of free speech is to help society arrive at the truth – speech that is in the 'public interest' – whereas speech that is not part of an argument aimed at the truth, purely emotive or bullying speech, is not worthy of protection.
[126] As at 31 March 2018.

communications. Two criminal offences are created by the Act. Posting a harmful digital communication is one (s 22) failing to comply with a court order is the other (s 21). Pursuant to s 22 of the Act, a person commits a criminal offence if:[127]

*(a) They post a digital communication with the intention that it causes 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.*

As mentioned above, 'harm' is defined in s 4 as 'serious emotional distress'. In determining whether a post 'would cause harm', the court may take into account any factors that it considers relevant, including:[128] the extremity of the language use, the age and characteristics of the victim, whether the digital communication was anonymous, whether the digital communication was repeated, the extent of circulation, whether the digital communication is true or false, and the context in which the digital communication appeared.

Anyone who commits this offence is liable to a term of imprisonment not exceeding two years, or a fine not exceeding $50,000 or (in the case of a body corporate) a fine not exceeding $200,000.[129] There is a second criminal offence created by the Act, that of failing, without reasonable excuse, to comply with an order of the District Court made pursuant to ss 18 or 19 of the Act. A person who fails to comply with a court order is liable to a term of imprisonment not exceeding 6 months or a fine not exceeding $5,000 (for a natural person) and a fine not exceeding $20,000 (for a body corporate).[130] The case law on s 22 is discussed below in Part 3.

#### 2.3.5.3 Safe harbour provisions

Online content hosts[131] can be held criminally and civilly liable under the Act. However, the so-called 'safe harbour' provisions protect online content hosts from civil and criminal liability if they receive a 'notice of complaint' and comply with s 24(2). Section 24(2) sets out a process: the host has to notify the author within 48 hours of receiving a notice of complaint and if the author is not able to be contacted within 48 hours then it must take down or disable the content.[132] These provisions

[127] HDCA 2015, s 22(1)(a)-(c).
[128] HDCA 2015, s 22(2).
[129] HDCA 2015, s 22(3).
[130] HDCA 2015, s 21 – Offence of non-compliance with order.
[131] An 'online content host' is defined as the person who has control over the part of the electronic retrieval system, such as a website or an online application, on which the communication is posted and accessible by the user: HDCA 2015 s 4.
[132] HDCA 2015 s 24(2)(a).

provide a quick and effective method for taking down material.[133] One of the strengths of the legislation is that a 'notice of complaint' can be issued by Netsafe.[134] That may mean that the court is rarely asked to invoke these provisions, assuming that online content hosts will normally comply with Netsafe's requests.

*2.4 Concerns about the HDCA and free speech*

Before the HDCA was passed, there was concern that although it had good intentions, it might also stifle free speech online. A similar debate arose last year in Germany when the 'NetzDG' bill was being debated.[135] The opposition to the bill was that it went too far and that 'it may well pick up in its drift-net the sorts of noise and criticism that make for the talk of a free society.'[136] Journalists were particularly worried about how it would impact them.[137] There were concerns from the media that the communication principles were 'ludicrously wide'.[138] It was alleged that the law could legally ban 'serious TV journalism' (since television and radio were included as 'electronic communications') and that it threatened to criminalise people for exposing politicians, which is beneficial for society in the aim of holding our elected officials accountable.[139] One blog in particular was severely critical of how the Act would erode freedom of expression.[140]

So far, those fears have proven to be unfounded, for a number of reasons. First, a survey of the cases that have been brought before the District Court and High Court show that *none* of them have involved journalists' freedom of expression. Secondly,

[133] This may lead to more requests to web hosts such as Google, Facebook and Youtube, as discussed above in Part 1.
[134] HDCA 2015 s 25(1).
[135] Patrick Evans, 'Will Germany's new law kill free speech online?' *BBC Trending* (18 September 2017) <www.bbc.com/news/blogs-trending-41042266> accessed 24 March 2018.
[136] David Seymour, 'Editorial: Harmful Digital Communications Bill goes too far' *Stuff* (4 July 2015) <www.stuff.co.nz/dominion-post/comment/editorials/69957563/editorial-harmful-digital-communications-bill-goes-too-far> accessed 9 March 2018.
[137] Tim Watkin, 'Sloppy law change may endanger free speech' *Stuff* (29 June 2015) <www.stuff.co.nz/national/politics/opinion/69810737/sloppy-law-change-may-endanger-free-speech> accessed 7 March 2018. Watkin alleged that Act would 'undermine journalists' ability to critique, cartoonists' ability to lampoon and satirists' ability to just take the mick'.
[138] A major daily newspaper, *The Press,* voiced its opposition to the HDC bill and one of its claims was that the 10 communication principles were ludicrously wide: see Editorial 'Digital communications statute a threat to free speech' *The Press* (30 June 2015) <www.stuff.co.nz/technology/digital-living/69786622/editorial-digital-communications-statute-a-threat-to-free-speech> accessed 9 March 2018. They particularly criticised two things: the prohibition on making a false allegation, claiming that proving this would be incredibly difficult and could result in 'endless argument' and the phrase 'serious emotional harm' was a 'disconcertingly subjective notion'.
[139] See Gareth Hughes, 'New law poorly-drafted, vague and could criminalise free speech' *Stuff* (6 July 2015) https://www.stuff.co.nz/the-press/opinion/69955436/new-law-poorlydrafted-vague-and-could-criminalise-free-speech last accessed 8 March 2018 and see Bryce Edwards, 'Political roundup: Dangers for democracy in today's cyber-bullying law' *NZ Herald* (30 June 2015) <www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11473451> accessed 8 March 2018.
[140] No Right Turn 'This law should not be passed' 26 June 2015 <http://norightturn.blogspot.co.nz/2015/06/this-law-should-not-be-passed.html> accessed 8 March 2018.

the District Court can not order material to be taken down unless one of the ten communication principles is violated. Thirdly, the Court is mandated to take the NZ Bill of Rights Act 1990 into account before making any order. Thus, it has a statutory duty to balance the harm of the digital communication against the right to freedom of expression under s14 of the NZBORA 1990. Fourthly, any complainant must first approach Netsafe and it will consider whether the communication does breach one of the communication principles and causes 'severe emotional harm'. A complainant may still seek an order from the District Court, even if Netsafe does not pursue it, but this 'triage' service helps to filter out unwarranted complaints. So far, the HDCA 2015 has not stifled freedom of expression in a way that threatens journalistic expression. Part 3 will now examine how the courts have applied the Act.

## *PART 3 – CASE ANALYSIS - HOW NEW ZEALAND COURTS APPLY THE HDCA 2015*

This part of the paper looks at the emerging case law on the HDCA 2015. To date, there have been four High Court decisions and one Court of Appeal decision: all s 22. As yet, no civil cases have been reported and no criminal case has been appealed to the Supreme Court. Although the case law is still evolving, a brief review of the decisions may help to understand how the Act is being interpreted by judges. The first High Court decision was handed down on 24 March 2017 in *Police v B*. It was followed by *Brittin v Police* on 2 October 2017, *Smith v Police* on 21 November 2017 and the latest decision, *Butler v Police,* on 1 December 2017. The only Court of Appeal case was *Waine v R* on 6 July 2017 but it is not very helpful in terms of HDCA analysis (it mainly involved sentencing principles) so it is not discussed here.[141] The High Court cases are discussed first and then the District Court decisions.

### *3.1 High Court decisions on the HDCA 2015*

#### 3.1.1 *Police v B* – the meaning of 'serious emotional distress'

The first case to reach the High Court was the case of *Police v B*.[142] It was an appeal from the District Court case of *The Queen v Partha Iyer*.[143] It was a landmark case in so far as *The Queen v Partha Iyer* was the first defended hearing on the HDCA. The

[141] *Waine v R* [2017] NZCA 287 [6 July 2017]. It was an unsuccessful appeal against sentence and conviction involving an individual who threatened to post intimate pictures of a former girlfriend.
[142] *Police v B* [2017] NZHC 526 [24 March 2017]. The full judgment is available here: https://forms.justice.govt.nz/search/Documents/pdf/jdo/c7/alfresco/service/api/node/content/workspace/SpacesStore/3a60b2f3-bdbd-411f-bf69-fb28fb143d87/3a60b2f3-bdbd-411f-bf69-fb28fb143d87.pdf accessed 9 March 2018.
[143] *The Queen v Partha Iyer* [2016] NZDC 23957 [28 November 2016]. The fact that *Police v B* is an appeal from *R v Partha Iyer* was not immediately evident, due to the fact that in the High Court judgment, Downs J noted in footnote 1 that this case was an appeal from *R v B* [2016] NZDC 23957. Research into this matter reveals that *R v Partha Iyer* was District Court case 23957. Thus, it is submitted that *Police v B* was not an appeal from *R v B*, rather, it was an appeal from *R v Partha Iyer*. Note that neither 'Partha Iyer' nor 'B' are real names. Name suppression was granted and therefore the names are anonymised by the Ministry of Justice to prevent identification of the parties and hence protect the victim.

case turned on the meaning of 'harm', defined in the Act as 'serious emotional distress'.[144] The facts may be summarised as follows. The respondent/defendant (the husband) and the complainant (the wife) were married but separated at the time of the offending. The wife had obtained a temporary protection order against her estranged husband. On 4 August 2015, the wife went out with another man. The following day, the husband sent that man a text message; he also sent a screenshot of that message to his estranged wife.[145] The message asked if the man had had fun with 'my wife' and it remarked that the man was not the complainant's type. The husband also called his estranged wife and said: 'I know where you went, where you parked your car and where you were sitting'. He admitted following his wife and her friend.[146] Later that month, the respondent and complainant met in a park. He told her that he would post photographs of her online if she did not stay away from other men.[147] He also ordered her to cancel the protection order. She felt as if she was being black-mailed; she said she felt scared and anxious.[148] On about 29 August 2015, a friend of the complainant received a Facebook 'invite' from someone. She clicked on the notification. She found 'not very nice pictures' of the complainant. She took a screenshot and sent it to the complainant. The complainant recognised the photos: she had taken them of herself after separating from the respondent. The photos posted to Facebook were of the complainant lying on a bed in her underwear. She said both photos were personal and she did not know how her estranged husband had got hold of them. She was very upset. She contacted Facebook and made a Police complaint.[149] The respondent (the husband) admitted posting the images when interviewed by Police. The husband was charged by the Police with two offences: breach of a protection order[150] and posting a harmful digital communication.[151]

The matter came before Judge Doherty in the District Court. At the end of the prosecution case, instead of opening its defence, the defence counsel applied for both charges to be dismissed on the basis that there was no case to answer.[152] If successful, there would be no need to continue with the trial and the defendant would be

[144] 'Harm' is defined in s 4 of the HDCA 2015.
[145] *Police v B,* para 4.
[146] *The Queen v Partha Iyer* [2016] NZDC 23957, para 9.
[147] *Police v B,* para 5.
[148] *Police v B,* para 5.
[149] *Police v B,* para 6.
[150] An offence under s 49(1)(b) of the Domestic Violence Act 1995.
[151] An offence under s 22 of the HDCA 2015.
[152] This application was made pursuant to s 147(4)(b) of the Criminal Procedure Act 2011 which provides that the court may dismiss a charge at any time before or during the trial if, *inter alia,* the court is satisfied that there is no case to answer: Criminal Procedure Act 2011 <www.legislation.govt.nz/act/public/2011/0081/latest/DLM3360237.html> accessed 28 March 2018.

acquitted. Judge Doherty had to decide whether there was a *prima facie* case to answer. On the first charge (breaching a protection order), he was satisfied that there was a case to answer. On the second charge (under the HDCA), he was not.

Judge Doherty held that there was evidence that the respondent had posted a digital communication with intent to cause harm, and that the communication would cause harm to an ordinary reasonable person in the victim's position (thereby satisfying s 22(1)(a) and (b)).[153] The defendant had argued that there was no proof that a Facebook post qualifies as a 'digital communication'. Judge Doherty referred to s 4 of the HDCA where a 'digital communication' is defined in broad terms as meaning 'any form of electronic communication'. The judge held:[154]

> *In order to determine the present application, I do not consider that an in-depth knowledge of how Facebook operates is necessary in and of itself…The definition [in s 4(a) of "digital communication"] is expansive, and does not purport to limit the communication to certain media or platforms…The definition of "posts a digital communication" is similarly broad…It is sufficiently broad to include the act of uploading a picture onto a Facebook account…*

In this case, the Court was satisfied that the defendant had posted a digital communication for the purpose of s 22(1). The judge accepted a screenshot of the offending image as proof of posting. He accepted that the images were posted with the intention of causing harm and that they would cause harm to an ordinary, reasonable person in the position of Mrs Iyer.[155] However, the judge held that the communication did not actually cause *this* woman harm (ie. 'serious emotional distress') thereby failing to satisfy s 22 (1)(c). The District Court judge held that 'while the evidence clearly points to some degree of emotional distress, it is not sufficient to satisfy me it has reached the threshold of serious emotional distress'.[156] Therefore, there was no case to answer on the s 22 charge. The Police appealed the 'no case to answer' decision to the High Court.

On appeal to the High Court, Downs J reviewed the legislative definition of 'harm' in the HDCA 2015. Downs J made five observations about the definition of 'harm', some of which are, respectfully, rather obvious. First, it is exhaustive and it is concerned only with serious emotional distress.[157] Second, the Act is not concerned with minor

[153] *The Queen v Partha Iyer* [2016] NZDC 23957, para 71.
[154] *The Queen v Partha Iyer* para 26.
[155] Thereby satisfying s 22(1)(a) and (b).
[156] *R v B* [2016] NZDC 23957, para 73.
[157] *Police v B,* para 21.

emotional distress.[158] Third, determination is part fact, part value-judgment and the legislature has adopted a 'somewhat elastic concept'.[159] Fourth, in determining whether 'serious emotional distress' was caused, his Honour said:[160]

> *I incline to the view that consideration should be given to the obvious factors such as the nature of the emotional distress; its intensity; duration; manifestation; and context including whether a reasonable person in the complainant's position would have suffered serious emotional distress.*

Fifth, interpretation of the phrase 'serious emotional distress' is not helped by reference to a dictionary or thesaurus or other jurisdictions' comparable laws. In summary, Downs J held that 'serious emotional distress' is 'a broad compendious expression that means what it says.'[161]

Downs J then went into some depth describing the evidence of what the photos were and how the complainant reacted to the material.[162] He placed some weight on a witness who described the complainant as being 'very shocked' and 'very depressed'. He also highlighted the evidence of the complainant herself that it would have been a 'big huge embarrassment' for family or colleagues to have seen the images on Facebook.[163] Although the District Court judge did not consider that she had actually suffered 'severe emotional distress', Downs J came to the opposite conclusion. He found that when considering the evidence in its totality and with reference to context, the evidence was capable of establishing harm as defined by the Act.[164] Thus, the Police appeal was successful—there was a *prima facie* case to answer—and the lower court's decision on s 22 was quashed. The case was remitted to the District Court for **retrial** on this point.[165]

A procedural difficulty then arose as to whether there was supposed to be a 'retrial' (a complete rehearing where the Crown would start afresh and be allowed to bring new evidence about 'harm') or a 'continuation' (continue the original hearing from the end

[158] *Police v B,* para 22.
[159] *Police v B,* para 23.
[160] *Police v B,* para 24.
[161] *Police v B,* para 25.
[162] Downs J mentions that the communication consisted of two images showing the complainant lying on a bed, possibly naked. A witness, the complaint's friend 'J', stated that the posting of the images on the fake Facebook page contained links to pornographic websites: *Police v B,* para 26-27.
[163] *Police v B,* para 29. Note that the estranged husband had posted the images on a fake Facebook account using a name similar to the complainant's Facebook name.
[164] *Police v B,* para 43.
[165] *Police v B,* para 44.

of the prosecution's case when the 'no case to answer' application was made).[166] Downs J in the High Court essentially left it to the parties to decide.[167] They consented to the latter. Thus, the continuation took place in the District Court on 10 May 2017 and the reserved decision was handed down on 24 May 2017.[168] The judge continued from the point at which he had previously made the (erroneous) decision that there was 'no case to answer'. That is, the hearing continued from the end of the prosecution's case. Naturally, the prosecution did not have the opportunity to lead new evidence on whether the victim had suffered 'harm'. On the continuation, Judge Doherty held that the charge under s 22 could not be proven because he was not satisfied beyond reasonable doubt that the victim had suffered 'harm'.

This outcome was hardly surprising. When substituting Downs J's decision that *there was* a case to answer, Judge Doherty held that, on the same evidence, the charge had not been proven beyond reasonable doubt.[169] The defendant was acquitted.

This case was touted by academics as being potentially quite important to the interpretation of 'harm' in s 22.[170] Although it is an important case—it was the first defended hearing, the first appeal and both judges grappled with the meaning of 'serious emotional distress—the clearest lesson to draw from this case is how important it is for the prosecution to lead evidence that proves a victim actually suffered 'serious emotional distress'. Two judges reached opposite conclusions on the same evidence as to whether there was *prima facie* evidence of 'serious emotional distress'. The precedential weight of the High Court decision is minimised to some extent because it was not an appeal after a full trial (where the standard of evidence is 'beyond reasonable doubt'), instead, it was an appeal from a 'no case to answer' application which has a lower standard of proof.[171] Nevertheless, the High Court and



[166] This procedural problem was raised because of the wording of Downs J in paragraph 44 of his judgment when he stated that the 'charge is to be retried' and then he went on to say that 'there is merit in the case continuing before Judge Doherty if scheduling permits that course'. These are two opposing options. He chose not to clarify which of the two he was ordering: see *Police v B,* para 44.
[167] *NZ Police v B,* Minute of Downs J, para 3.
[168] *Police v B* [2017] NZDC 9627. This decision has not been made available online but is on file with the author.
[169] *Police v B* [2017] NZDC 9627 para 32.
[170] For instance see Sally Carter 'The Harmful Digital Communications Act 2015- Two Years On' in NZLS CLE *Cyber Law – Applying Cyber to the Real World* (April 2017) at 24 and David Harvey, 'R v Iyer [2016] NZDC 23957' 17 February 2017, *Auckland District Law Society,* https://www.adls.org.nz/for-the-profession/news-and-opinion/2017/2/17/r-v-iyer-[2016]-nzdc-23957/ last accessed 20 March 2018.
[171] On a 'no case to answer' application under s 147(4)(b) of the Criminal Procedure Act 2011, the application can only succeed if the prosecution has not been able to present any credible evidence that would prove each essential element in the alleged offence: *Haw Tua Tau v Public Prosecutor* [1982] AC 136, [1981] 3 All ER 14 (PC) at 151-152, as cited by Judge Doherty in *The Queen v Partha Iyer* at para 4. By contrast, the criminal standard of proof is that the evidence proves the charge beyond reasonable doubt.

District Court decision discloses just how difficult it is going to be to strike the right balance in interpreting the term 'harm'.

### 3.1.2 *Brittin v Police* – an appeal against sentence

The second case to come before the High Court was *Brittin v Police.*[172] It was also a landmark case because it was the first appeal to the High Court against sentence for a HDCA offence. The facts of this case are as follows. In November 2015, Mr Brittin met the victim through a Facebook dating site. Mr Brittin was 20 years old and the victim was 30 years old. They communicated for about two weeks by phone and text message. The victim sent Mr Brittin several very revealing photographs of herself through Facebook messenger. The relationship soured and that is when the offence was committed. Mr Brittin posted the images that the victim had previously sent him to an R18 Facebook website. He also posted the her name, mobile phone number and a lewd message (to the effect that the victim was someone who would readily have sexual relations with anyone). All messages and photos were posted from Mr Brittin's own Facebook account. Shortly afterwards, the victim began receiving text messages from strangers that caused her to become, 'mentally and emotionally stressed'. She then changed her phone number to stop the unsolicited texts.[173] In her victim impact statement, she gave evidence that this had a serious impact on her – she had been humiliated. Her friends and family were aware of the postings. She reported that she had lost self-confidence and appetite.[174] She had nightmares, she felt 'destroyed' and she had 'lost all trust and faith in people'.[175] This was what might be called the 'paradigm case' under s 22 of the Act.[176]

Mr Brittin pleaded guilty. In the District Court Judge Mabey QC noted the maximum sentence was two years imprisonment. Since this offending was one of the most serious cases, he adopted a starting point of 18 months. He considered that 'deterrence, denunciation and accountability' should be paramount because that is consistent with the purposes of the Act.[177] He gave a three month deduction for Mr Brittin's 'previous good character' and expressions of remorse, and another 20 percent (three months) deduction for the guilty plea, arriving at a sentence of 12 months.

[172] *Britten v Police* [2017] NZHC 2410 [2 October 2017].
[173] *Britten v Police,* para 4.
[174] *Britten v Police,* para 5.
[175] *Britten v Police,* para 5.
[176] This comment was made by Downs J in *Butler v Police* [2017] NZHC 2972 at para 4.
[177] *Britten v Police,* para 5.

Judge Mabey QC declined an application for home detention[178] so as not to give the 'wrong message'.[179] Mr Brittin appealed the sentence as being 'manifestly unfair'. He also appealed the denial of home detention. In the High Court Woodhouse J reviewed s 22 of the Act.[180] He noted that there were too few cases to enable a reasonably reliable assessment of relative gravity.[181] Woodhouse J held that there were some errors in sentencing principles applied and a failure to take account of Mr Brittin's age and the impulsive nature of this actions. As a result, Woodhouse J felt that this case was at the 'midpoint' of offending of this nature so the starting point ought to have been 12 months, not 18 months, imprisonment. With discounts, the term of 7 months prison was appropriate. On the home detention point, Woodhouse J found that Judge Mabey QC was wrong in principle. There is no need to go into the reasoning here since they pertain to the Sentencing Act 2002 and lie beyond the remit of this paper. In summary, Woodhouse J held that he would have imposed a sentence of six months home detention.[182] The sentence of 12 months was quashed and a sentence of seven months was imposed with leave to apply for home detention.[183]

### 3.1.3 Case 3: *Smith v Police* – an appeal against conviction and sentence

The third case to reach the High Court was the case of *Smith v Police,* decided by Edwards J.[184] It was also an appeal against conviction and sentence. Over an 8-month period, Mr Smith posted sexually explicit images about A, R and R's sister to several Instagram accounts that he set up under a false identity.[185] The offending began the day after his 17th birthday. A, R and R's sister were between 14 and 17 years of age at the time.[186] Mr Smith knew A and R because he had attended intermediate school with them. They went on to attend different high schools, but they stayed in touch via social media. Mr Smith pleaded guilty to two charges of posting digital communications with intent to cause harm (pursuant to s 22 of the HDCA 2015). In the District Court he

[178] 'Home detention' is a sentence wherein the offender is required to remain at an approved address under electronic monitoring with limitations as to when they can be away from the residence. They are also under the supervision of a probation officer. It is available if the court would otherwise impose a short-term sentence of imprisonment (Sentencing Act 2002, s 15A).
[179] *Britten v Police,* para 15 citing para 27 of the District Court judge's decision.
[180] *Britten v Police,* para 19ff. Note that s 22 of the HDCA 2015 requires that (a) the person posts a harmful digital communication with the intention to cause harm to the victim; and (b) that the posting would cause harm to an ordinary reasonable person in the position of the victim; and (c) posting the communication causes harm to the victim.
[181] *Britten v Police,* para 26.
[182] *Britten v Police,* para 59.
[183] *Britten v Police,* paras 62-64.
[184] *Smith v Police* [2017] NZHC 2856 [21 November 2017]. This decision is available here: https://forms.justice.govt.nz/search/Documents/pdf/jdo/4e/alfresco/service/api/node/content/workspace/SpacesStore/0bc230c1-ac48-47a3-b43f-24f5cbd9e21d/0bc230c1-ac48-47a3-b43f-24f5cbd9e21d.pdf last accessed 10 March 2018.
[185] *Smith v Police,* para 1.
[186] *Smith v Police,* para 1.

sought a 'discharge without conviction'.[187] His application was declined and he was sentenced to 12 months supervision and three months community detention for both HDCA charges.[188] He appealed the decision not to grant him a discharge without conviction.[189] That aspect of the High Court case is not strictly relevant here as it mainly relates to sentencing principles. However, the case is relevant to the extent that it forms part of the emerging case law on s 22 of the HDCA 2015 and it provides an example of the type of conduct that can be successfully prosecuted. One of the notable aspects of the facts in this case is that some of the images used by the offender were photos that had originally been taken by the victims and posted on their own Instagram accounts. Smith used the images, altered some, and posted his own sexually explicit wording in comments on the photos. He eventually removed these.[190] Some months later, Smith set up another Instagram account under another false identity. He posted three images of cartoon figures in sexually explicit poses (commonly referred to as 'hentai'), that mentioned the victims by name.[191] He commented on each of the pictures. These latter images sparked the complaint to the Police. In the victims' impact statements, they described their anxiety, stress and difficulties in trusting people as a result of the offending. They said the Instagram posts made them feel 'disgusted, guilty…and unclean.'[192] The defendant pleaded guilty so there was no need to analyse the HDCA. In considering the appeal, Her Honour held that 'the consequences of being branded with a conviction must be measured against the sexually explicit material Mr Smith posted over an eight-month period. Those posts caused considerable anxiety to the young females he specifically targeted.'[193] Edwards J dismissed the appeal.

### 3.1.4 Case 4: *Butler v Police* – appeal of sentence

The fourth and most recent (at the time of writing) case to come before the High Court was *Butler v Police*, on 1 December 2017.[194] This was another decision of Downs J.[195] Mr Butler pleaded guilty in the District Court to a charge under s 22 of the HDCA and

[187] *Police v Smith* [2017] NZDC 13864 (discharge without conviction).
[188] *Police v Smith* [2017] NZDC 14864 (sentence).
[189] A 'discharge without conviction' is a sentencing option open to a judge in New Zealand when a person is found guilty or pleads guilty. A discharge without conviction is deemed to be an acquittal. It is only available if the direct and indirect consequences of conviction would be out of all proportion to the seriousness of the offence. It is not an option if the offence has a minimum sentence (Sentencing Act 2002, s 106). However, it was an option here because s 22 HDCA 2015 does not have a minimum sentence.
[190] *Smith v Police* [2017] NZHC 2856 [21 November 2017], paras 7-11.
[191] *Smith v Police,* para 10.
[192] *Smith v Police,* para 11.
[193] *Smith v Police,* para 61.
[194] *Butler v Police* [2017] NZHC 2972 [1 December 2017]. Hearing and oral judgment on 1 December 2017.
[195] Downs J decided the first appeal under the HDCA 2015, *Police v B,* discussed above at 3.1.1.

was sentenced to four months imprisonment. He appealed, arguing this was manifestly excessive. The facts of this case are slightly different from the run-of-the-mill HDCA offence. In 2002, the defendant, Mr Butler, was convicted of indecent assault in relation to the victim when she was nine years old. He received 18 months in prison for that offence. On 25 February 2017, he posted a message to the victim's Facebook account, which said: "You are ugly and a bloody lier (sic). And, 'don't hug her she will have you arrested, it can't be about sex'.[196] This was a private message so no one other than the victim could read it. The victim felt traumatised by the message, which she regarded as both 'intrusive and shocking'.[197] Although this case is very different from *Brittin,* the four month prison sentence was upheld because of several factors. First, Mr Butler had previously sexually assaulted the victim. Second, the digital communication re-victimised her many years after the event. Third, Mr Butler had previously served a sentence of home detention but home detention had a limited effect as a deterrent on him. The lawyer for Mr Butler pointed out something interesting: had Mr Butler made the very same observation to the victim in the street, he would have committed no offence. Downs J accepted that.[198] However, he reminded the defendant that the capacity for harm from digital technology has been recognised in the Act and indeed this case had unusual aggravating features.[199] The appeal was dismissed.

*3.2. District Court decisions on the HDCA 2015*

At the time of writing,[200] a total of 22 District Court decisions have been published online in connection with HDCA prosecutions. By law, all HDCA proceedings must be published.[201] That figure seems to represent 20 prosecutions because some cases came before the courts more than once.[202] Six observations are offered here on a thematic basis rather than attempting a case-by-case analysis.

1. Almost every prosecution in the District Court involved a male defendant: only one prosecution involved a female defendant.[203]

[196] *Butler v Police,* para 2.
[197] *Butler v Police,* para 2-3.
[198] *Butler v Police,* para 8.
[199] *Butler v Police,* para 8-9.
[200] 30 March 2018.
[201] HDCA 2015, s 16(4) provides that 'The decision, including the reasons, must be published.'
[202] For example, *Police v Valli* and *Police v Moore* came before the court for trial and again for sentencing.
[203] The only case the author found in any New Zealand court involving a female offender is *NZ Police v Potiki* [2017] NZDC 15878 [12 December 2017]. Potiki is not the real name of the defendant. The defendant was found to have posted abusive content on the web using Facebook Messenger. She was also in breach of a protection order that her former partner had obtained. The victim was her former partner, a man.

2. Every case (except two) involved a female victim(s).[204] It is clear that in New Zealand harmful digital communications offences are almost exclusively committed by men against women. This observation is consistent with trends in other countries, such as the US.[205]

3. Almost every prosecution resulted in a guilty plea or a guilty verdict. This may indicate that the Police generally do not pursue prosecutions unless they are confident of succeeding.

4. Prosecutions under the HDCA are often combined with other offences such as breach of a protection order, intentional damage, drug possession, intimidation, resisting police, threatening behavior, and excess breath alcohol charges. However, the HDCA is usually the most serious of the offences, and as such, it usually attracts the largest portion of the sentence.[206]

5. The court frequently emphasizes that whether the original photos or videos were originally taken/made voluntarily is irrelevant. The definition of an 'intimate visual recording' in the HDCA clearly states that an offence can be committed whether the photography, videotape or digital image was made **with or without the knowledge or consent of the subject of the recording.**[207] For example, in one of the early prosecutions, *Police v Tamihana*, Mr Tamihana, was charged under s 22 of the HDCA because he had sent a Facebook request to the mother of his former girlfriend (the mother was the victim).[208] The link contained a video attachment with the comment '[w]hat your daughter's really up to'.[209] The court pointed out that 'whether your partner was a willing party to that or not, is totally irrelevant…'[210] The maximum

[204] *NZ Police v Bust* [2016] NZDC 4391 [14 March 2016]. This is the only one of two District Court cases that involves a male victim. In *NZ Police v Bust* the defendant sent threatening text messages to the complainant (a man) and his father regarding a drug debt. In *NZ Police v Potiki,* the victim was a man, the former partner of the defendant (a woman).
[205] Danielle Keats Citron 'Civil Rights in Our Information Age' in Levmore and Nussbaum (eds) *The Offensive Internet, supra* n 13 at 32, where Citron notes that 'Working to Halt Online Abuse' found that from 2000 to 2007, 72.5 percent of individuals reporting cyber harassment identified themselves as women and 22 percent identified themselves as men.
[206] For example, see *Police v Valli* [2017] NZDC 17182 [4 August 2017], para 3. Mr Valli was charged with a raft of offences including excess breath alcohol, careless driving, resisting police, intimidation and threatening behavior, but the judge noted that 'the most serious charge you face is that of causing harm by posting a digital communication.'
[207] HDCA 2015, s 4, definition of an 'intimate visual recording'. Contrast this definition with the definition of 'intimate visual recording' in the Crimes Act 1961, s 216G, which has a higher penalty (up to 3 years in prison, s 216H) for a recording made without the knowledge or consent of the person who is the subject of the recording.
[208] *NZ Police v Tamihana* [2016] NZDC 6749 [18 April 2016].
[209] The video was opened and played by the mother. The video was of a sexual nature depicting a scene filmed voluntarily between the victim's daughter and another consenting party. The mother reported feelings of despair and was aware that it was 'payback' for her not approving of the relationship between the defendant and her daughter: *NZ Police v Tamihana* paras 9-11.
[210] *NZ Police v Tamihana,* para 11.

sentence was two years, the judge took nine months imprisonment as the starting point and gave discounts for the early guilty pleas and added three months for previous convictions for violent offending. In total, he was sentenced to eleven months in prison and he was not entitled to a substitution of home detention.[211] This was also a feature of *Police v Valli,* wherein the victim had sent the defendant photos of herself 'in various stages of undress' during their relationship. After the relationship broke down, Mr Valli posted the images on various Facebook sites and tagged his former girlfriend's name so that the images would show up in the Facebook pages of the victim's friends (she had 1000 Facebook 'friends'). The images were removed by Facebook after complaints from the victim and her family and friends.[212] It is important that people are aware of this fact: the crime is committed regardless of whether the original photos were taken with consent.

6. The s 22 HDCA offences often happen in the context of a relationship breakdown whereby the man is seeking revenge or retaliation against the woman. For example in *The Queen v Partha Iyer*, the defendant posted semi-nude pictures of his wife, from whom he was separated, on a Facebook page that he created.[213]

7. Interpreting the meaning of 'serious emotional distress' has proven to be one of the more challenging tasks for the courts. In *The Queen v Partha Iyer* (appealed and then continued as *R v B*) the judge noted that he could not find the exact phrase in any other legislation (in New Zealand or overseas). He concluded that the harm must be 'more than trivial' and 'being merely upset or annoyed as a consequence of a digital communication would not be sufficient to invoke the sanction of criminal law.'[214] The evidence in this case was that the victim felt anger, frustration, anxiety and some degree of emotional distress. She was 'almost crying' when she saw the images online. Although the distress lasted 'a long time', on balance he did not feel that the emotional harm rose to the level of 'serious emotional distress'.[215] Judge Doherty observed that the definition of harm is designed to balance two competing concerns: the serious effects of calculated emotional harm, and the importance of maintaining free speech.'[216] This balancing exercise will continue to pose problems for judges until a

[211] The judge said that, 'to not imprison you would send totally the wrong message to you and others who might embark on this sort of behavior': *ibid*, para 21.
[212] *Police v Valli,* para 4.
[213] *The Queen v Partha Iyer* [NZDC] 23957 [28 November 2016].
[214] *The Queen v Partha Iyer,* para 54.
[215] *R v B* [2017] NZDC 9627 paras 28-32 (this was the continuation of the District Court trial).
[216] *The Queen v Partha Iyer,* para 56.

more expansive body of case law is developed around the term which will help to both define the term and provide parameters as to what harm is serious and what falls short.

### *PART 4 – COMPARATIVE ANALYSIS*

To date, no jurisdiction has employed the exact legislative solution that NZ has adopted. Moreover, no other legislation has used the term 'serious emotional distress' to define 'harm' caused by digital communications. The role played by 'Netsafe' in New Zealand is possibly unique, when one takes into account the nature of the HDCA, how Netsafe evolved and the role it plays in both receiving complaints and educating users on safe Internet practices. According to Netsafe, there are 'very few organisations' like it in the world.[217] However, some jurisdictions have legislation that is broadly comparable; a selection are mentioned briefly.

### The United Kingdom

Broadly equivalent laws in the UK are found in the Criminal Justice and Courts Act 2015 (ss 32-35) and the Malicious Communications Act 1988 (s 1). There is no specific, comprehensive statute as there is in New Zealand. The Malicious Communications Act 1988 is a very short piece of legislation which makes it an offence to send a letter, electronic communication, or article of any description, with the intent to cause distress or anxiety.[218] In contrast with the HDCA, neither 'distress' nor 'anxiety' are defined. 'Electronic communication' is defined to include any communication, however sent, that is in electronic form.[219] The electronic communication must either (a) convey a message which is indecent or grossly offensive; or (b) convey a threat; or (c) convey information which is false and known or believed to be false by the sender.[220] Some of the prosecutions under the HDCA[221] would not satisfy (b) or (c) so they would have to satisfy (a). They may well succeed but it would presumably become a matter of interpretation to the individual judge as to whether a photo/text/email is 'indecent' or 'grossly offensive'. The offence in the UK also has a statutory defence to communications that convey a threat: there is no offence if the threat was used to reinforce a reasonable demand.[222] That defence is not

[217] Email from Sean Lyons, Director of Technology and Partnerships at Netsafe, to author (16 March 2018).
[218] Malicious Communications Act 1988 (UK), s 1(1)(a).
[219] Malicious Communications Act 1988 (UK), s (1)(2A)(b).
[220] Malicious Communications Act 1988 (UK), s 1(1)(a)(i) and s 1(1)(b) both use the phrase 'indecent or grossly offensive' to describe prohibited letters and electronic communications.
[221] For example, *Police v Moore* [2017] NZDC 14864 and 13686 (the hentai and rape fantasy case) and in *Police v Tim Forrester* [2017] NZDC 16010 (posting full nude photos of victim on work-based Facebook page and a corporation Facebook page) the intention was to humiliate and embarrass the victim but there was no threat so these types of cases would have to be brought under s
[222] Malicious Communications Act 1988 (UK), s 1(2).

provided for in the New Zealand legislation, thus the New Zealand legislation is rather stricter—and it is submitted better for victims—than its UK equivalent. The penalty for the offence in s 1 of the Malicious Communications Act 1988 is a maximum of two years imprisonment, or a fine or both (if the charge is laid by indictment), or a maximum term of 12 months in prison, or a fine or both (if the charge is laid summarily).[223] This is slightly different from NZ in so far as there is no maximum fine in the UK, and there are different maximum prison sentences depending on how the charge is laid. To round out the discussion of the UK legislation, it is worth noting that it is an offence to disclose private sexual photographs and films with intent to cause distress.[224] There are three statutory defences provided, one of which mentions journalistic material.[225] The UK offence does not define a 'private sexual photograph or film', but the term might have a narrower scope than the NZ equivalent, 'intimate visual recording'. The UK provision only seems to include material that is sexual in nature. Also, the UK legislation does not allow the court to presume intent merely from the fact that distress was 'a natural and probable consequence of disclosure.'[226] In New Zealand, the legislation asks whether an ordinary, reasonable person in the position of the victim would be harmed, and also, whether this particular victim was harmed.[227] A discussion of the case law on these provisions is beyond the scope of this work but would no doubt be helpful in understanding how effective the UK law has been and this may form the basis of future research.

**Canada**

Canada passed a new statute to combat cyberbullying in 2014. The 'Protecting Canadians from Online Crime Act 2014' amended the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act.[228] It is not a standalone, comprehensive solution to harmful digital communications like New Zealand's HDCA 2015, but it created a number of provisions which amended other statutes. The key amendment for present purposes was the creation of an offence in s 162.1 of the Criminal Code. Everyone who knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person knowing that the person depicted in the image did not give

[223] Malicious Communications Act 1988 (UK), s 1(4).
[224] Criminal Justice and Courts Act 2015 (UK), s 33 <www.legislation.gov.uk/ukpga/2015/2/section/33/enacted> accessed 24 March 2018.
[225] Criminal Justice and Courts Act 2015 (UK), s 33(3), (4) and (5) set out the defences.
[226] Criminal Justice and Courts Act 2015 (UK), s 33(8): 'A person charged with an offence under this section is not to be taken to have disclosed a photograph or a film with the intention of causing distress merely because that was a natural and probably consequence of the disclosure'.
[227] Criminal Justice and Courts Act 2015 (UK), s 33(8) *cf* HDCA 2015 s 22 (1).
[228] Protecting Canadians from Online Crime Act 2014 (Canada), assented to on 9 December 2014.

their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct, is guilty of an offence. The penalty is higher than in the UK and NZ: a maximum of five years in prison.[229] There is no fine provided for in the legislation.

**USA**

The closest US law to New Zealand's HDCA is Michigan's Penal Code, which was considered by the New Zealand drafters. Section 750.411i criminalises stalking and harassment, which includes making 'unconsented contact' via, *inter alia,* sending mail or electronic communications to that individual.[230] Section 750.411i(d) is quite similar to s 22 of the HDCA because the Michigan law requires that the contact would cause a reasonable individual to suffer emotional distress, and that actually causes the victim to suffer emotional distress.[231] A comprehensive account of the bullying laws across the US is provided by the Cyberbullying Research Center.[232]

**Kuwait**

Kuwait has enacted a cybercrime law: Law No 63 of 2015 (the 'Cybercrime Law'). Kuwait's Cybercrime Law does not criminalise cyberbullying or online harassment. The article in it that is closest to New Zealand's s 22, is Article 3(4), which states that anyone who uses the Internet to 'threaten or blackmail a natural or legal person' commits an offence and is liable to a sentence not exceeding three years or a fine of between 3,000 and 10,000 dinar, or both.[233] The punishment increases if the blackmail is to get the person to commit an indecent or shameful act. This is a narrowly framed offence. It might cover some examples of cyberbullying, but the law is probably not broad enough to criminalise the sending or posting of communications that cause serious emotional harm, as the New Zealand offence does. Many of the New Zealand prosecutions involved the posting/sending of harmful communications that did not involve blackmail, but they did cause severe emotional distress. Article 4(5) of the Kuwaiti Cybercrime Law would also fail to catch the kind of offending that the New Zealand law has caught because it criminalises the instigation or deduction of a male or female to commit acts of prostitution or debauchery – acts that would presumably

[229] Protecting Canadians from Online Crime Act 2014, s 162.1(1), if the charge is laid indictably.
[230] *See* the meaning of 'unconsented contact' in the Michigan Penal Code Act 328 of 1931, s § 750.411i(1)(f)(v) Contacting that individual by telephone. (vi) Sending mail or electronic communications to that individual.
[231] The Michigan Penal Code Act 328 of 1931, s § 750.411i, <http://www.legislature.mi.gov/(S(iy0be1tfnoeyuahs1bubuceh))/mileg.aspx?page=GetObject&objectname=mcl-750-411i> accessed 21 March 2018.
[232] Cyberbullying Research Centre, 'Bullying Laws Across America' <https://cyberbullying.org/bullying-laws> accessed 24 March 2018.
[233] Law No 63 of the year 2015 (Kuwait's Cybercrime Law).

have to occur after and as a result of the posting.[234] This would not criminalise the man who has on his phone photos or videos (obtained consensually) of his former wife/girlfriend and decides to post them on an app such as Facebook or Instgram as an act of revenge.

Like the other GCC states, Kuwait's law against cybercrime focuses on criminalizing actions such as illegally accessing computing systems and cyber fraud, but it also creates some new criminal offences that are not in line with international norms. For example, Article 4(4) criminalises the act of creating a website or publishing, sending or saving information or data which 'would compromise public morality'. The term 'public morality' is not defined in the law. Depending on its interpretation, it could result in the imprisonment of people who express political opinions. Notably, there is no public interest defence, as there is in the UK and Canadian legislation.

Of greatest concern is Article 6 of the Cybercrime Law because it appears to stifle free speech. Article 6 punishes anyone who uses the internet to commit crimes that are set out in Law No 8 of 2016 (the 'Press and Publications Law').[235] The Press and Publications Law states that all web-based publications, including electronic news, must obtain a license from the government before they can operate.[236] Furthermore, Article 27 of the Press and Publications Law stated that the chief editor and article writer or author will be punished if they publish anything that is prohibited by Article 21 of the Printing and Publishing Law 2006. That article, Article 21, prohibits the publication of a long list of things, including anything that would:[237]

> *1. Disdain or contempt the Constitution of the State.*
> *2. Disdain or insult jurists or members of the public prosecution or to state something that is considered as a disparagement to the integrity and impartiality of the judicial system…*
> *3. Insulting the public morals or instigating to violate the public order…*

[234] Article 4(5): 'Anyone who instigates or seduces a male or female to commit acts of prostitution and debauchery, or helps to do so by using the internet or one of the means of information technology [is punishable by imprisonment of a term not exceeding three years and a fine of not less than three thousand dinar and not exceeding ten thousand dinars or either of them].' Translation provided by Salma Alessa, 'Cyberbullying between Kuwait and New Zealand' unpublished LLM paper, 2016.
[235] Article 6 of the Cybercrime Law: 'Shall be punished according to penalties mentioned in sections (1,2,3) of article (27) from the press and publication law, anyone who uses the internet or any other means of information technology that was set forth herein to commit crimes mentioned in articles (19,20,21) of the same law referred to above' (sic). Translation provided by Salma Alessa, *ibid.*
[236] Article 6 of Law No 8 of 2016, as translated in *The Kuwait Times* (14 February 2016) <http://news.kuwaittimes.net/website/law-no-8-of-2016-regarding-the-regulation-of-electronic-media/> accessed 22 March 2018.
[237] Article 20 of Law No 3 of 2006 on Printing and Publishing, as translated in *The Kuwait Times* (14 February 2016) <http://news.kuwaittimes.net/website/law-no-8-of-2016-regarding-the-regulation-of-electronic-media/> accessed 22 March 2018. This is reproduced from the source and the errors in the quote above are reproduced from the source.

*4. News regarding official secret communications and publishing of agreements and treaties which the government of Kuwait concludes, before publishing them in the official gazette…*
*5. Influencing the value or the national currency or what would lead to worries about the economic status of the country or publishing news about the bankruptcy of businessmen or the commercial companies or banks or the money exchangers, except by special permission of from the competent court.*
*6. Revealing what goes on in any meeting…*
*7. Infringement on the dignity of any persons or their lives or religious believes, and instigating hatred or disdain of any of the society's strata or to publish information about their financial statuses or to reveal a secret that would harm their reputation or wealth or their trade names.*
*Encroachment into the private life of an employee or person who is charged in a public service…*
*9. Causing harm to the relationships between Kuwait and other Arab or friendly countries*
*10. If the specialized newspaper went beyond the purpose of the license which is granted to it.*
(sic erat scriptum)

All of these prohibitions (except paragraph 7) are aimed at protecting the State and/or business people – they are not aimed at protecting ordinary people from emotional distress caused by digital communications. Kuwait does not appear to criminalise communications that cause serious emotional distress as is the case in New Zealand, the UK, Canada and the US State of Michigan, to name a few jurisdictions that have legislated against communications which cause emotional harm.[238] Moreover, there are no take-down procedures in the Kuwait Cybercrimes Law, a solution which most victims are concerned to access above all else.

The above list of prohibitions in Article 21 is alarming. Article 20 of the same law provides further limitations. It is apparent that these provisions violate the right to free speech in Kuwait and might not be demonstrably justified limitations in a free and democratic country.[239] By way of the Cybercrime Law, all of the above listed items are also prohibited from electronic publication. These laws are out of step with comparable laws in other countries, some of which have been discussed in this paper. That may be why the Cybercrime Law and the Press and Publications Law have been

[238] Other US states that have made it an offence to send electronic communications without legitimate purposes which cause a reasonable person to suffer substantial emotional distress include: Rhode Island General Laws § 11-52-4.2; Missouri Revised Statutes, Title XXXVIII, §565.090; 2011 Minnesota Statutes, §947.0125; Delaware Code, Title 11, chapter 5, §1311; 2011 Florida Statutes, Title XLVI, chapter 748, §748.048; Massachusetts General Laws, Part IV, Title I, chapter 265, §43A: see p83 n 159 of NZLC Ministerial Briefing Paper 'Harmful Digital Communications: The adequacy of the current sanctions and remedies' (August 2012) <www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20MB3.pdf> accessed 22 March 2018.
[239] Article 20 of Law no 3 of 2006 (the Printing and Publishing Law) prohibits criticism of the Emir. That prohibition also applies to digital media as per the 2015 law. This type of prohibition is not found in any of the other jurisdictions analysed in this paper. It is significant that when Germany was debating the new 'NetzDG' law in 2017, there was in the original draft a provision that would have barred ' defamation of the President of the Federation' but after criticism, this clause was removed: Patrick Evans 'Will Germany's new law kill free speech online?' *supra* n 135. Free speech is never unlimited, but there have to be limitations on the limitations that are invariably placed upon it.

criticized by human rights organisations.[240] An analysis of that criticism is beyond the scope of this paper. Suffice to say that Kuwait's—and all of the GCC's—cybercrime laws have been analysed by other researchers, and found to be generally deficient.[241] In summary, the GCC states tend to criminalise acts that other countries do not, they tend to limit free speech, they lack provisions on procedural powers and international cooperation and they do not create criminal offences for cyberbullying. All of these are central to the question of whether legislation is fit for purpose.[242]

**International and regional conventions**

At the time of writing, there is no comprehensive international convention that governs cybercrime—or even the subset of cyberbullying/online harassment—across all jurisdictions. There is a Council of Europe convention, the so-called 'Budapest Convention on Cybercrime', which has been signed by 56 nations.[243] The UN says that this is the most used multilateral instrument for the development of domestic cybercrime legislation.[244] Although it recommends national regulation in some aspects of cybercrime (eg. child pornography, computer-related fraud, computer-related forgery, copyright infringement) it does not mention cyberbullying or online harassment. In fact, there is no definition of cyberbullying at the European level, and only Spain has criminalised it.[245]

The Arab League has sponsored two documents that pertain to cybercrime. The Arab Convention on Combating Information Technology Offences (2010) and the Model Law on Combatting Information Technology Offences (2004). Neither directly suggests criminalizing cyberbullying or online harassment. These documents focus on State security and potential economic (rather than personal emotional) harm. The closest that either of them comes to the current issue is in the over-simplistic Articles 13 and 14 of the 2010 Convention which mention 'Gambling and sexual exploitation'



[240] For example *see* Human Rights Watch, 'Kuwait: Cybercrime Law a Blow to Free Speech' (22 July 2015) <www.hrw.org/news/2015/07/22/kuwait-cybercrime-law-blow-free-speech> accessed 22 March 2018.
[241] Joyce Hakmeh 'Cybercrime and the Digital Economy in the GCC Countries' *Chatham House* (June 2017) <www.chathamhouse.org/sites/files/chathamhouse/publications/research/2017-06-30-cybercrime-digital-economy-gcc-hakmeh.pdf> accessed 22 March 2018,
[242] Hakmeh 'Cybercrime and the Digital Economy in the GCC Countries', *ibid,* esp at 9.
[243] Council of Europe, Convention on Cybercrime, Budapest 23.XI.2001, European Treaty Series No 1850 <www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561> accessed 21 March 2018.
[244] See United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime,* February 2013, p xix <www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> accessed 21 March 2018 [hereinafter UNODC, *Comprehensive Study on Cybercrime*].
[245] Sam Morgan (trans.) 'Cyberbullying: A creeping phenomenon, only punished by law in Spain' *Euractiv* (10 November 2016) <www.euractiv.com/section/social-europe-jobs/news/cyberbullying-a-creeping-phenomenon-only-punished-by-law-in-spain/> accessed 21 March 2018.

(Article 13) and 'Offence against privacy by means of information technology' (Article 14) (sic). These articles are too vague to be meaningful.[246] Suffice to say, the Arab League has not turned its attention to the personal emotional harm caused by digital communications. As a result, many of the domestic cybercrime laws in the Gulf states do not include provisions that would specifically combat cyberbullying.[247]

It is fair to surmise that at the international level, personal harm caused by harmful digital communications is still very poorly regulated.[248] It is difficult to imagine how international consensus could emerge to facilitate a comprehensive UN convention that encompasses cyberbullying/online harassment. National laws and interpretations of the freedom of expression are currently too divergent to be able to reach an international consensus, but this is an area worthy of further research.[249] Some fundamental rules may be able to be agreed upon and may form the basis of a convention which at least combats online harassment. The UN has recommended the development of a comprehensive multilateral instrument on cybercrime, so it may just be a matter of time before this matter progresses.[250]

## *PART 5 – TRENDS AND RECOMMENDATIONS*

This final part of the paper contains some broad observations of current trends followed by a set of recommendations for governments, policy-makers and law schools to consider.

### *5.1 Teaching ICT law in universities*

An important trend to note in the area of combatting harmful digital communications is the importance of 'law and technology' papers in law schools and the increase in ICT centres. A few words on these two trends is offered here.



---

[246] Arab Convention on Combatting Information Technology Offences, full-text available here <http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences> accessed 21 March 2018.

[247] For example, the UAE has passed Federal Law No 5 of 2012 (the 'Cyber Crimes Law') which tackles internet fraud and forgery, unlawful access and disclosure of information, etc: Federal Decree-Law no 5 of 2012, Issued on 25 Ramadan 1433 AH, 13 August 2012 AD, On Combatting Cybercrimes, <http://ejustice.gov.ae/downloads/latest_laws/cybercrimes_5_2012_en.pdf> accessed 27 March 2018. The most relevant provision is Article 21, which creates an offence of photographing others or creating, transferring, disclosing, copying or saving electronic photos for the purpose of defamation or of offending another person or for attacking or invading his privacy. This is punishable by up to 6 months in prison and a fine of up to 500,000 dirhams, or both.

[248] UNODC, *Comprehensive Study on Cybercrime*, *supra* n 244, xii.

[249] See discussion in Chris Reed, *Internet Law – Text and Materials* (2nd ed. Cambridge University Press, 2004) ch 7 esp p268. There is an argument that a consensus can be built on the basis of the international law principle of *jus cogens*: see for example Victor Mayer-Schonberger and Teree E Foster 'Regulatory Web: Free Speech and the Global Information Infrastructure' (1997) 3(1) *Michigan Telecommunications and Technology Law Review* <https://repository.law.umich.edu/mttlr/vol3/iss1/3/> accessed 21 March 2018.

[250] UNODC, *Comprehensive Study on Cybercrime*, *supra* n 244, pxx.

### 5.1.1 ICT courses/papers

In New Zealand, three of the six law schools offer at least one course in the area of 'law and technology'.[251] Some of the courses currently being offered in New Zealand universities at undergraduate and postgraduate level include:

- Law and Information Technology – LAWCOMM426 (University of Auckland);[252]
- Media Law in the Digital World – LAWGENRL711 (University of Auckland);[253]
- Cyber Law - LEGAL 435 (University of Waikato); [254]
- Law and New Technologies - LEGAL 492 (University of Waikato);
- Information and Data Protection Law – LAWS423 (University of Otago);
- Law and Emerging Technologies - LAWS 428 (University of Otago);
- Media Law: Privacy and the Media – LAWS 456 (University of Otago).
- Legal Aspects of Cyber Security - LEGAL 526 (University of Waikato, LLM);
- Law and Information Technology – LEGAL 574 (University of Waikato LLM);

### 5.1.2 ICT Centres

Under the leadership of recently retired Judge David Harvey, Auckland University has established the 'New Zealand Centre for ICT Law'. It is a specialist centre 'which investigates, studies and considers the implications of ICT within the context of law, technological developments and its impact upon society'.[255] It also:[256]

a) *Serves as a focus for promoting and undertaking research into the interface between law and new communications technologies.*
b) *Studies the implications of new communications technologies upon law and the policy that informs legal outcomes.*

Otago University has established the New Zealand Law Foundation Centre for Emerging Technologies. It has secured a $400,000 grant from the NZ Law Foundation to undertake a 2-year project on 'Artificial Intelligence and Law in New Zealand'.[257] Law and technology is a key area of interdisciplinary research and development in New Zealand. This trend is in line with overseas developments. At University College

[251] The author read the LLB and LLM (where applicable) paper offerings for all six law schools and could not locate a directly relevant course at the University of Canterbury, Victoria University or Auckland University of Technology (AUT). However, those universities did offer courses in media law and/or privacy that might touch on harmful digital communications.
[252] Auckland Law School, LAWCOMM426 – Law and Information Technology, 'Course description' <www.law.auckland.ac.nz/en/for/current-students/current-undergraduate-students/cs-course-planning/cs-course-descriptions/elective/LAWCOMM426.html> accessed 20 March 2018.
[253] This will be taught in April 2018 for the first time. The course will cover, *inter alia,* the HDCA 2015. The course outline is available here: <www.law.auckland.ac.nz/en/for/future-postgraduates/fp-study-options/fp-courses/timetable/LAWGENRL711.html> accessed 20 March 2018.
[254] University of Waikato, LLB degree.
[255] New Zealand Centre for ICT Law, 'About the Centre'<www.law.auckland.ac.nz/en/about/centres-and-associations/new-zealand-centre-for-ict-law.html> accessed 20 March 2018.
[256] *Ibid.*
[257] New Zealand Law Foundation, News Item (January 2017) <www.lawfoundation.org.nz/?p=7680> accessed 21 March 2018.

London (UCL) is the Dawes Centre for Future Crime.[258] It was established in 2016 with a £3.7 million grant from the Dawes Trust. The Dawes Centre for Future Crime will 'identify emerging crime threats, and work with front-line law enforcement, policy makers and industry to deliver pre-emptive interventions for the benefit of society.'[259] UCL also has the SECReT, a £17 million international centre for PhD training in security and crime science.[260] The Gulf states have made some inroads in this area. For instance, NYU-Abu Dhabi has established the 'Center for Cyber Security'.[261]

*5.1.3 Online 'watchdogs' and complaint/education services*

New Zealand has the organisation 'Netsafe' (discussed above). Netsafe is the first 'port of call' for someone who experiences online harm. Netsafe is unusual because of the breadth of its role, including its statutory role pursuant to the HDCA 2015. However, there are roughly comparable institutions that promote online safety in several countries. One of the other best examples comes from Australia: it has the Office of the eSafety Commissioner, which is responsible for promoting online safety for all Australians. The eSafety Commissioner receives complaints and reports about cyber-bullying, conducts research into attitudes and experiences, helps complainants to get material removed (it requests social media services to remove content within 48 hours) and it also provides a wide range of educational and informational resources to schools, parents, women, senior citizens and youth.[262] It asserts a '100% success rate in getting serious cyberbullying material taken down.'[263] It is worth noting that it regards 'cyber-bullying' as something that only happens by definition to children aged 18 years or younger. Adults many report an incident to the Australian Cybercrime Online Reporting Network (ACORN). ACORN 'is a national policing initiative of the Commonwealth, State and Territory governments. It is a national online system that allows the public to securely report instances of cybercrime.'[264] ACORN has a much broader mandate than just cyberbullying.



[258] Dawes Centre for Future Crime, Home <www.ucl.ac.uk/dawes-future-crime> accessed 21 March 2018.
[259] *Ibid.*
[260] It is the first centre of its kind in Europe: it offers integrated PhD programmes for multidisciplinary security or crime-related research: UCL SECReT, Home <www.ucl.ac.uk/secret> accessed 21 March 2018.
[261] NYU-Abu Dhabi, 'Centre for Cyber Security' <https://nyuad.nyu.edu/en/research/centers-labs-and-projects/nyuad-ccs.html> accessed 21 March 2018.
[262] Office of the eSafety Commissioner, 'About the Office' <www.esafety.gov.au/about-the-office/role-of-the-office> accessed 21 March 2018.
[263] Office of the eSafety Commissioner, 'Online Wellbeing Hub' <www.esafety.gov.au/online-wellbeing-hub> accessed 21 March 2018.
[264] Australian Cybercrime Online Reporting Network, 'About the ACORN' <www.acorn.gov.au/about-acorn> accessed 21 March 2018.

There are other institutions abroad that are focused solely on young people: in the UK there is the UK Safer Internet Centre.[265] It has three main functions: an awareness centre (to provide advice and support), a 'Helpline' (to provide support to professionals working with children and young people with online safety issues) and a 'Hotline' (an anonymous and safe place to report and remove child sexual abuse imagery and videos, wherever they are found in the world).[266] Childnet International is a UK-based charity organization, founded in 1995, that works with partners around the world to make the internet safer for children.[267] The UK is also the base for the Internet Watch Foundation (IWF), which works with Internet companies to protect child victims – it works with partners worldwide to remove child sexual abuse images.[268] In terms of assisting schools in the UK to safeguard students online, the South West Grid for Learning (SWGfl) is the leading organisation. It operates across the UK, Europe and worldwide.[269] To round out this discussion it is worth noting that Canada has a national public awareness campaign called 'Get Cyber Safe', a government-run campaign that is part of Canada's Cyber Security Strategy.[270] It includes cyberbullying material. There is the Dutch-inspired International Association of Internet Hotlines (INHOPE), an active global network of Hotlines, dealing with illegal content.[271] INHOPE has 48 member countries (but none from the MENA region).

*5.2 Recommendations*

A number of recommendations can be drawn from this research. They are summarised here as follows.

1. A comprehensive national cyber security strategy is essential for every country. Such a strategy must take into account *all* aspects of cybercrime, encompassing not only security and economic harm but also emotional harm.[272]

[265] It provides safety tips, advice and resources to help children and young people stay safe online: UK Safer Internet Centre, 'Home' (no date) <www.saferinternet.org.uk/> accessed 21 March 2018.
[266] UK Safer Internet Centre, 'About' (no date) <www.saferinternet.org.uk/about> accessed 21 March 2018.
[267] Childnet, 'What we do' <www.childnet.com/what-we-do> accessed 21 March 2018.
[268] Internet Watch Foundation, 'Our remit and vision' (no date) <www.iwf.org.uk/what-we-do/why-we-exist/our-remit-and-vision> accessed 21 March 2018.
[269] SWGfl, 'Online Safety Services' (no date) <https://swgfl.org.uk/products-services/online-safety/> accessed 21 March 2018.
[270] Government of Canada, 'Canada's Cyber Security Strategy' (5 August 2016) <www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx> accessed 21 March 2018.
[271] INHOPE, 'Who we are' (no date) <www.inhope.org/gns/who-we-are/at-a-glance.aspx> accessed 21 March 2018. Its main aim is to remove child sexual abuse imagery internationally.
[272] Note that there were calls in 2017 for Kuwait to adopt a national cyber security strategy, but the calls seemed limited to warding off hacking of computer systems, with an emphasis on the economic and security risks. A cyber strategy should encompass those, but personal harms, too. See CyberSenseWorld, 'Kuwait looks to boost cyber security' 13 June 2017 <http://cybersense-world.com/2017/06/13/kuwait-looks-to-boost-cyber-security/> accessed 21 March 2018.

2. Every government should also initiate reviews in two key areas: 1) all existing laws, as they pertain to cyberbullying/online harassment to determine whether they adequately protect all individuals from harmful digital communications; and 2) commission social-science research to measure the extent of current cyberbullying/online harassment along the lines of the UK's 'Ditch the Label' research. If a country has a Law Commission, that is the ideal body for legal review. However, if there is no such body, the review could be undertaken by a university or an independent think-tank.[273]
3. Law reform: All jurisdictions that are considering a new way forward should at least consider New Zealand's model. New Zealand found that the best solution was an entirely new law, the HDCA 2015, to create a new criminal offence and a new civil regime to takedown material and hold hosts accountable, but this law also amended some other laws to bring them into line with the digital age. Having one comprehensive law, which encompasses all aspects of the cyberbullying problem, is a workable and powerful solution.
4. An organization like 'Netsafe' is needed in all jurisdictions. If a country does not already have one, it should consider establishing an organisation like Netsafe or the Office of the eSafety Commissioner. Every country needs an independent, free-to-access, confidential service staffed by professionals from a range of areas (law, technology, education) who can receive all complaints about personal online harm. This organization should be empowered to 'triage' the complaints (ie advise complainants on their options), direct victims to the Police if necessary, approach web hosts to take down content and, if necessary, help victims take civil proceedings in court as a last resort. Netsafe is an excellent one-stop-shop for combatting cyber-bullying which is certainly worth considering.
5. All jurisdictions that have yet to tackle this issue should at least consider the possibility of a 'Communications Tribunal' or an independent commissioner to hear complaints and provide legal redress by quicker, cheaper means that normal courts.[274] Having technical expertise available to a legal tribunal, combined with a fast-tracked process, might be a good solution for some jurisdictions.
6. The New Zealand HDCA is a good piece of legislation, but the civil penalties may be a concern. They are yet to be tested. However, a fine of $200,000[275] seems

[273] At the University of Auckland in New Zealand, Dr Claire Meehan has received $23,000 from the Faculty Research and Development Fund to examine online sexual harm and what schools are doing to keep children safe: see Auckland University, 'Sex, drugs and cybercrime' (2 June 2016) <www.auckland.ac.nz/en/about/news-events-and-notices/news/news-2016/06/sex-drugs-and-cybercrime.html> accessed 20 March 2018.
[274] See the recommendation of the NZLC, discussed above at section 1.2.
[275] The HDCA 2015 s 21(2) imposes a fine not exceeding $20,000 on a body corporate if they fail, without reasonable excuse, to comply with an order made under s 18 or 19 of the Act (eg. a take-down order).

somewhat light for a large corporation. Germany's 'Netzwekdurchsetzungsgesetz' or 'NetzDG' law imposes fines on hosts of €50 million if big social networks such as Facebook, Google and Twitter fail to take-down content. There is also no means of having material reinstated in New Zealand (or in Germany) if the initial 'notice of complaint' is found to have been made in error.

7. The New Zealand HDCA seems to be striking the right balance between freedom of expression and protecting individuals from harm. However, the anonymisation process used by the Department of Justice to protect the victims creates some difficulties for researching case law on this provision.[276]
8. Education must play an important role in combatting cyber-bullying. It has not been the focus of this paper, but it is obvious that 'law alone cannot be the sole answer to problems of cyber-victimization'.[277] Netsafe has a contract with the New Zealand Ministry of Education whereby it provides advice and training to teachers and schools' Boards of Trustees on how to promote safe digital behavior in schools. Currently the NZ Police has representatives visiting all New Zealand high schools to communicate messages about cyberbullying. This strategy is a good idea for all jurisdictions to consider. Since the problem disproportionately affects youth, the need for appropriate education and policies in schools, universities and other training facilities is beyond debate.
9. Universities and schools should have disciplinary policies in place to protect their faculty and students from harmful content which negatively affects the learning environment – even if there is no national law protecting students and faculty from cyberbullying. The US has had many cases whereby students and professors have been harmed by online speech. This is a topic that should be discussed within all universities so that clear guidelines can be decided upon and communicated to all stakeholders.
10. Scholarship and research are essential if societies are to stay up-to-date with the challenges of the digital age. Universities around the world are adding 'cybercrime' and 'law and technology' to their law schools' list of paper offerings, and even LLM and PhD specialties in this area are emerging. Some universities, like the Universities of Auckland and Otago in New Zealand, are establishing standalone 'ICT Centres' which can specifically focus on all aspects of cyber law. These

[276] For example, one case *The Queen v Partha Iyer* was appealed to the High Court where it was referred to as *R v B* and then when it continued in the District Court the name is unclear but probably will eventually be published as *R v B*. This process may need to be streamlined to ensure that the same name is used throughout the process and also that all cases involving the HDCA are indeed posted online pursuant to HDCA s 16.

[277] Lipton J, 'Combatting Cyber-Victimization' (2011) *Berkeley Tech Law Journal* 26, 1103, 1116 <https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1901&context=btlj> accessed 28 March 2018.

centres are part of the future: all law schools should consider establishing a specialist centre or research group for the study of ICT-related issues. Ideally, they should be staffed by experts across different disciplines including law, social sciences, technology and education. These centres should work on keeping abreast of the legal issues that *continue* to arise from technology, make recommendations to government and monitor the implementation of new laws.

The interface between law and technology and law is changing rapidly. Every society needs to be equipped for the challenges that already exist and those that are yet to be identified. If it has not already done so, every government needs to devise a comprehensive strategy for how to deal with the many facets of social and legal problems posed by new technology – and it has to keep revisiting this strategy to see if it is fit for purpose. All aspects of cybercrime, including cyberbullying, need to be part of it. Therefore, every jurisdiction—including every law school within each jurisdiction—needs to urgently consider how well it is prepared for the digital future and how to best exploit, and protect itself, from the inherent dangers that are connected with the opportunities.