LAW·COMMISSION
TE·AKA·MATUA·O·TE·TURE

Wellington, New Zealand |August 2 0 1 2

Ministerial Briefing Paper

HARMFUL DIGITAL COMMUNICATIONS: The adequacy of the current sanctions and remedies

The Law Commission is an independent, publicly funded, central advisory body established by statute to undertake the systematic review, reform and development of the law of New Zealand. Its purpose is to help achieve law that is just, principled, and accessible, and that reflects the heritage and aspirations of the peoples of New Zealand.

The Commissioners are:

Honourable Sir Grant Hammond KNZM – President

Dr Geoff McLay SJD; Mich

Honourable Dr Wayne Mapp Ph D; Cantab

The General Manager of the Law Commission is Brigid Corcoran

The office of the Law Commission is at Level 19, HP Tower, 171 Featherston Street, Wellington

Postal address: PO Box 2590, Wellington 6140, New Zealand

Document Exchange Number: sp 23534

Telephone: (04) 473-3453, Facsimile: (04) 471-0959

Email: com@lawcom.govt.nz

Internet: www.lawcom.govt.nz

FOREWORD

In New Zealand, as in many other countries, there is growing and strong concern about the use of new communication technologies to cause harm. Young people are particularly vulnerable, but the problem is by no means confined to them: there are examples of the most disturbing and damaging communications between adults as well. There is a widespread desire that something be done.

Because of these concerns, the Minister Responsible for the Law Commission, the Honourable Judith Collins, has asked the Law Commission to expedite the part of its project on the New Media which deals with this topic.

The Commission has considered the many submissions it received on its issues paper "The New Media meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age." It has also undertaken further research, commissioned an online survey and consulted with a number of key agencies and persons. We record our particular thanks to the Police, the Chief Coroner, the Human Rights Commission, NetSafe, Trade Me, Judge David Harvey, Dr John Fenaughty and Steven Price for so generously making available their time, experience and expertise. We also wish to acknowledge our debt to Steven Price's writings on the subject.

Something needs to be done. We present our findings and recommendations in this paper. They form an integrated package which we believe is a proportionate response to a growing problem.

In order to meet the shortened time frames it was agreed with the Minister that we would produce a briefing paper containing our recommendations rather than a formal report. However, in every other respect the contents of this paper reflect the normal processes employed by the Commission in arriving at its final position. This paper will be attached to our final report on the New Media, as an appendix, in due course.

This project was led by John Burrows. The legal and policy advisers were Cate Honoré Brett, Rachel Hayward and Joanna Hayward.

Hon Sir Grant Hammond KNZM
President of the Law Commission

Harmful Digital Communications: the adequacy of the current sanctions and remedies

CONTENTS

Summary

HOW THIS REPORT CAME ABOUT

1. In New Zealand, as in many other jurisdictions around the world, there is growing concern about the use of new communication technologies to cause harm. Cyberspace, in one commentator's view, has provided a "vast unsupervised public playground" where bad actors can harass, intimidate, and defame, causing emotional and psychological distress to others with relative impunity.[1]
2. Young people, who are both guinea pigs and pioneers in this technological revolution, are particularly vulnerable. In 2011, the Prime Minister John Key called for a "national conversation" on how to reduce bullying in our schools after cell phone videos of children being bullied became prominent on the internet.[2]
3. In recent months New Zealand's Coroners, Police and the Post Primary Teachers' Association (PPTA), which represents secondary school teachers, have all expressed concerns about cyber-bullying and the ways in which the abuse of communication technologies is contributing to some significant issues facing adolescents. These range from truancy and school failure to issues such as depression, self-harm and suicide.[3]
4. In May 2012, in response to these rising concerns, the Minister responsible for the Law Commission, the Hon Judith Collins, asked us to fast-track part of our project reviewing the adequacy of the regulatory environment for dealing with new and traditional media in the digital era.
5. Our preliminary proposals were set out in an Issues Paper *The News Media Meets 'New Media': rights, responsibilities and regulation in the digital age* published online in December 2011.[4] In this paper we considered the problem of harmful

---

1 Report of the Nova Scotia Task Force on Bullying and Cyberbullying *Respectful and Responsible Relationships: There's No App for That* (Nova Scotia, 29 February 2012) at 12.

2 Audrey Young "PM Tells Schools to Act Against Bullies" *The New Zealand Herald* (online ed, New Zealand, 29 March 2011).

3 Simon Collins and Vaimoana Tapaleao "Suicide link in cyber-bullying" *The New Zealand Herald* (online ed, New Zealand, 7 May 2012); Submission of New Zealand Police (March 2012); Submission of New Zealand Post Primary Teachers' Association (March 2012).

4 Law Commission *The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the*

digital communication by citizens as part of a wider review of the adequacy of the regulation of both new and traditional media in the digital era.

6. In this report, prepared at the Minister's request, we deal exclusively with the part of our review which is concerned with the use of new communication technologies by citizens. We address three questions:

   (a) how to adapt our laws to ensure they are fit for purpose in the digital era;

   (b) how to ensure these laws can be understood and accessed by ordinary citizens; and, critically

   (c) how citizens can access meaningful remedies when they have experienced significant harm as a result of digital communication.

7. Our proposals are focused primarily on the law. But amending the law and introducing new offences will not be enough. Unless the law is understood by citizens, consistently enforced, and its remedies meaningfully applied, it is of limited value. Hence we are as much concerned in this report with putting forward proposals for how to make the law *accessible* and *effective* in the age of mass participatory media as we are with the creation of new offences.

8. Even then, better and more accessible laws will only go so far in addressing digital communication harms. We must also address the growing information and power asymmetries which exist in cyberspace. The digital divide applies not only in relation to access to technology but also with respect to people's ability to harness the power of technology for legitimate and illegitimate purposes.

9. For concepts like "digital citizenship" to have meaning, there will need to be a collaborative approach. This will require involvement from a number of participants including parents, schools, law enforcement agencies, policy makers and the domestic and global corporations which act as intermediaries between citizens and the networked public spheres in cyberspace where an increasing amount of our lives are spent.

10. Hence we emphasise the need for our recommendations to be treated as a package: law change without education and without mechanisms for effective enforcement will not succeed.

11. The fundamental planks of our reform, which are summarised on pages 14-20, are:

Digital Age (NZLC IP27, 2011).

- **The creation of a new criminal offence tailored for digital communication.**
- **Amendments to the Harassment Act 1997, the Human Rights Act 1993, the Privacy Act 1993 and the Crimes Act 1961 to ensure that the provisions of these Acts can be readily applied to digital communications.**
- **The establishment of a Communications Tribunal to provide citizens harmed by digital communications with speedy, efficient and cheap access to remedies such as takedown orders and "cease and desist" notices.**
- **New legal requirements for all New Zealand schools to help combat bullying of all kinds, including cyber-bullying**.

12. Some of the proposals we put forward in this report are novel and in the following summary we are only able to outline them in broad terms. We strongly encourage readers to refer to relevant sections of the report for a full explanation of what is proposed. A draft bill is annexed to the report.
13. Although this report has been fast-tracked, its content and structure reflect the usual processes undertaken by the Commission when finalising recommendations for Government. These include a three month period for submissions, and further research and consultation following the publication of our Issues Paper.

OUR APPROACH & TERMINOLOGY

14. In this report we consider the issue of cyber-bullying within the wider context of harmful digital communication. It is a subset of the type of communication harms we have been asked to address. Adolescents and schools are not immune from the law and while it is important not to criminalise young people, it is also important that they understand what society expects and the types of behaviours it will punish.
15. Throughout this report we use the term "harmful digital communication" to describe the type of behaviour our reforms are targeting. We have adopted this term in preference to the term "speech harms", which we used in the Issues Paper, because we think it better reflects the multi-media nature of much digitally mediated interaction in cyberspace.
16. The term applies not only to one-to-one communication but more broadly to the range of digital publishing which occurs in cyberspace. This includes the uploading of user-generated content (audio-visual, pictures or text) on websites and platforms such as

YouTube and Facebook, and the use of micro-blogging sites like Twitter to disseminate information and opinions.

17. The distinguishing feature of electronic communication is that it has the capacity to spread beyond the original sender and recipient, and envelop the recipient in an environment that is pervasive, insidious and distressing.

18. The concept of harm is also pivotal to this report. In the context of this report we use the term "harmful" to describe the full range of serious negative consequences which can result from offensive communication including physical fear, humiliation, mental and emotional distress. Not all harms arising from communications are proscribed by law. The criminal law has typically been concerned with protecting citizens from communication harms which invoke fear for physical consequences, either personal or proprietary, or which are obscene or harmful to children. The civil law, in the past, also typically shied away from providing remedies for emotional harm as such. However, as we demonstrate later, in both civil and criminal spheres the law has been moving towards recognition of, and protection from, emotional harm.

19. Nevertheless we recognise that there will be some difficult issues at the margin. Within the community at large and within younger demographics particularly, the threshold for when a communication causes the level of distress that can be described as "harmful" and when it simply causes annoyance or irritation may sometimes be difficult to pinpoint.

20. But we have reached the view that when the level of emotional distress can be described as *significant*, the law has a role to play.

The importance of freedom of expression

21. This report is primarily about the laws to which we are all accountable when we communicate. Its recommendations are not aimed at censorship. Nor are they about criminalising speech which offends people *simply* because it may be abusive, nasty, vulgar, untrue or inflammatory.

22. Freedom of expression is a fundamental human right enshrined in the New Zealand Bill of Rights Act 1990. The Act specifies that freedom of expression "may be subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society." Precisely where the law sets those limits is a reflection of our core values as a society, including what value we place on tolerance, civility and inclusivity.

23. Overseas jurisprudence increasingly recognises differences in the value of different kinds of speech. Political speech is seen as being of the highest importance, gratuitous personal attacks and "hate speech" the lowest – although even there the reaction of the law must not be disproportionate: freedom of speech is too important.

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

25. For example, many New Zealanders will be surprised to learn that our current Telecommunications Act 2001 contains a little known (or used) provision, dating back to 1987, prohibiting the use of a telephone to intentionally offend someone by using "profane, indecent, or obscene language". The Act also makes it an offence to use the telephone "for the purpose of disturbing, annoying, or irritating any person, whether by calling up without speech or by wantonly or maliciously transmitting communications or sounds, with the intention of offending the recipient."[5]

26. The threshold ("disturbing", "annoying", "irritating", "offending") seems low by today's robust standards. There is perhaps doubt whether it would now survive a Bill of Rights vet.[6]

27. However, clearly there must be some limits to what is regarded as acceptable expression. That is the task we are confronting in this report and the task Parliament will grapple with should it decide to proceed with the changes we are recommending. We believe the limitations on freedom of expression which we recommend are justified, indeed necessary, to mitigate the harms which we have identified.

---

5 Telecommunications Act 2001, s 112(a), s 112(b).

6 Although we support the premise that causing offence may in some circumstances constitute a criminal offence, we believe the threshold created in this offence may be so low as to be incompatible with the Bill of Rights Act and today's robust communication environment. Nor is it clear the provision as currently drafted applies to all digital communication. We therefore believe that consideration should be given to reviewing this provision– see chapter 4, para [4.79].

SUMMARY OF CONTENTS

The problem

28. In chapter 2 of this report we revisit the problem described in our Issues Paper, and address the following critical questions:

    (a) What differentiates digital communication and how do these differences affect the nature and severity of harms associated with speech abuses?

    (b) How serious is the problem – and in particular, how is it impacting on vulnerable sections of the population, especially the young?

29. With respect to the first question, we note the following critical features which distinguish digital communication and its associated harms from offline communication:

- The viral nature of cyberspace and the potential for information to be disseminated instantly to worldwide audiences;
- The ubiquity of the technology which means communications are no longer constrained by time and place but can be accessed anywhere, anytime by anyone;
- The persistence of information disseminated electronically;
- The ease with which digital information can be accessed/searched;
- The facility for anonymous communication and the adoption of multiple online personae.

30. We conclude that these characteristics are producing novel ways in which people can cause harm to one another. And, as a recent Nova Scotia report on cyber-bullying notes, they have also unlocked the potential of the bully:[7]

> Traditional bullying tends to take place in secluded places, like washrooms, hallways and school buses, where there is little adult supervision. The cyber-world provides bullies with a vast unsupervised public playground, which challenges our established methods of maintaining peace and order – it crosses jurisdictional boundaries, is open for use 24 hours a day, seven days a week, and does not require simultaneous interaction.

31. The facility to generate, manipulate and disseminate digital information – which can be accessed instantaneously and continuously – is producing types of abuse which simply have no precedent or equivalent in the pre-digital world.

---

7 Report of the Nova Scotia Task Force on Bullying and Cyberbullying *Respectful and Responsible Relationships: There's No App for That* (Nova Scotia, 29 February 2012) at 12.

32. Citizens, including teenagers and younger, with no specialist expertise or technical assistance can, in effect, cause irreparable harm to one another's reputations and inflict enduring psychological and emotional damage.

33. In chapter 2 of the report we provide examples of how these defining characteristics of digital communication are giving rise to novel harms. We discuss the range of serious impacts that covert and overt bullying can have on adolescents, including contributing to educational failure, depression and self-harm. With respect to suicide and self-harm, we emphasise that bullying is only one of a number of complex inter-related risk factors. Its impact, like the impact of other stressors, will vary according to a range of variables including the person's resilience, their home and school environment and any underlying personality or psychiatric disorders – most significantly, depression.

34. We also stress the importance of approaching adolescent aggression within the broader context of adult aggression and role modelling. NetSafe, an organisation focused on improving cyber safety in New Zealand, emphasised in its submission that more than half of the approximately 75 serious complaints they deal with each month involve adults, the majority of whom have been directed to them by Police after exhausting other avenues of complaint.[8]

35. NetSafe noted that "the distress of those contacting our service is often painfully apparent. The majority of adult targets contact us after being threatened with physical harm."[9]

36. Although unable to provide quantitative data, Police submitted that staff were dealing with a "growing number of complaints from members of the public who have been intimidated, bullied, harassed and threatened on the Internet."[10]

37. We note that the paucity of quantitative national data on cyber-related communication harms creates challenges for policy makers.

---

8 NetSafe was established in 1998 as an independent non-profit organisation committed to improving community understanding of the internet and how to enhance safety and security online. It works with a range of governmental and non-governmental organisations including its core strategic partners, the Ministry of Education, the Ministry of Economic Development and InternetNZ, a non-profit open membership organisation whose aim is to promote and protect the internet in New Zealand.

9 Submission of NetSafe (24 February 2012) at 1.

10 Submission of New Zealand Police (March 2012) at 3.

38. Independent research we commissioned suggests that as many as one in ten New Zealanders has some personal experience of harmful communication on the internet. That rate more than doubles to 22 per cent among the 18-29 demographic who are the heaviest users of new media.[11] Research undertaken by NetSafe's former Research Manager, Dr John Fenaughty, in conjunction with the University of Auckland found that 1 in 5 New Zealand high school students experienced some form of cyber-bullying or harassment in 2007.[12]

39. These figures are broadly consistent with the academic literature although estimates vary depending on the different definitions, samples and methodologies used.

40. Irrespective of the quantum of the problem, in our view, this potential to cause significant harm, some of it indeed devastating, demands an effective legal remedy.

The case for change

41. As Google pointed out in its submission to this review, "the mere existence of harmful speech is not sufficient to justify additional regulation. It is necessary to show that existing legal and self-regulatory remedies are ineffective."[13]

42. In chapter 3 we review the effectiveness of the range of tools available to manage and mitigate the types of harm described in chapter 2. We discuss the concept of "digital citizenship" and the importance of empowering users through education about the use of digital technology and the rights and responsibilities that accompany this. We also review the self-regulatory systems already in place within different networked public spheres on the internet such as user "terms of use agreements" and community moderation and reporting tools.

43. In Google's view the paradigm shift in how citizens use new media, and in particular the degree of control and choice they are able to exercise over how they interact and what they consume, has fundamental implications for how problems such as harmful content should be managed in the digital era:[14]

---

11 Under s 6(2)(b) of the Law Commission Act 1985 the Commission is mandated to "initiate, sponsor, and carry out such studies and research as it thinks expedient for the proper discharge of its functions." For a full discussion of the research refer chapter 2, para 2.20 of this report.

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

13 Submission of Google New Zealand Ltd (14 March 2012) at 16.

14 Ibid, at 15.

> [O]line communities set, refine and enforce their own community standards. If content is made available that is considered to be unacceptable or offensive, users will protest and remedial action can be taken very quickly. Online businesses risk their livelihood if inappropriate content is repeatedly published as audiences and users will quickly switch to other sites.

44. Both Google and Facebook argued that policies directed at reducing the problem of harmful communication in cyberspace need to focus in the first instance on empowering users by educating them about their rights and responsibilities as "digital citizens" and providing them with the technological tools to exercise these rights and responsibilities effectively. These strategies are reinforced by the "terms of use" agreements employed by many internet intermediaries and, ultimately, by the legal systems which apply to the users themselves and the content they create.

45. We endorse this approach and believe it is both consistent with the principles of freedom of expression and reflects the practical realities of the new era of mass participatory media.

46. The question we address in chapter 3 is whether this combination of self-regulation, underpinned by domestic law, is in fact providing effective remedies for those who experience significant harms as a result of communication abuses. *In other words, is there a gap between the reach of the self-regulatory systems on the web and the reach of the law?*

47. In our view there is such a gap. In paragraphs 3.63 – 3.92 we put forward our reasons for reaching this conclusion. These are based on our own research into the effectiveness of self-regulatory tools; the evidence of submitters and our review of New Zealand's existing speech laws. The following critical points inform our assessment:

    (a) User empowerment is a laudable ideal but for the moment there exist a number of important information and power asymmetries in cyberspace. The digital divide applies not only in relation to access to technology but also with respect to people's ability to harness the power of technology for legitimate and illegitimate purposes.

    (b) Self-regulatory systems on the internet are extremely variable reflecting the huge spectrum of services, platforms and content hosts available to users. Given the unprecedented volume of data exchanged on the internet every day, and the global nature of many internet intermediaries, it is inevitable that even the most sophisticated self-regulatory systems will fail at times.

(c) The most serious types of harmful digital communication will often involve a breach of the law. A number of the examples cited in chapter 2 of this report did in fact end up being prosecuted under existing offences. However, the existing law is not always easily applied to digital communication and not all of the new and potentially more damaging harms arising from the use of new technology are covered by existing laws. This is particularly so with respect to the severe emotional distress which can be caused by invasive and ubiquitous digital communications.

(d) Critically, the law, like terms of use agreements, is only useful if it is accessible and enforceable – and capable of providing effective remedies. While the existing criminal and civil law could deal with many types of harmful digital communications, in practice there are a number of obstacles that impede access to justice by those who have suffered harm. These include:

(i) A lack of knowledge of the law and/or the availability of redress, by both victims and enforcement officers;

(ii) The complexity of identifying possible defendants in an online situation;

(iii) The breadth and speed of spread of information on the internet;

(iv) Problems of establishing jurisdiction, where material is hosted overseas.

48. Submissions confirmed the themes that had emerged from our preliminary research and consultation as to the problems people encounter in accessing help to deal with cyber-offending, and their resulting sense of powerlessness.

49. While it is not possible to overcome all of these problems, we believe our package of reforms will make a significance difference.

SUMMARY OF RECOMMENDATIONS

1. A new communications offence tailored for digital communication

50. One of the key conclusions we reach in chapter 2 of this report is that the new communication technologies can have effects which are more intrusive and pervasive, and thus more emotionally harmful than in the pre-digital era. The impacts of such behaviour can derail lives and contribute to mental illness, suicide and self-harm. Overseas jurisdictions, including the United Kingdom, Australia and some states in

America, are increasingly moving to criminalise communication causing serious distress and mental harm.[15]

51. In New Zealand currently the criminal law currently provides only limited protection against communications which cause mental distress – in the absence of physical threats.

52. We recommend the introduction of a new offence which targets digital communications which are "grossly offensive or of an indecent, obscene or menacing character" *and* which cause harm.

53. While criminalising young people is to be avoided, in egregious cases, this new offence could be applied to anyone over the age of 14, with those aged between 14 and 17 being tried in the Youth Court (see paragraph 4.76 of the report and recommendation R1 for a full explanation of the offence and draft wording).

54. Types of digital communications covered by the offence would include comments on websites, message boards and blogs, and in the social media (e.g. Facebook and Twitter), and also emails and texts. The distinguishing feature of electronic communication is that it has the capacity to spread beyond the original sender and recipient, and envelop the recipient in an environment that is pervasive, insidious and distressing.

2. Amendments to existing laws to ensure fitness for purpose

55. With the exception discussed above, we conclude that by and large New Zealand's existing criminal and civil law is capable of being applied to digitally mediated communications. However we recommend a number of amendments to both criminal and civil laws to make them better fit for this purpose. These include amendments to **the Harassment Act 1997, the Human Rights Act 1993, the Privacy Act 1993 and the Crimes Act 1961** to ensure that the provisions of these Acts can be readily applied to digital communications.

56. In some instances we recommend extending their scope to cover behaviours enabled by new communication technologies such as the publication online of intimate photographs. Under our proposed amendments it would be an offence to publish intimate photographs or recordings of another person without their consent. We also recommend that the laws about online sexual grooming be tightened.

15 See chapter 4 at [4.73]-[4.75] for a discussion of these developments.

57. We recommend that it become an offence to incite a person to commit suicide, irrespective of whether or not the person does so.

3. The establishment of a Communications Tribunal

58. In chapter 3 of this report we point out that even the most sophisticated web-based moderation and reporting systems cannot always provide the type of timely, tailored response required in cases of serious harm.

59. **To bridge this gap we recommend the establishment of a specialist Communications Tribunal capable of providing speedy, cheap and efficient relief outside the traditional court system**. It would in effect operate like a mini-harassment court specialising in digital communications. New Zealand already has precedents for such informal methods of dispute resolution in the form of the Tenancy Tribunal, the Human Rights Review Tribunal and the Disputes Tribunal.

60. The Tribunal we propose would comprise a District Court judge supported (where necessary) by an expert internet adviser. There would be a number of judges designated to act. It would have the following features and powers:

    (a) The Tribunal's jurisdiction would be protective, rather than punitive or compensatory. It would not have any powers to impose criminal sanctions. It would be limited instead to providing civil remedies, such as takedowns and cease and desist orders. In some cases it might also require apologies, right of reply, corrections or retractions. We do not propose that it have any power to award monetary compensation.

    (b) The Tribunal would be a solution of last resort and the threshold for obtaining a remedy would be high. Complainants would have to demonstrate that the communication complained about had caused significant harm, including distress, humiliation or mental harm. They would first have had to attempt to resolve the matter through other avenues.

    (c) Before granting a remedy the Tribunal would need to determine that the communication not only caused significant distress but that it also breached one or more of a set of principles we have proposed. These principles will be substantially derived from the existing and proposed criminal and civil laws we have discussed in this report. They would make accessible to ordinary citizens the fundamental legal rights and responsibilities which attach to the use of modern communication technologies.

(d) Among the other factors the Tribunal would have to take into account would be: the *nature* and *purpose* of the communication and whether it was the type of speech requiring high protection, such as political speech; the truth or falsity of the statement; the context in which it was expressed; and the conduct of the complainant – including the extent to which that conduct may have contributed to the harm suffered.

(e) An order by the Tribunal would not preclude a complainant from also pursuing a civil action or criminal prosecution. Its role is to provide a speedy and accessible remedy in cases of significant harm. Punishment is a matter for the courts.

(f) The news media would not be subject to the Tribunal except in cases where the news media outlet responsible for publishing the offending content was not subject to one of the established regulatory bodies – the Broadcasting Standards Authority or the Press Council or any regulator which may replace them.

61. Those entitled to complain to the Tribunal should be the victims themselves or parents or guardians where the victim is a child or young person. In addition the Chief Coroner, Police and School Principals would have direct access to the Tribunal in serious cases involving threats to safety or where there has been a breach of the Coroners Act 2006 with respect to publishing details of a suicide.

62. In the first instance the target of Tribunal orders would be the author of the offending communication. Where that person's identity was unknown the Tribunal would have the power to require Internet Service Providers and other intermediaries to reveal the person's identity to the Tribunal.[16] Once notified, anyone subject to an order would have the opportunity to defend the proposed action. In some egregious cases the Tribunal may decide to make the identity of an offender publicly known as a form of deterrence. In cases where the author could not be located an ISP or web administrator may be required to remove or amend the offending content.

63. We propose that the Tribunal would be empowered to make orders against minors in cases of persistent and serious cyber-bullying which have not been satisfactorily resolved by a school or other agency.

16 These proposed powers to obtain account details are similar to those vested in the Copyright Tribunal under provisions of the Copyright (Infringing File Sharing) Amendment Act 2011.

4. The establishment of a statutorily recognised mediation agency

64. Before a complainant came to the Tribunal there would need to be evidence they had taken steps to resolve the problem themselves. This requirement serves two purposes: first it would ensure the Tribunal was not overwhelmed with trivial cases, and second, it is consistent with the premise that the first line of defence against harmful communication in cyberspace should be users themselves.

65. We recommend that NetSafe be given statutory recognition as an "approved agency" responsible for triaging and, where possible, mediating complaints before they reach the Tribunal.[17] As we have already noted, the non-profit NGO NetSafe is one of few organisations specifically focused on bridging the digital divide and actively promoting digital citizenship through education, advice and practical technological support. It works collaboratively with a number of government departments and organisations including the Police, and the Ministries of Education and Economic Development.[18] It has undertaken pioneering work in the education sector around responsible use of online technologies and initiated the National Task Force on Cyber-Bullying. As noted by Google in its submission to us, NetSafe's programmes have been described as "world leading".[19]

66. We recommend that the advisory and mediation functions NetSafe currently carries out be given formal recognition. Specifically we propose that NetSafe be deemed an "approved agency" with the responsibility to advise complainants and, where appropriate, attempt to achieve a resolution by negotiation, mediation and persuasion. In cases involving clearly criminal behaviour, or where the harm was so immediate and significant, complaints could be re-directed immediately to the Police and/or Tribunal.

67. In order to carry out this front-line advisory effectively NetSafe would require a significant boost in resourcing.

---

17 While in our view NetSafe is ideally suited to perform these functions, the proposed legislation would provide for the Minister to appoint any person or organisation as an "approved agency" including for example Police or the Human Rights Commission.

18 The functions of the Ministry of Economic Development have now been integrated into the Ministry of Business, Innovation and Employment.

19 Submission of Google (14 March 2012) at 27.

The role of ISPs and other Intermediaries

68. The development of consistent, transparent, and accessible policies and protocols for how intermediaries and content hosts interface with our proposed Tribunal and with the approved agency (our recommendation is NetSafe) will be critical to their effectiveness.

69. We recommend that the approved agency work with these private sector agencies, including New Zealand's telecommunications companies, to develop such guidelines and protocols. Trade Me, an organisation which has both considerable technical and regulatory expertise would be an invaluable partner in that process.

5. Cyber-bullying and schools

70. The law changes proposed in this report and the back-stop created by the proposed new Communications Tribunal will support the work of parents and schools combatting cyber-bullying. Young people aged 14 and over will be subject to the new electronic communications offence. They will also be subject to the rulings of the Communications Tribunal. The Chief Coroner, Police and School Principals will be able to seek the Tribunal's assistance in cases where there is a risk to life including potential contagion effects with respect to youth suicides.

71. In addition we make the following specific recommendations:

(a) Introduce the following new legal requirements for all New Zealand schools to help combat bullying of all forms, including cyber-bullying:

(i) The National Administrative Guidelines for public schools should include a requirement that a school must implement an effective anti-bullying programme;

(ii) The law should be amended to make it a criterion for registration of a private school that the school provide a safe and supportive environment that includes policies and procedures that make provision for the welfare of students.

(b) In addition, we recommend the Ministry of Education consider;

(i) The development of an agreed definition of bullying behaviour, including cyber-bullying, encouraging schools to use it in anti-bullying policies;

(ii) The establishment of on-going and routine data collection systems with standardised methods for defining and measuring covert and overt forms of bullying;

(iii) The development of measurable objectives and performance indicators for activities intended to improve school safety; and

(iv) The development of reporting procedures and guidelines.

(c) We also propose that schools explore expanding the use of Information and Technology contracts, which are routinely used in schools, to educate students about their legal rights and responsibilities with respect to communication. These contracts could incorporate the communication principles which will underpin the work of the new Communications Tribunal. This distillation of the law into simple and accessible principles could provide teachers and parents with a valuable tool for introducing young people to some of the fundamental values which are reflected in our law.

72. A full discussion of each of these recommendations, and the policy rationale for them, can be found in the relevant sections of this report. In particular we draw readers' attention to chapter 4 where we address the Bill of Rights issues raised by our proposals.

Chapter 1: What this is about

THE SCOPE OF THIS INQUIRY

Our terms of reference

1.1 In October 2010 the Law Commission was asked by the Government to review the adequacy of the regulatory environment in which New Zealand's news media is operating in the digital era.

1.2 As part of this review we were asked to deal explicitly with the following questions:

- how to define "news media" for the purposes of the law;
- whether, and to what extent, the jurisdiction of the Broadcasting Standards Authority and/or the Press Council should be extended to cover currently unregulated news media and, if so, what legislative changes would be required to achieve this end; and
- whether the existing criminal and civil remedies for wrongs such as defamation, harassment, breach of confidence and privacy are effective in the new media environment and, if not, whether alternative remedies may be available.

1.3 In November 2011 we published an Issues Paper, *The News Media Meets 'New Media': rights, responsibilities and regulation in the digital age,* setting out our preliminary response to the questions posed in our terms of reference and putting forward for public debate a number of preliminary proposals for reform.[20]

1.4 These proposals included changes to existing legislation relating to speech offences and the establishment of two new bodies for adjudicating complaints – one for the news media and another to deal with harmful communications involving private citizens.

1.5 The proposals were widely debated in both traditional and new media forums during a four-month consultation period between December 2011 and March 2012. We received 72 formal submissions and many hundreds of comments and contributions from those participating in online discussions and forums.[21]

---

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

21 The submissions to this review are available on the Law Commission's website at

Cyber-bullying

1.6 Since the publication of our Issues Paper there has been growing concern about the problem of cyber-bullying. Coroners, Police and the Post Primary Teachers' Association (PPTA), which represents secondary school teachers, have all drawn our attention to their concerns about the ways in which the abuse of communication technologies is contributing to truancy, school failure and a range of adolescent problems including depression, self-harm and suicide.[22]

1.7 In May 2012, in response to this public concern, the Minister responsible for the Law Commission, the Hon Judith Collins, asked us to fast track our final recommendations with respect to the third leg of our original terms of reference – the adequacy of the current legal framework for dealing with harmful communications in the digital era.

1.8 Governments in Australia, the United Kingdom, Canada and some states of America are all grappling with these issues and considering ways in which the law and educational policy can effectively intervene to prevent harm to young people.[23]

1.9 The academic literature has established a clear association between bullying and other forms of aggression and a number of negative outcomes for adolescence, including educational failure, depression and self-harm.

1.10 In this report we consider the issue of cyber-bullying within the wider context of harmful digital communication. It is a subset of the type of communication harms we have been asked to address. Adolescents and schools are not immune from the law and while it is important not to criminalise young people, it is also important that they understand what society expects and the types of behaviours it will punish. In chapter 6 of this report we discuss how our overall policy package can support schools and parents in tackling cyber-bullying.

OUR PRELIMINARY PROPOSALS

1.11 In our Issues Paper we reviewed the criminal and civil law of New Zealand to assess its fitness for the digital age. We also considered whether the current legal provisions

<www.lawcom.govt.nz>.

22 Simon Collins and Vaimoana Tapaleao "Suicide link in cyber-bullying" *The New Zealand Herald* (online ed, New Zealand, 7 May 2012); Submission of New Zealand Police (March 2012); Submission of New Zealand Post Primary Teachers' Association (March 2012).

23 For a discussion of the various reports and legislative responses initiated in these jurisdictions see chapter 6 at paras 6.62 –6.70 of this report.

were capable of responding adequately to the types of communication harm which have no precedent in the offline world, such as malicious impersonation or hijacking of another person's online identity.

1.12 As well as assessing the fitness of the law, we raised concerns about the difficulties of accessing and enforcing the law effectively in cyberspace, given the porous nature of the internet, the speed with which content can be disseminated and the difficulty in identifying perpetrators and holding them to account.

1.13 In response to these challenges we put forward a number of preliminary proposals for discussion. These included giving courts the power to issue takedown orders when content was clearly in breach of the law. We raised for discussion two alternative new mechanisms for dealing with harms arising from speech abuses: a Communications Tribunal or a Communications Commissioner.

1.14 The proposed Communications Tribunal was designed to operate as a "mini-court," administering speedy, efficient and relatively cheap justice to those who have been significantly damaged by unlawful communications.

1.15 The second option we put forward for discussion was the establishment of a Communications Commissioner, possibly attached to the Human Rights Commission. The Commissioner would not have the enforcement powers of a Tribunal but rather his or her role would be to provide information and where possible assist in resolving problems in an informal manner, for example through mediation.

THE CONTENTS OF THIS REPORT

1.16 In order to meet the shortened time frames it was agreed with the Minister that we would produce a briefing paper outlining our recommendations for law change rather than a formal report. However in every other respect the contents of this report reflect the normal processes employed by the Commission in arriving at its final policy position. This has included commissioning further independent research, close consideration of the public submissions and on-going consultation with key stakeholders.

1.17 In chapter 2 of the report we revisit the problem of harmful speech on the internet. We outline what submitters told us about the scope and severity of the problem and what our own research reveals. Within this context we also discuss the phenomenon of cyber-bullying, drawing on both New Zealand and international literature.

1.18 Having summarised the problem we then address the question posed by our terms of

reference – are the current remedies fit for the digital age? In chapter 3 we describe a three-tiered approach to addressing harmful digital communication. The first line of defence lies with user empowerment, which includes educating people about their rights and responsibilities as digital citizens and in the use of technology to give effect to these. Secondly, this user empowerment is supported by the self-regulatory tools and infrastructure which private companies have developed to promote good behaviour and deal with problem speech on the net. The third tier is the legal framework which applies to all online communication and which anchors user empowerment and the self-regulatory systems. We access the strengths and weaknesses of this three-tiered approach and set out our conclusions about its effectiveness.

1.19 In chapters 4 – 6 we turn to the solutions. In chapter 4 we outline the specific law changes we are recommending to Government. In chapter 5 we outline our proposal to establish a new Communications Tribunal to provide citizens with access to a quick and affordable means of remedying significant harms arising from digital communications. And finally in chapter 6 we make some specific recommendations about cyber-bullying and how law change may support the many initiatives in this area.

Terminology

1.20 In our Issues Paper we used the term "speech harms" to describe communications which cause harm to others. This encompasses defamatory speech which harms others' reputations; speech which threatens others or which is intended to inflict serious emotional damage; and speech which results in the invasion of a person's privacy.

1.21 However in our view this term does not adequately capture the characteristics of digitally mediated communication which may incorporate speech, text and audio visual elements. We think the term "harmful digital communication" better describes the problem our reforms target.

1.22 The term applies not only to one-to-one communication but more broadly to the range of digital publishing which occurs in cyberspace including the uploading of user-generated content, including audio-visual material on websites and platforms such as YouTube and Facebook, and the use of micro-blogging sites like Twitter to disseminate information and opinions.

1.23 We take a similarly broad view of what is meant by the term 'expression' in the context of human rights debates. As we discuss in chapter 4, our courts have held that

flag burning[24] and lying down in front a car[25] as a protest are forms of 'expression'. So we take the word 'expression' as being wide enough to cover all the types of communication with which we deal in this paper.

1.24 The term "cyber-bullying" is also increasingly used to describe a range of abusive or harmful electronic communications. In the offline world, "bullying" usually implies a repeated behaviour carried out in the context of adolescent peer relationships. An implied power imbalance exists between aggressor and victim. However the term cyber-bullying is often applied more loosely to encompass all forms of electronically communicated abuse, whether one-off or persistent.

1.25 In this report we reserve the term cyber-bullying to describe the range of intentionally harmful communications which occur within the context of adolescent relationships.

1.26 The concept of harm is also pivotal to this report. In the context of this report we use the term "harmful" to describe the full range of serious negative consequences which can result from offensive communication including physical fear, humiliation, mental and emotional distress.

1.27 Not all harms arising from communications are proscribed by law. The criminal law has typically been concerned with protecting citizens from communication harms which invoke fear for physical consequences, either personal or proprietary, or which are obscene or harmful to children. The civil law, in the past, also typically shied away from protecting emotional harm as such. However, as we demonstrate later, in both civil and criminal spheres the law has been moving towards recognition and protection of that sort of harm. We recognise that within the community at large and within younger demographics particularly, the threshold for when a communication causes the level of distress that can be described as "harmful" and when it simply causes annoyance or irritation may sometimes raise difficult issues at the margins. But we have reached the view that when the level of emotional distress can be described as significant the law has a role to play.

1.28 Finally, this report makes frequent reference to the various private businesses which provide the interface between users and much of cyberspace. These businesses perform a wide variety of functions and services including: platforms and tools which enable users to create, publish and share their own content (user-generated content); search

24 *Morse v Police* [2012] 2 NZLR 1 (SC).

25 *Police v Geiringer* (1990-1992) 1 NZBORR 331. See however the comment by Paul Rishworth and others *The New Zealand Bill of Rights* (Oxford University Press, Melbourne, 2003) at 313.

tools, web browsers and applications which provide an interface with the internet, and connectivity services which provide access. Throughout this report we use the generic term internet "intermediaries" and "content hosts" to describe these entities which typically do not themselves create content. In some contexts we refer more precisely to "internet service providers" (ISPs) when we are referring specifically to the simple function of providing internet connectivity. However it should be noted that many internet businesses provide a mix of services: for example many telecommunication companies not only provide connectivity but have also entered into agreements with media companies to provide content. Similarly a community of bloggers operating their own website will often be both content creators, and "hosts" to the content provided by their community of contributors.

1.29 It should also be noted that these entities vary enormously in their size, sophistication, and the degree of control they exert over their users. These distinctions can be important when considering what role these various entities should play in monitoring and enforcing the domestic laws to which those who use their services are subject.

THE PRINCIPLES UNDERPINNING OUR RECOMMENDATIONS

1.30 The package of reforms we recommend in this report are underpinned by the following principles and premises.

The role of the law

1.31 The law has a vital role to play in civil society. It embodies our common values and defines the behaviours we regard as acceptable and unacceptable. However in a democratic society people's freedom should only be limited to the extent necessary to protect others from harm. This principle is of vital importance when considering laws which constrain people's right to freedom of expression, a fundamental human right upon which all other rights depend.

1.32 However no rights are absolute. In any civil society a balancing of rights will sometimes be required in order to protect other important interests such as the right to a fair trial, the right to privacy, and the right to protect one's reputation. The New Zealand Bill of Rights Act 1990 requires that the rights protected in that Act, including freedom of expression, "may be subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."[26]

26 New Zealand Bill of Rights Act 1990, s 5.

1.33 Precisely where the law sets those limits is a reflection of our core values as a society, including what value we place on tolerance, civility and inclusivity. As discussed earlier, technology itself plays a critical role in shaping – and challenging – our values and our concept of what is acceptable behaviour. This dynamic relationship between technology and social values has always been reflected in the law and lies at the heart of this current debate about how we respond to digital communication harms.

1.34 While the law has an important role to play in anchoring and reinforcing socially acceptable behaviour, it must be acknowledged that laws targeting harmful communication can only go so far. Harmful communication is often part of a wider pattern of aggressive behaviour, in both the adult and young person contexts. That wider pattern may require a range of solutions, both legal and non-legal. But the law has an important part to play as one of the tools.

The law, technology & harm

1.35 In principle, laws should reflect broad principles which are capable of being applied in a technology-neutral manner. On one level the abuse of new communication technologies to cause intentional harm to another can be seen as an extension of offline behaviours. However this is too simplistic. For the first time in history, individuals with access to basic technology can now publish, anonymously, and with apparent impunity, to a potentially mass audience. This facility to generate, manipulate and disseminate digital information which can be accessed instantaneously and continuously is producing types of abuse which have no precedent or equivalent in the pre-digital world.

1.36 In our view the resulting emotional harms that can arise from the misuse of digital communication technologies are of such a serious nature as to justify a legal response.

1.37 For reasons of principle and practicality, recourse to the law should be the last resort reserved for those who have suffered serious harm. We endorse the views expressed by Google and Facebook in their submissions that user empowerment, digital citizenship and self-regulatory solutions must be the first line of defence in tackling harmful communication in cyberspace. [27]

27 In its submission Facebook described the concept of "digital citizenship" in the following terms:

"Digital citizenship typically describes the rights – and also the responsibilities – that each of us has in the online world, similar to the rights and responsibilities enjoyed offline. This can include, for example, the right to own information that we create online, and to represent ourselves accurately to the audience of our choice. It also includes the responsibility to treat others as we want to be treated, to respect people's

1.38 However we also believe that there are significant power and information asymmetries in cyberspace which mean not all are able to harness these new technologies to defend themselves from illegitimate attack.

1.39 Self-regulatory systems and tools are also highly variable across the internet. When they are absent or ineffective, citizens who have suffered serious harm should, in our view, have a right to access effective legal remedies. These remedies must be proportionate, and provide meaningful solutions.

1.40 Ensuring that the law is fit for purpose in the digital age is only one part of our challenge. To be useful, the law must also be understood, and accessible to citizens.

1.41 Given the fundamental importance of cyberspace and communication technologies we do not, in principle, support remedies which depend on terminating citizens' access to the internet. However, we note that many of the private businesses providing access and services reserve the right to de-activate accounts for non-compliance with terms of use contracts.

The need for a collaborative approach

1.42 As a matter of principle the target of any criminal or remedial actions must be focused on the author of the offending communication, rather than the entities providing access, publishing platforms and services – so called internet intermediaries.

1.43 However, creating a civil cyberspace will require the active collaboration of users, educators, parents, and those global internet and telecommunications businesses whose profitability depends on the billions of people engaging online.

1.44 Finally, it is vital that policy or legal responses to a phenomenon such as cyber-bullying are not rooted in a defensive or reactionary response to new technology. This technology is enabling young people to connect, relate and access information in ways that were hitherto unimaginable. The challenge we face is how to create a digitally responsible citizenry – not how to "control" or artificially constrain that technology or people's access to it.

digital space, and to stand up for others online."

Chapter 2: Understanding harmful digital communication

INTRODUCTION

Context

2.1 The number of citizens using digital communication technologies and participating in networked public spheres such as Twitter and Facebook is growing exponentially. More than 90 per cent of New Zealanders in the 15-49 age group are mobile phones users and in May 2011, 1.9 million New Zealanders had active internet connections via mobile phones.[28] A survey of New Zealand secondary school students carried out in 2011 found that 65 per cent of pupils had a Facebook account.[29]

2.2 In our Issues Paper, *The News Media Meets 'New Media': Rights, Responsibilities and Regulation In The Digital Age* we described how this digital revolution has placed the tools of mass publishing in the hands of every citizen with access to the internet.[30] It has brought incalculable benefits to society and transformed nearly every facet of life. However, it has also created novel ways in which people can use technology to harm others – instances of which are reported around the world on a daily basis.[31]

2.3 Securing cyberspace from a range of threats is a priority for governments all over the

28 Statistics New Zealand "Internet Service Provider Survey: 2011" (press release, 14 October 2011); *Household Use of Information and Communication Technology: 2009* <www.stats.govt.nz/browse_for_stats/industry_sectors/information_technology_and_communications/hhold-use-of-ict/household-ict-2009-tables.aspx>.

29 CensusAtSchool NZ is a voluntary online survey of New Zealand students in Years 5 – 13. The survey is a joint venture between Statistics New Zealand, the University of Auckland and the Ministry of Education. The 2011 census results were based on surveys of 24,941 students. <www.censusatschool.org.nz/about/>.

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

31 See for example BBC News "Rutgers webcam spy Dharun Ravi sentenced to 30 days" (online ed, 21 May 2012) at <www.bbc.co.uk/news/world-us-canada-18149395> and Sarah O'Meara "Internet Trolls Up Their Harassment Game With 'Beat Up Anita Sarkeesian'" The Huffington Post (6 July 2012) at <www.huffingtonpost.co.uk/2012/07/06/internet-trolls-online-beat-up-anita-sarkeesian-game_n_1653473.html>; "Parent outrage at Facebook bullying" The Gisborne Herald (reproduced on nzherald, online ed, 5 May 2012).

world, including our own.[32] In its latest survey, global security company Symantec assessed that cyber-crime, including financial scams and fraudulent transactions using stolen identities, cost New Zealand an estimated $625 million in 2011.[33]

2.4 Although these global reports do include some indicators of social harms online, to date there has been less emphasis on measuring the economic and psycho-social impacts of harms resulting from the misuse of digital communications technologies such as attacks on reputation, malicious impersonation, sexual and racial harassment, and invasions of privacy.

2.5 Global internet companies such as Google and Facebook provide users with tools to report content which is offensive and which breaks their terms of use. However as yet there is no independent means of assessing how frequently these tools are used and to what effect.[34]

2.6 The lack of consistent measurement and reporting of incidents involving communication abuses presents a challenge for policy makers and indeed we make recommendations later in this report about the need for better data collection in this area by Police and schools.

2.7 In response to this paucity of data the Law Commission requested an independent market research company to undertake research into New Zealanders' perceptions of a number of issues relating to the media and the internet. We summarise the findings in relation to harmful digital communication in the following discussion.

2.8 We also draw heavily on submissions and in particular the assessment of organisations such as NetSafe and the Police who are often contacted by those experiencing significant cyber-related harms.[35]

---

32 For example in 2011 the Ministry of Economic Development created a multifaceted Cybersecurity Strategy for New Zealand. For details refer <www.med.govt.nz/sectors-industries/technology-communication/cyber-security >.

33 Computer security company Symantec has published a number of surveys on cybercrime based on interviews with 20,000 adults in 24 countries including New Zealand. The 2011 Norton Cyber Report estimated that cybercrime, which included financial scams, viruses and malware as well as identity theft and harassment cost New Zealanders NZ$625.5 million in 2010-2011.

34 Google publishes a six-monthly "Transparency Report" documenting the number of government or court initiated requests it has received to either remove content associated with one of its products or services or to reveal information about a user. However these reports to do not extend to the use of community reporting tools to flag content or the amount of content removed as a result of such community reporting.

35 NetSafe was established in 1998 as an independent non-profit organisation committed to improving community understanding of the internet and how to enhance safety and security online. It works with a

2.9 In the following discussion we set out our findings based on these various sources of information and address the following critical questions:

- What differentiates digital communication and how do these differences affect the nature and severity of harms associated with speech abuses?
- How serious is the problem – and in particular, how is it impacting on vulnerable sections of the population, especially the young?

2.10 Throughout this discussion we use the general term "harmful digital communication" to cover the spectrum of behaviours involving the use of digital technology to intentionally threaten, humiliate, denigrate, harass, stigmatise or otherwise cause harm to another person. We reserve the term cyber-bullying for such abuses which occur within the context of adolescent peer relationships.

THE PREVALENCE OF DIGITAL COMMUNICATION HARMS

General population

2.11 Submissions to our review revealed a spectrum of opinion about the size and significance of the problem. These views often reflected the submitter's organisational perspective. At one end of the spectrum, Google argued that the Commission had failed to demonstrate that there was any pressing problem that were not being adequately dealt with either by the self-regulatory tools available on the internet, or, in the case of significant harms, by the existing laws such as privacy, defamation and contempt.[36]

2.12 At the other end of the spectrum, NetSafe, Police and the Post Primary Teachers' Association (PPTA) argued that the problem was significant and growing. Police submitted that "existing and potential harms to the public from speech abuses are significant" and although unable to provide quantitative data, staff were dealing with a "growing number of complaints from members of the public who have been intimidated, bullied, harassed and threatened on the Internet." [37]

range of governmental and non-governmental organisations including its core strategic partners, the Ministry of Education, the Ministry of Economic Development and InternetNZ, a non-profit open membership organisation whose aim is to promote and protect the internet in New Zealand.

36 Submission of Google New Zealand Ltd (14 March 2012) at 3.

37 Submission of New Zealand Police (March 2012) at 3. Submission of the Post Primary Teachers' Association (March 2012) at [2.1].

2.13 In June 2012 the *Otago Daily Times* reported that Police in Oamaru and Dunedin were dealing with complaints from the public relating to threatening and offensive text messages on a daily basis. According to Police the content of the texts ranged from "ambiguous threats to threatening to kill, commit suicide and text messages which breached protection orders".[38]

2.14 The PPTA submitted that cyber-bullying was a serious problem which occupied the "blurred space between home and school" making it unclear whose responsibility it was to respond. The effects it argued were very serious:[39]

> Cyber-bullying is implicated in truancy, may lead to suspension when the victim reacts to it in the non-virtual world and most tragically, to suicide.

2.15 NetSafe, which has collaborated with a number of government agencies including Police, and Internal Affairs, to provide a channel for reporting serious cyber offending, estimated that on average its support staff were assisting 75 people each month who were dealing with various forms of electronic harassment or abuse.[40] Of these 75 complaints, NetSafe estimated approximately half would typically relate to serious harassment or other online abuse being experienced by an adult, and half would involve various forms of cyber-bullying or harassment involving adolescents.

2.16 NetSafe tells us that the majority of those who utilise their services have either been directed to them by schools or the Police and have often exhausted other avenues of complaint. In its submission NetSafe noted that "the distress of those contacting our service is often painfully apparent. The majority of adult targets contact us after being threatened with physical harm."[41]

2.17 It seems plausible to assume that both the Police and NetSafe are dealing with some of the more extreme and persistent cases involving serious harm. However not all those experiencing harms will either know of the existence of NetSafe or will feel motivated or empowered to complain. Without any centralised reporting system it is difficult to gauge the size of this larger pool experiencing harms.

2.18 However there are a number of indicators which suggest the problem is not insignificant. For example a survey of 13,713 New Zealand households carried out by Statistics New Zealand between October 2009 and January 2010 found that seven per

38 Andrew Ashton "Police want culprits to get message on text bullying" Otago Daily Times (online ed, 10 June 2012).

39 Submission of the Post Primary Teachers' Association (March 2012) at [2.1].

40 Submission of NetSafe (24 February 2012) at 1.

41 Ibid.

cent of 15-19 year olds and five per cent of 20-29 year-olds had received harassing or threatening messages via their mobile phones in the preceding 12 months and similar percentages had been the victim of personally targeted online harassment.[42] Approximately half of those in the 15-29 year-old age group who had experienced harassment were sufficiently concerned to report the incident.

2.19 Vodafone New Zealand told us that since November 2010 over 60,000 account holders have made use of the text and pxt blocking facility which the company launched to assist customers to combat mobile bullying and harassment.[43]

2.20 To further assist us in assessing the scope of the problem we commissioned independent research company Big Picture to undertake research into a number of critical issues under consideration as part of the review.[44]

2.21 The research targeted a representative sample of 750 New Zealanders aged 18-70 and was conducted via an online survey comprising a combination of structured and open-ended questions completed between 15 and 22 March 2012.

2.22 In line with our terms of reference, the research had a split focus: part one of the survey inquired into public perceptions of news media standards, accountabilities and complaints bodies while part two focused on the internet and people's experiences of speech harms in the digital environment.

2.23 The research found that one in ten (10 per cent) of the total sample reported that they had "personal experience of harmful speech on the internet." (Survey participants were told examples of harmful speech might include things like cyber-bullying and harassment, harm to reputation or invasion of privacy.) However this jumped to nearly a quarter (22 per cent) of 18-29 year-olds, who are much higher users of social media. Maori and Pacific Islanders and those not in paid employment also reported higher

---

42 Statistics New Zealand *"Household use of Information and Communication Technology: 2009"* <www.stats.govt.nz/browse_for_stats/industry_sectors/information_technology_and_communications/hhold-use-of-ict-info-releases.aspx>.

43 In addition Vodafone told us that between March 2010 – March 2012, the company issued warnings to 5,250 customers as a result of using their phones in abusive or illegal way. Vodafone's mobile terms and conditions include an agreement "not to use your Mobile Device or the Services for an abusive, illegal or fraudulent purpose." Persistent offenders can also have their ability to text deactivated for a specified period or in extreme cases have their account deactivated.

44 Under s 6(2)(b) of the Law Commission Act 1985 the Commission is mandated to "initiate, sponsor, and carry out such studies and research as it thinks expedient for the proper discharge of its functions." Big Picture is an independent market research company based in Auckland. <www.bigpicture.co.nz/home>.

rates at 19 and 17 per cent respectively.

2.24 Researchers also attempted to gauge the extent to which participants regarded harmful speech online such as cyber-bullying, harassment, and reputational damage as a problem. Of the total sample 59 per cent said they were either "extremely concerned" or "concerned" and a further 25 per cent were "mildly concerned". Although 54 per cent of 18-29 year-olds said they were concerned about online speech harms, only 11 per cent rated themselves as "extremely concerned" compared with 20 per cent of the total sample. It appears that although younger people experience online speech harms more frequently, they are less concerned by it.

2.25 A higher proportion of Maori and Pacific Island respondents reported they were "extremely concerned" about harmful speech than the general population (32 per cent compared with 20 per cent of the total sample).

2.26 Significantly, when asked where they would go if they experienced "a serious problem with harmful speech on the internet" two fifths (42 per cent) of participants that responded said they did not know. A further 20 per cent said they would go to the Police and 17 per cent to the website's own complaints system.

2.27 While this research involved a relatively small sample and in some cases required respondents to grapple with unfamiliar concepts, it does seem to indicate that there is an emerging awareness and experience of online speech harms within the general population and within the younger demographic particularly.

Adolescents

2.28 NetSafe estimates that 1 in 5 New Zealand high school students experienced some form of cyber-bullying or harassment in 2007. This estimate is based on research undertaken by NetSafe's former Research Manager, Dr John Fenaughty, in conjunction with the University of Auckland. The research, conducted between 2007-2011, involved surveying and interviewing around 1,700 New Zealand secondary school students about how frequently they encountered – and how successfully they dealt with – a range of different cyber "challenges" or risks.[45] These challenges included cyber-bullying and harassment, unwanted sexual solicitation and unwanted exposure to inappropriate content of both a sexual and non-sexual matter. Study participants were asked "In the past year has someone ever tried to use a mobile phone

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

or the internet to bully or to be mean and hurtful to you?" Most interpreted cyber-bullying or harassment as meaning "the transmission of mean and hurtful communications and content to someone online or on-mobile." This might directly target an individual, such as text bullying, or involve indirect/relational aggression, such as spreading malicious rumours via social networking sites.

2.29 A third of those surveyed reported at least one experience of electronic bullying or harassment in the past year. Of these, 24 per cent reported that the bullying was via mobile phones and 17.5 per cent via the internet. The highest incidence of cyber-bullying was reported among 15-19 year-old females, at 36.9 per cent. Just under a third (29.3 per cent) of the total sample had been exposed to unwanted sexual content and 18 per cent had experienced unwanted sexual solicitation.

2.30 One of the challenges for researchers is understanding how such incidents actually affect young people given the changing norms in cyberspace. For example, content which adults might find highly insulting or offensive may be considered neither in the context of a text exchange between peers.

2.31 For this reason Fenaughty did not assume that every challenging incident online resulted in harm but rather explored the extent to which adolescents were distressed by the various cyber challenges. Significantly, he found around half of those who had experienced some form of cyber-bullying in the previous year reported a level of distress associated with the event. In terms of the percentage reporting distress associated with the range of different risks encountered by the group, cyber-bullying rated second only to unwanted exposure to inappropriate content such as violent or gruesome images.

2.32 A number of other studies have been carried out examining the incidence of various forms of digital abuse, including text bullying, among New Zealand secondary school students. These include a 2006 survey of 1,153 11-18 year-olds from two New Zealand secondary schools in which 41 per cent reported having been text bullied – half of these on a one-off basis and 14 per cent on a more persistent basis.[46]

2.33 Another study collected questionnaires from 3,400 year 9 and 10 secondary school students in the Tasman Police District in which 35.8 per cent of all students reported being subject to some form of cyber-bullying in the last year, and 18.5 per cent of all students reported subjecting another person to some form of cyber-bullying in the last

46 J Raskauskas and JE Prochnow "Text-Bullying in New Zealand: A Mobile Twist on Traditional Bullying" 16 New Zealand Annual Review of Education (2006) 89-104.

year.[47]

2.34 These rates were significantly lower, however, than rates of reported physical aggression. 68.3 per cent of participating students reported some form of physical aggression (the use of physical presence or indirect bodily force towards another person or their personal possessions to intentionally cause harassment, intimidation, humiliation or provocation) against them in the last year. Even higher were reported rates of relational aggression (receiving behaviour from their peers that involved disparaging and manipulating actions, embarrassing comments and disclosures, exclusion and indirect harassment) with 90.8 per cent of students reporting some form of this being used against them in the past year.[48]

2.35 Last year's report on improving outcomes for New Zealand adolescents by the Prime Minister's Chief Science Advisor noted that although the data was unclear it was likely that at least 15 per cent of New Zealand adolescents have been victims of text or online bullying of some sort.[49] Within this definition it included "behaviours such as spreading rumours about the target, sending threatening messages, posting photographs or videos online to embarrass the target, and posting content (e.g. through Facebook or on a blog) to damage the reputation or friendships of a targeted individual."

2.36 Prevalence studies from around the world have produced divergent results reflecting different sample sizes and methodologies, different definitions of cyber-bullying and digital harassment and the different access young people have to the various cyber platforms and technologies.

2.37 For example, in Britain a recent survey of 4,605 11 to 16-year-olds found 28 per cent had experienced some form of cyber-bullying.[50] For a quarter of these the electronic

---

47 Dr Donna Swift *The Girls' Project. Girl Fighting: An investigation of young women's violent and anti-social behaviour* (Stopping Violence Services, Nelson, 2011) at 25.

48 A definition of relational aggression cited by Swift at 18 is "negative social behaviours that are intended to harm relationships, social roles and/or social standing": R Pronk and M Zimmer-Gembeck "It's "mean" but what does it mean to adolescents? Relational aggression described by victims, aggressors and their peers" 25(2) Journal of Adolescent Research (2010) 175 – 204.

49 A report from the Prime Minister's Chief Science Advisor *Improving the Transition: Reducing Social and Psychological Morbidity During Adolescence* (Office of the Prime Minister's Science Advisory Committee, May 2011) at 124 [3.2.1] "PMCSA Report".

50 Emma-Jane Cross and others *Virtual Violence II: Progress and Challenges in the Fight against Cyberbullying* (A report commissioned by Nominet Trust in association with the National Association for Head Teachers, London, 2012) at 6 <www.beatbullying.org.pdfs/Virtual-violence-II.pdf>.

harassment was sustained over a period of time.

2.38 A 2009 report on the prevalence of covert bullying, including cyber-bullying, among Australian students found that 7.8 per cent of 12-15 year olds reported frequent (every few weeks or more) experiences of online or mobile bullying.[51] Behaviours classified as cyber-bullying included "threatening emails", "nasty messages or prank calls", someone sending or posting "mean or nasty" comments or pictures, someone "pretending to be them to hurt others" or being "deliberately ignored or left out of things on the Internet."

2.39 As we discuss later in this chapter, in May 2012 New Zealand's Chief Coroner, Judge Neil MacLean, expressed concern about the emergence of cyber-bullying as a background factor contributing to the high rates of suicide and self-harm among adolescents in this country.

WHAT IS DIFFERENT ABOUT DIGITAL COMMUNICATION?

> As a person who has been subjected to death threats and other bullying over the internet, I know how serious these are. During that period, I felt nervous leaving my house, and did not feel safe walking along the streets. The language used stigmatised me, and it affected my self-esteem, and my mood. This was in the form of e-mails sent to my work, e-mail sent to me through academia.org, and a page set up on Facebook, specifically for abusing me.

2.40 This submitter to our review conveyed in matter-of-fact terms how modern communication technologies can be employed on multiple fronts to besiege an individual. Not only did the threats undermine this man's physical sense of safety but they also invaded his professional relationships and spilled over into social media via Facebook. Other submitters described the loss of their reputations and unravelling of their lives as a consequence of the viral nature of harassment campaigns conducted via the internet. One described how defamatory and false information disseminated via Twitter by an acquaintance using an pseudonym effectively infected their identity:[52]

> This material is available to anyone who 'Googles' my name i.e. potential employers, work colleagues, customers etc. The nature of the comments is very humiliating and damaging to my reputation.

2.41 For those unfamiliar with the power of modern communication technologies it is sometimes difficult to fully appreciate the ways in which it can be subverted. Nor is it possible to appreciate the extent to which young people's lives are enmeshed in social

51 D Cross and others *Australian Covert Bullying Prevalence Study* (Child Health Promotion Research Centre, Edith Cowan University, Perth 2009).

52 Submitter's name withheld (submission dated 12 March 2012).

media. These two factors together are critical to understanding the ways in which digital communication can damage in ways which find no real parallel in the pre-digital world.

2.42 These differences arise from the nature of the technology itself and how it is shaping our communication culture. When misused, the technology can exacerbate the harms associated with abusive communication in a number of important ways:

(a) Perpetrators can be anonymous or adopt multiple online personae and construct fake profiles as a platform to attack others. The ability to send anonymous texts and comment anonymously may have a disinhibiting effect on the communicator, disconnecting them from their victim and the consequences of their actions; while from the vistim's perspective, the anonymity of the abuser can exacerbate the victim's sense of powerlessness;

(b) In the past a person's home life was to some extent insulated from workplace or school-based bullying. Now mobile phones and the internet mean the harassment can penetrate all aspects of the victim's life. Given the ubiquity of technology and the extent to which it is enmeshed in our everyday lives, it is not possible to simply "walk away" or disengage from cyberspace;

(c) The viral nature of the internet and digital communication can magnify the impacts of bullying by creating potentially large "audiences" of bystanders and/or recruiting peers to participate in the bullying activity. Bystanders may experience significant trauma simply from witnessing harassment;

(d) The permanence of digital information and searchability of the web means damaging content can survive long after the event and can be used to re-victimise the target each time it is accessed. The potential for cached material to be "re-discovered" long after it was initially posted can exacerbate the harms as the target may be uncertain how widely the content has spread and who has seen it.

2.43 Mobile phones, which for the young are now as basic a tool as a pen, are now capable of being used to record and distribute photographs and short video clips. Even amateur users can upload such audio-visual content to social media sites, making them available to potentially large audiences instantaneously.

2.44 In the course of his practice at NetSafe, Dr John Fenaughty explained he had encountered examples of young people being sent threatening text messages accompanied by disturbing images of dead or mutilated bodies, thereby increasing the distress associated with the words. In other instances, images of the victim may be

manipulated in degrading or threatening ways and distributed among peer groups with the intention of humiliating the target. Intimate photographs may be used in a similar way to stigmatise and humiliate another person

2.45 For young people the distress associated with the possession and dissemination of intimate photographs and video recordings can be particularly acute. This was graphically demonstrated in the 2010 case of a 16-year-old Christchurch student who was forced to relocate schools and cities after two male acquaintances coerced her, while drunk, into performing various sexual acts which they recorded on a cell phone.

2.46 In May 2012 the now 21-year-old ring leader was sentenced to 12 months jail after a jury found him guilty of making and possessing an indecent publication the content of which the Judge described during sentencing as "disturbing and harrowing." In a Victim Impact Statement the young woman provided a compelling account of how online and offline bullying and abuse engulfed her as knowledge of the existence of the video became commonplace around her school community and on Facebook:

> In less than a day after it happened, I started getting more abuse at school, people started calling me XXXX XXXX, slut and I was being humiliated in front of the class and the kids at school, it got so bad that I could not stay in class and I could not walk around at lunch time without being abused. The kids were saying I've seen your video and there was stuff on Facebook about it, apparently X and X wrote a synopsis about what happened. I heard that X connected his phone to his big TV and showed the video…

2.47 The Judge also pointed out that the fact these images were stored on the offender's cell phone and shown to others, and that the existence of these images became widely known among the young girl's school and community exacerbated the impact on the victim:[53]

> Someone published details on Facebook, and she was instantly notorious. The evidence does not establish whether it was the footage, or an account of the incident that was published. The victim's parents disowned her. She was held up to public ridicule. She had no option but to leave her school and community. She made several suicide attempts. She is now living with another family in a different community and trying to get her life back on track.

2.48 Although it was unclear from the evidence how widely the video had been viewed, the fact that the images had been stored on the perpetrator's phone meant there remained the potential for them to be shown at any time and for them to re-emerge in the future.

2.49 This point was emphasised by a Sydney magistrate in April this year during the trial of a 20-year-old man who had placed nude photographs of his girlfriend on Facebook in an act of revenge after their relationship ended. In sentencing the man to six months'

53 *R v Broekman* DC Christchurch CRI-2011-061-000199, 3 April 2012.

jail the Magistrate drew attention to the "incalculable damage" that can be done to a person's reputation by the irresponsible posting of information in such places as Facebook:[54]

> The harm to the victim is not difficult to contemplate: embarrassment, humiliation and anxiety at not only the viewing the images by who people who are known to her but also the prospect of viewing by those who are not. It can only be a matter of speculation as to who else may have seen the images and whether those images have been in stored in such a manner which, at a time the complainant least expects, they will again be available for viewing, circulation or distribution.

2.50 This case was reported to be the first instance in Australian history in which a person was jailed for uploading intimate photos in social media. It mirrors the case of a 20-year-old New Zealand man who received a four month jail sentence in 2010 for a similar offence.[55] Similarly in May 2012 police successfully prosecuted a 22-year-old Christchurch man under a little used provision of the Telecommunications Act after he sent a text to a woman threatening to place naked photos of her on Facebook.[56]

2.51 The facility to manipulate digital images also creates new ways of inflicting emotional harm on others, as NetSafe pointed out in its submission:[57]

> Manipulation of digital images has been used to create seemingly offensive situations that are entirely fictional. NetSafe is aware of local instances where the publication of sensitive images of targets of such harassment has been associated with suicidal behaviour and ideation.

2.52 A notorious example of this type of malicious manipulation of digital images came to public attention in the Britain in September 2011 after a 25-year-old English man was jailed for posting fictional videos and mocking messages relating to the deaths of a number of teenagers, including one who had been hit by a train. As well as posting taunting and highly offensive messages on the teenagers' Facebook memorial pages Sean Duffy also created a YouTube video called "Tasha the Tank Engine" featuring the dead girl's face superimposed onto the front of a fictional train engine.[58]

2.53 While such an extreme example of malicious use of communications technology has not been reported in New Zealand, Police did refer us to instances where they had

---

54 Heath Aston "Ex-lover punished for Facebook revenge" *Sydney Morning Herald* (reproduced on Stuff, New Zealand, 23 April 2012).

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

56 David Clarkson "Man in court over naked pic threats" (31 May 2012) < www.stuff.co.nz >.

57 Submission of NetSafe (24 February 2012) at 1.

58 See "Internet Troll Jailed After Mocking Teenagers" *The Guardian* (online ed, 13 September 2011) <www.guardian.co.uk/uk/2011/sep/13/internet-troll-jailed-mocking-teenagers>. The defendant was charged with two counts under the Communications Act 2003 (UK) – <www.thelawpages.com/court-cases/Sean-Duffy-7443-1.law>. For the relevant offence (s 127), see chapter 4 at [4.74].

intervened after peers of suicide victims had posted offensive and denigrating messages on memorial pages created for the deceased.[59]

2.54 Later in this report we consider whether such behaviour should be criminal in New Zealand.

2.55 It is also a relatively simple matter to create false profiles and accounts on the web and this is an increasingly common form of harassment used by those wishing to inflict harm on someone with whom they have some form of relationship.

2.56 In our Issues Paper we gave a number of examples of such harassment by impersonation, including that of a South Island secondary school teacher who battled unsuccessfully for more than a year to have a false Facebook page containing lewd comments removed from the site. Another recent example of malicious impersonation involved a professional woman whose job required her to maintain a strong online profile but who found her profile had been linked to a pornography site in such a way that when her name was "googled" it was indexed to an item which said "Hottest Whore" and sent searchers directly to the pornographic site. This had caused immense distress to the woman and her family. Currently there is no offence directly applicable to this type of behaviour.

2.57 In another American case, a man whose advances had been rebuffed by a female acquaintance set up bogus accounts in her name and impersonated her in online chat rooms and email, suggesting she fantasised about being raped. He published her physical address and phone numbers, including details about her home security system. On at least six occasions men arrived at the woman's door in response to the supposed invitation to rape her.[60]

2.58 NetSafe also provided examples of threatening, abusive and malicious postings made using email, websites, forums, blogs and mobile telephones. Personal information obtained in one context could often be used to harass a person in numerous different ways, as illustrated by this complainant to NetSafe:

> someone is stalking me and my family. They are sending me mail in the post, they have got a phone sim and text….they got all my kids private info and are putting it up on fake Facebook pages, they

59 Law Commission *The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age* (NZLC IP27, 2011) at [7.2].

60 In April 1999 the offender pleaded guilty to three counts of solicitation for sexual assault and one count of stalking: Joanna Lee Mishler "Cyberstalking: Can Communication via the Internet Constitute a Credible Threat and Should an Internet Service Provider be Liable if it does?" (2000) 17 Computer and High Technology Law Journal, 115 at 116.

> have included my neighbour and old boss and a current colleague – it's sexually explicit and harassment and stalking. There have been threats but we have no idea who is doing it. …the police know but say there is nothing they can do to trace this person.

2.59 Variants of this type of behaviour have been reported around the world including the case of female students at Yale Law School who were eventually forced to sue those responsible for a sustained anonymous campaign of sexual harassment launched by a group of young males on the college admissions web forum.[61]

2.60 An article on the online site of Wired magazine backgrounding the events which gave rise to the damages lawsuit explained how harms caused by the original postings had been amplified by the web:[62]

> The Jane Doe plaintiffs contend that the postings about them became etched into the first page of search engine results on their names, costing them prestigious jobs, infecting their relationships with friends and family, and even forcing one to stop going to the gym for fear of stalkers.

2.61 The ease with which people can share content on the web and comment on other's posts also offers the potential for mob-like behaviour – the anonymity afforded posters often encouraging more extreme forms of abuse and minimising the chances of accountability.

2.62 This was illustrated in a recent British case in which a 45-year-old British woman became the target of what has been described in court as "vicious and depraved" abuse after posting supportive comments about an "X Factor" contestant on her Facebook page. Anonymous attackers responded by creating a false profile in her name using her picture to post explicit comments and vilifying her. In an interview with the Independent newspaper the woman explained how this seemingly trivial affair rapidly spiralled out of control:[63]

> At the time I thought of it as banter. But after a few days people started saying to me 'You're popping up all over the internet'. People were inciting hatred against me. They weren't just targeting me, they were also dragging young girls into it as well. They weren't playing.

2.63 In June 2012, in what has been hailed as a landmark case, the High Court granted the woman a disclosure order compelling Facebook to reveal the IP addresses and account details of those responsible for posting the offensive content.

---

61 Ryan Singel "Yale Students' Lawsuit Unmasks Anonymous Trolls, Opens Pandora's Box" *Wired* (Online ed, 30 July 2008) < www.wired.com >. For a full discussion of online harassment see for example Martha C Nussbaum "Objectification and Internet Misogyny" in Saul Levmore and Martha C Nussbaum (eds) *The Offensive Internet: privacy, speech and reputation* (Harvard University Press, 2010) at 68.

62 Ibid.

63 Terri Judd "Landmark ruling forces Facebook to drag cyberbullies into the open" *The Independent* (online ed, 9 June 2012).

HOW DOES CYBER-BULLYING DIFFER?

2.64 As we have discussed above, digital communication differs in significant ways from earlier forms of communication. The "text bomb" and the video clip of the school yard brawl that is viewed 32,000 times on YouTube within 24 hours have no precedents in the pre-digital era.

2.65 The authors of a recent Nova Scotia report on cyber-bullying nicely summarised the ways in which these new communication platforms and technologies have unlocked the potential of the bully:[64]

> Traditional bullying tends to take place in secluded places, like washrooms, hallways and school buses, where there is little adult supervision. The cyber-world provides bullies with a vast unsupervised public playground, which challenges our established methods of maintaining peace and order – it crosses jurisdictional boundaries, is open for use 24 hours a day, seven days a week, and does not require simultaneous interaction.

2.66 The authors note that while some young users simply do not comprehend the public nature, reach and longevity of their on-line communications, others exploit these characteristics to maximum effect.[65]

> The immediacy of online transactions encourages impulsive acts with no thought to the consequences, a behaviour pattern that is already common in many youth, and peer pressure may further promote harmful deeds that unfortunately have instant and powerful impact with no effective retraction possible.

2.67 A good example of this type of behaviour has been seen in New Zealand over the past 18 months with the emergence of anonymous Facebook pages where large numbers of students from one or more secondary schools participated in mob-like harassment of fellow students. The pages' administrators are typically anonymous and the pages are often used as a vehicle for spreading vicious and damaging allegations about other teenagers. As NetSafe has reported, in some cases these sites would attract hundreds of followers within the space of 24 hours and include highly offensive comments and claims about other students including denigrating their physical appearance and sexuality. Most recently the *New Zealand Herald* reported that a group of local mothers had complained to the police and alerted schools to an anonymous Facebook page containing threatening and damaging posts about local Gisborne teenagers.[66]

---

64 Report of the Nova Scotia Task Force on Bullying and Cyberbullying *Respectful and Responsible Relationships: There's No App for That* (Nova Scotia, 29 February 2012) at 12.

65 Ibid.

66 "Parent outrage at Facebook bullying" *New Zealand Herald* (online ed, New Zealand, 5 May 2012).

2.68 These sites illustrate how effectively social media can be used to intentionally harm others by damaging their peer relationships. Malicious rumours, often concerning a person's relationships or sexuality, whether true or false, can be spread virally and the anonymity encourages others to participate at least by reading the contents if not actively commenting. Individual teachers and schools have also been targeted.

2.69 Researchers point to such sites as examples of the ways in which bullying behaviour often occurs as part of complex social interactions between peer groups and needs to be understood in this relational context.

Impacts of cyber-bullying

2.70 The Australian Covert Bullying Prevalence Study noted that covert bullying, which goes unnoticed or unaddressed by adults, including cyber-bullying, presents particular risks to its victims and challenges for those attempting to prevent it:[67]

> …research into how to address covert bullying is still in its infancy. This is due in part to the erroneous perception that while covert bullying is unpleasant it is generally considered to be a less harmful form of behaviour. Emerging research indicates, however, that covet bullying has the potential to result in more severe psychological, social, and mental health problems than overt bullying, and is not only more difficult for parents and schools to detect, but also has the capacity to inflict social isolation on a much broader scale than overt bullying. Furthermore, the recent digital media revolution of the last decade has provided an additional platform and encouraged a communication culture within covert bullying can operate among young people.

2.71 To date there has been limited New Zealand research specifically on cyber-bullying harms. As discussed earlier, as part of his study of students' resilience in the new digital environment, Dr John Fenaughty sought information about the emotional/psychological impact various cyber challenges had on survey participants. Significantly, around half of those who had experienced some form of cyber-bullying in the previous year reported a level of distress associated with the event. In terms of the percentage reporting distress associated with cyber challenges, this rated second only to unwanted exposure to inappropriate content such as violent or gruesome images.

2.72 The most common strategies reported by those who had experienced distressing cyber-bullying were "ignoring the problem" (69.5 per cent); confrontation/fighting (51.2 per cent) peer support (29.6 per cent) technical solution (7.9 per cent). Just over half reported resolving the problem.

---

67 D Cross and others *Australian Covert Bullying Prevalence Study* (Child Health Promotion Research Centre, Edith Cowan University, Perth 2009) at 3.

The link between cyber-bullying, suicide and self-harm

2.73 In May 2012 New Zealand's Chief Coroner, Judge Neil MacLean, expressed concern about the emergence of bullying, and cyber-bullying in particular, as a "background factor" in New Zealand's high youth suicide rate. He also noted that bullying featured as one of the factors researchers found when investigating incidences of self-harm among adolescents.[68]

2.74 This was followed on June 1 by the release of Coroner Wallace Bain's findings in relation to the death in July 2009 of a 15-year-old North Island girl. The Coroner found that this teenager had died as a result of taking a fatal dose of her father's heart medication but that there was enough doubt about her actual intent to prevent him from reaching a finding of suicide. The Coroner concluded that the teen had taken the medication in response to the end of her relationship with the 27-year-old with whom she had been having an affair and that her actions, and subsequent communications, suggested this was a cry for help.

2.75 In his findings the Coroner drew attention to the impact on the teen of a series of highly abusive and threatening text messages written by her lover's wife in the days and hours leading up to her death. As part of his recommendations the Coroner called for stronger legal penalties for those who use new technologies to inflict emotional harm on others – particularly vulnerable young people.

2.76 As a society we are understandably disturbed by the possibility that the misuse of technology may now be playing a role in New Zealand's persistently high rates of youth suicide. However, it is also vital to consider this issue within the much broader context of adolescent mental health and well-being. New Zealand researchers have developed a clear understanding of the risk factors associated with suicide and self-harm in adolescents, and while exposure to bullying and other forms of aggression certainly features as a risk factor, it is only one strand in a complex picture.

2.77 In New Zealand to date there has been only a handful of cases where coroners have explicitly considered the role of technology in a young person's suicide. We reviewed the findings of five such inquests conducted between February 2006 and June 2011. The ages of the young people ranged between 12 and 17 years of age.[69]

---

68 Simon Collins and Vaimoana Tapaleao "Suicide link in cyber-bullying" *New Zealand Herald* (online ed, New Zealand, 7 May 2012).

69 One of the first cases to come to public attention involved the death of a 12-year-old Putaruru girl in February 2006. Although the coroner made no reference to bullying in his brief findings, it is apparent

2.78 In many respects an analysis of these cases illustrates the complexity of the underlying issues associated with youth suicide. In a few cases it is appears that bullying was a contributory factor and that the particular characteristics of digital communications which we discussed earlier – including the disinhibiting effects of texting and the "wrap-around" nature of digital interactions – may have amplified the emotional impact and harms.

2.79 However in other cases the role that digital technology may have played appears to be far more nuanced: for example, even when there was no evidence of malice or intention to harm the recipient, there was the suggestion that texting itself could result in distorted communication which could, in some contexts, have a far greater emotional impact than verbal or face-to-face communication. One coroner referred to the impact of a "texting frenzy"; another referred to the impact of a highly emotionally charged late night text exchange between a vulnerable young man and two young female friends where the possibility of one or more of their suicides was discussed.

2.80 But what is also abundantly clear from these cases, and the research literature, is that bullying is only one of a number of complex inter-related risk factors associated with suicide and its actual impact, like the impact of other stressors, will vary according to a range of variables including the person's emotional resilience, their home and school environment and any underlying personality or psychiatric disorders – most significantly, depression.

2.81 Alcohol and drug use in adolescents is also another very important risk factor. Both can reduce inhibitions and heighten the normal impulsivity associated with adolescents and may lead a vulnerable young person to respond catastrophically to a stressor such a relationship break-up, or physical or emotional conflict. So for example, an abusive anonymous text message or degrading comment left on a social media site may act as a trigger for self-harm or suicide in some contexts.

Contagion effect

2.82 As this discussion demonstrates, there are a number of novel ways in which digital

---

from the witness statement provided by the child's mother that her daughter had been subjected to a sustained period of bullying involving both texts and emails. It was also however apparent that the 12-year-old had been exposed to a number of suicide deaths within the close-knit community, including that of a cousin a matter of days earlier. In an interview with the *New Zealand Herald* the mother acknowledged that there were likely to be a number of factors contributing to her daughter's death but that the 'orchestrated campaign' of threatening and pejorative texts and emails had played a part.

communications technology can be used to cause emotional and mental harm to vulnerable adolescents. Bullying can create a downward spiral in a vulnerable young person's life, leading to social isolation and depression which in turn heightens the risk of suicide and self-harm.

2.83 Alongside these factors research also suggests that the networked world presents another challenge for those attempting to prevent suicide – the risks associated with the detailed discussion and glamorisation of suicide.

2.84 These issues were examined in depth by Otago University's Department of Preventive and Social Medicine as part of research into a suspected suicide cluster in a rural New Zealand community in 2006.[70]

2.85 Researchers noted that while the mainstream media had adhered scrupulously to suicide reporting guidelines and had avoided all references to the emergence of a cluster of suicides in the community, discussion of the events was rife within social media.

2.86 The researchers concluded that "in view of other evidence linking publicity and social modelling to suicide contagion" it was likely that the use of texting and social media to spread information (factual and false) about the suicides had "increased the risk of suicide contagion" in relation to these suicides. The posthumous popularity and glamorisation of those who had committed suicide added to this risk:

> Many of those who took their own lives in the cluster received attention and dedications from hundreds of other people via Bebo.com, which may have added further to the risk of contagion.

2.87 In their recommendations the researchers noted the importance of the early identification of an emerging suicide cluster to enable timely and co-ordinated intervention. To achieve this the researchers recommended that suspected youth suicides should be immediately notifable not just to coroners but to public health services.

2.88 They also recommended taking immediate action to try to mitigate potential sources of contagion – "including removal of Bebo or Facebook sites". They also noted that texting and social media was being harnessed by many youth counselling agencies to

70 Lindsay Robertson and others "An Adolescent Suicide Cluster and the Possible Role of Electronic Communication Technology" The Journal of Crisis Intervention and Suicide Prevention (Crisis) 2012; DOI: 10.1027/0227-5910/a000140. Investigators undertook a forensic examination of eight suicides that were either linked temporarily, geographically or through some other inter personal connection. Among the key issues they explored was whether, and in what ways, the use of modern communication technology such as texting and social media, had impacted on these events.

deliver appropriate services to the young. However they also advocated that suicide prevention agencies actively monitored social media sites in the wake of youth suicides to detect anything which may give rise for concern:

> Electronic communications provide valued links between young people, but they may also become a source of suicide contagion following a suicide. When this escapes the scrutiny of the adult community it may make it difficult to recognise a cluster as it is developing. A multidisciplinary approach to recognising and responding to a suicide cluster is essential.

2.89 This research and its conclusions underscore the complexity of the issues and the need for policy makers to understand not only the risks associated with new media, but also the ways in which social media and technologies such as texting can be *protective* – both as channels through which young people can seek help but also via which they can connect with their peers.

2.90 In chapter 6 of this report we provide an overview of the policies and programmes which have been developed to tackle bullying in schools and we make some recommendations about how the law and the existing anti-bullying strategies can best confront cyber-bullying.

SUMMARY AND CONCLUSIONS

2.91 This discussion points towards a number of conclusions. First, as noted in the introduction to this chapter, the major research focus with respect to cyber-crime has been in relation to financial and other security threats. However increasing concern about cyber-bullying in particular is producing a growing body of quantitative and qualitative research into the prevalence and impact of harmful digital communication.

2.92 Independent research we commissioned suggests that as many as one in ten New Zealanders has some personal experience of harmful communication on the internet. That rate more than doubles to 22 per cent among the 18-29 demographic who are the heaviest users of new media. These figures are broadly consistent with the academic literature although estimates vary depending on the different definitions, samples and methodologies used.

2.93 However, as we have noted earlier, robust communication is a hallmark of the internet and not everyone exposed to abusive or offensive communication will be harmed. It seems incontrovertible that technology is influencing how we communicate and relate socially and, as the early adopters of this technology, young people are both shaping and being shaped by these new ways of interacting digitally. Free speech values and an abhorrence of censorship are deeply embedded in the culture of the internet,

challenging traditional concepts of where the line should be drawn with respect to communication which in the past has been regarded as so abhorrent or damaging that it requires legal prohibition and punishment.

2.94 But even allowing for changing communication norms, research suggests that a significant proportion of adolescents exposed to cyber-bullying and harassment experience distress as a result.[71]

2.95 In addition it is evident from the submissions of Police and NetSafe that a growing number of New Zealanders are turning to these organisations for help after experiencing significant distress as a consequence of harmful direct and indirect digital communication. We understand from NetSafe that many of the 75 people who turn to them for assistance each month have been diverted by the Police and have already exhausted all other avenues of complaint. Given NetSafe's modest public profile and the challenges the Police face in pursuing many cyber-related communication offences, it seems reasonable to assume that there is significant under-reporting of digital communication offences.

2.96 Another important conclusion which emerges from this discussion relates to the *nature* of the harms which can arise from digitally mediated communication. On one level the abuse of new communication technologies to cause intentional harm to another can be seen as an extension of offline behaviours. However this is too simplistic. For the first time in history individuals with access to basic technology can now publish, anonymously, and with apparent impunity, to a potentially mass audience. This facility to generate, manipulate and disseminate digital information – which can be accessed instantaneously and continuously – is producing types of abuse which simply have no precedent or equivalent in the pre-digital world. In other words, ordinary citizens, with no specialist expertise or technical assistance can, in effect, cause irreparable harm to one another's reputations and inflict enduring psychological and emotional damage. Irrespective of the quantum of the problem, in our view, this potential to cause significant, and potentially devastating, harm demands an effective legal remedy.

2.97 Finally, with respect to adolescence, it seems unarguable that digital communication technology has allowed relational bullying and personal harassment to reach a scale and sophistication hitherto unimaginable. It is also unarguable that, for the same reasons as discussed above, the harms which may arise from this type of wrap-around

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

bullying and harassment have been exacerbated.

2.98 However, this same technology is also empowering young people, including those who might otherwise be marginalised, by providing powerful new ways through which they can connect and interact. It also enables young people to seek out help and to seek assurance in ways which are not dependent on the quality of their adult relationships.

2.99 The weight of international and New Zealand evidence supports the view that cyber-bullying should not be approached as a discrete practice but as a manifestation of intentionally harmful acts perpetrated and experienced by adolescents within the context of individual and peer relationships. However, it is critical that policy makers are alert to the very real differences between covert and overt forms of aggression, and in particular the unique challenges created by digitally mediated bullying and harassment, which crosses over the boundary between school and home life.

2.100 Similarly, it is important that the risks associated with bullying generally and cyber-bullying specifically, including the association with suicide, are understood within the wider broader context of adolescent health and wellbeing. In this respect the PMCSA report provides an invaluable resource for policy makers attempting to understand the complex personal, social and environmental factors which are contributing to a range of poor outcomes for New Zealand adolescents.

Chapter 3: User empowerment and self-regulation – is it enough ?

ISSUES PAPER

3.1 As Google pointed out in its submission to this review, "the mere existence of harmful speech is not sufficient to justify additional regulation. It is necessary to show that existing legal and self-regulatory remedies are ineffective".[72]

3.2 In chapter 7 of our Issues Paper we described the existing legal and non-legal remedies available to curb harmful communication.[73] These include a substantial body of statute and judge-made law and the various self-regulatory systems which operate within many of the networked public spheres on the internet itself.

3.3 We reached the following preliminary conclusions about the adequacy of these legal and non-legal remedies:

(a) While the existing criminal and civil law is capable of dealing with many of the communication harms we have described, our preliminary view was that the law was not always capable of addressing some of the new and potentially more damaging harms arising from the use of new technology.

(b) In addition there were a number of impediments to the successful application of the law with respect to harmful digital communication. These included a lack of knowledge of legal rights and responsibilities; difficulties accessing the law; difficulties enforcing the law as a result of inadequate investigative resources and tools and difficulties in obtaining evidence and identifying perpetrators.

(c) With respect to the self-regulatory tools that have evolved within cyberspace, we stated that a lack of robust data made it difficult to assess their effectiveness.

3.4 In this chapter we return to the issue of self-regulation and discuss the strengths and weaknesses of the current non-legislative solutions to harmful digital communication. In doing so we draw on what submitters told us about their experiences of using these systems to resolve problems and our own research findings.

72 Submission of Google New Zealand Ltd (14 March 2012) at 16.

73 Law Commission *The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age* (NZLC IP27, 2011) at 160.

THE ADEQUACY OF EXISTING SELF-REGULATORY SOLUTIONS

Who constrains communication in cyberspace?

3.5 As both Google and Facebook pointed out in their submissions, the amount of data shared on leading internet properties is mindboggling: every minute there are an estimated 60 hours of video uploaded to YouTube; every day on average 483 million people around the world actively engage on Facebook,[74] uploading on average more than 250 million photos; each week an estimated 1 billion tweets are sent by Twitter users.[75]

3.6 Trade Me, a minnow by Facebook standards, but with an even greater penetration in the New Zealand market, has 2.9 million members who, on average, will publish 20,000 new posts on Trade Me message boards each day.[76] At any given time there may be as many as 550 million words contained on these message boards.

3.7 Because participation in these networked spheres is free it is sometimes assumed that cyberspace is the equivalent of a digital "commons", where free speech is unfettered and the only rules that apply are those which participants make up themselves.

3.8 In fact most interactions in cyberspace depend on intermediaries which provide the platforms and services which allow us to publish and access content and interact with others. These include internet giants such as Google whose search technologies have become the portal through which a vast number of people interface with cyberspace. Countless businesses around the world provide technologies and platforms for the creation and hosting of user-generated content. And the telecommunication sector provides internet connectivity.

3.9 Preserving the internet from censorship and regulation is a core objective of many cyber-based businesses – an objective which can have both a commercial and ideological imperative. For example Google's mission is to "facilitate access to information for the entire world, and in every language." Censorship is incompatible with this aim.

3.10 However this does not mean that Google and other global internet intermediaries are operating outside the law. These companies, and the individuals using their services,

74 Submission of Facebook (14 March 2012) at 2.

75 Submission of Google New Zealand Ltd (14 March 2012) at 21.

76 Submission of Trade Me (12 March 2012) at 1.

are all subject to the laws and regulatory systems of the countries in which they are domiciled. The terms and conditions to which users agree when contracting to use services such as Twitter, Facebook, YouTube and Google make clear that users are responsible for their own behaviour on these sites, but that the sites themselves are subject to the law and require those who use them to respect these legal boundaries.

3.11 For example, Twitter makes it clear that while it accepts no responsibility for content distributed on its platform, it reserves the right to restrict content and to co-operate with enforcement agencies when its terms of use have been violated:[77]

> We reserve the right at all times (but will not have an obligation) to remove or refuse to distribute any Content on the Services, to suspend or terminate users, and to reclaim usernames without liability to you. We also reserve the right to access, read, preserve, and disclose any information as we reasonably believe is necessary to (i) satisfy any applicable law, regulation, legal process or governmental request, (ii) enforce the Terms, including investigation of potential violations hereof, (iii) detect, prevent, or otherwise address fraud, security or technical issues, (iv) respond to user support requests, or (v) protect the rights, property or safety of Twitter, its users and the public.

3.12 Not surprisingly, given their pivotal role at the interface between users and cyberspace, internet intermediaries find themselves at the centre of policy discussions about how to manage the competing interests of freedom of expression versus other human rights. And while these companies often stress their passive role as intermediaries, nonetheless they are increasingly forced to grapple with complex decisions about if and when to accede to requests to remove content, deactivate accounts or block access to sites.

3.13 In its submission to this review the Equal Justice Project drew attention to this "inherent tension between the need for corporate accountability and the right of private commercial sectors to self-regulate within the operation of the law."[78]

3.14 And as these submitters went on to point out, these tensions have taken on a whole new dimension as a result of mass participatory media sites like Facebook:[79]

> In 2011, the official user count for Facebook was reported to be a monumental 854 million (monthly users); more populated that the average nation-state, yet the entity is largely free to determine guidelines and balances considerations for multiple jurisdictions against its own (user) interests. This observation does not purport to be a pretext to suggest active online-forum or corporate regulation, yet it points to an eerie lack of uniformed regulatory governance for such online mediums.

---

77 Twitter: Restrictions on Content and Use of the Services available at <www.support.twitter.com/groups/33-report-abuse-or-policy-violations#topic_166 >.

78 Submission of the Human Rights division of the Equal Justice Project, Faculty of Law, University of Auckland (received 30 March 2012) at [3.1].

79 Ibid.

3.15 At the other end of the spectrum from such internet giants are the millions of bloggers and website administrators each with their own particular objectives and communities of interest. Participation in these communities will often involve adherence to some sort of rules or norms but these may be minimalist, or, in some instances non-existent.

3.16 In other words, just as with traditional media, there are the mainstream global entities, such as Google and Facebook, with strong commercial imperatives to invest in sophisticated self-regulatory systems and, alongside these, an almost infinite number of medium-sized and niche sites with an equally diverse approach to the question of user rights and responsibilities.

3.17 Given this diversity it is clear that people's experiences in cyberspace will vary greatly depending on the environments in which they spend their time and how they interact with others.

3.18 This idea that users make active choices about their engagement in cyberspace has important implications for policy makers when thinking about how to respond to problems like harmful communication. Unlike broadcast media which pushes content out to passive audiences, the web requires users' active participation to search out or "pull in" content and make choices about what they expose themselves to.

3.19 In its submission Google described how "internet users are now much more in control of the content they consume and have been given the tools to create, edit, mash-up, distribute, share and comment on content like never before."[80]

3.20 In Google's view this paradigm shift in how citizens use media has fundamental implications for how problems such as harmful content should be managed in the digital era:[81]

> [O]nline communities set, refine and enforce their own community standards. If content is made available that is considered to be unacceptable or offensive, users will protest and remedial action can be taken very quickly. Online businesses risk their livelihood if inappropriate content is repeatedly published as audiences and users will quickly switch to other sites.

3.21 Rather than resorting to legal solutions to tackle abuses of these powerful new communication technologies, both Google and Facebook emphasised the importance of "bottom-up" solutions which harness the power of users and technology.

3.22 In summary then, these corporations argue that policies directed at reducing the problem of harmful communication in cyberspace need to focus in the first instance on empowering users by educating them about their rights and responsibilities as "digital

80 Submission of Google New Zealand Ltd (14 March 2012) at 15.

81 Ibid.

citizens" and providing them with the technological tools to exercise these rights and responsibilities effectively. These strategies are reinforced by the "terms of use" agreements by which users are contractually bound to internet intermediaries and, ultimately, by the legal systems which apply to the users themselves and the content they create.

3.23 We have no argument with this approach and believe it is both consistent with the principles of free speech and reflects the practical realities of the new era of mass participatory media.

3.24 However, the question to which we now turn is whether in practice this combination of self-regulation underpinned by domestic law is in fact providing effective remedies for those who experience significant harms as a result of communication abuses. Specifically, we are interested in whether there is a gap between the reach of the self-regulatory systems on the web, and the reach of the law.

3.25 In the following discussion we do not pretend to provide an exhaustive answer to this question – as mentioned earlier, there are literally millions of different destinations in cyberspace and billions of users. Instead we report what our own research and submitters have told us about their experiences and views of the current systems and laws.

SELF-REGULATORY TOOLS

3.26 As we noted above, internet intermediaries and content hosts vary hugely in their size, complexity and sophistication, and their commitment to user rights and responsibilities.

3.27 In their submissions both Google and Facebook emphasised the commercial imperative of investing heavily in developing tools and systems which support user safety:[82]

> Providers want their brand associated with comfort, safety and security. Ultimately, it is imperative to a provider's bottom line to get this right. Otherwise users will switch to a different service. That is particularly true in the highly-competitive world of the web, where an alternative is only a click away.

3.28 As discussed, like many privately owned internet services Google (which owns YouTube) and Facebook rely on a combination of contractual "terms and conditions" and community moderation to establish and maintain civil behaviour on their sites.

3.29 Typically, users must register and agree to comply with the site's terms and conditions

82 Ibid, at 14.

before being able to make use of the site. As Facebook pointed out in its submission, those using its platform are governed by the company's Statement of Rights and Responsibilities, which prohibits the posting of content that "harasses, intimidates or threatens any person, or that is hateful or incites violence."[83] These are complemented by a set of Community Standards, designed to provide a more "user-friendly summary of the legal terms set out in the Statement of Rights and Responsibilities."

3.30 By default, other users of the site become the agents for policing compliance with these rules and standards. Users have access to various tools allowing them to "vote" content off and "report" content which transgresses the rules in some way. Facebook told us its system "leverages the 845 million people" who use its site to monitor and report offensive or potentially dangerous content. This community moderation was backed up by "a trained team of global reviewers who respond to reports and escalate them to law enforcement as needed."[84]

3.31 In addition Facebook detailed a range of other measures it takes to minimise abuses of the site and to support vulnerable users. These included:

(a) Facebook's 'authentic identity' culture which mitigates against "bad actors who generally do not like to use their real names or email addresses";

(b) Facebook's own automated systems for removing content that violates policies, including the deployment of technology specifically developed to detect child exploitative materials;

(c) Facebook's partnerships with suicide prevention agencies, including three in New Zealand, which aim to ensure vulnerable users have access to appropriate support;

(d) Facebook's special safety and privacy tools that have been developed in recognition of the special needs of adolescent users. These include privacy default settings for accounts of minors that ensure that they do not have public search (i.e. search engine) listings created for them, thereby reducing the visibility of minors on the web.

3.32 When users report content that is believed to be in breach of the law or of the site's own terms and conditions Facebook told us it was quick to respond including, when appropriate, taking "corrective action":[85]

> In serious or potentially criminal matters, this involves account termination or referral to law

83 Submission of Facebook (14 March 2012) at 5.

84 Ibid, at 6.

85 Ibid, at 6.

> enforcement. For less serious matters, we will remove any content that violates our policies and direct people to the Community Standards when they next log in to further educate them about the policies that govern the site.

3.33 In a similar vein Google detailed the range of policies and processes it employed "to minimise and provide remedies for harmful speech online."[86] These included:

(a) Clear policies regarding what content is and is not acceptable, such as the YouTube Community Guidelines;

(b) Tools that provide users with simple and effective ways to report any content that breaches community standards or guidelines, or otherwise causes concern to site users (e.g., the YouTube flag system);

(c) Tools that enable parents to determine what level of content they wish their children to be exposed to on YouTube and the Android Market online app/game store;

(d) Educational initiatives such as its partnership with NetSafe to create the Google Family Safety Centre.

3.34 Trust and safety are also critical to the success of New Zealand's leading domestic internet property, Trade Me. In its submission Trade Me outlined the systems it has put in place to protect users including a 24 hour, seven day a week "policing team" staffed by Trade Me employees capable of responding to a range of user problems. While Trade Me's primary focus relates to the integrity of their sales processes, they have also expended significant resources in developing technology and systems to ensure their Community Message Boards are not used harmfully or in breach of the law.[87] Users can also fast-track unsuitable content for review.

3.35 In its submission Trade Me provided us with a snap shot of how these systems were used by the Trade Me community in November 2011. In the previous month:[88]

- Members placed close to 600,000 posts on the message boards;
- Trade Me received some 2,500 reports from members about these posts;
- In response the message board team responded by removing 700 individual posts and a number of full threads;

86 Submission of Google New Zealand Ltd (14 March 2012) at 15.

87 For example in its submission Trade Me explained that when it becomes aware of a name suppression order that is likely to be breached it typically sets message board alerts designed to bring potential infringements to its attention.

88 Submission of Trade Me Limited (12 March 2012) at 40.

- Over the same time the community voted off 6,643 posts.

Assessing the effectiveness of self-regulatory solutions

3.36 Given their dominance of the networked public spheres, and the extraordinary volume of data exchanged by the millions of people around the world who use Facebook and Google services each day, it is inevitable that breaches will occur. For example, anyone who types the phrase "school fights + New Zealand" into the YouTube search engine will find a selection of video clips featuring student assaults. Some are clearly staged, some are featured within the context of a news programme, many are several years old. An infamous Australian clip involving a retaliatory assault in a Sydney school has been viewed more than 7 million times since it was posted a year ago. The most recent New Zealand clip was posted in February 2012 and had been viewed more than 7,000 times when we accessed it in June. It appears to feature a brawl captured on a cell phone.

3.37 Of course anyone who views these clips must first have *intentionally* sought them out. If they were offended by the content of the video they are free to report them using the simple tools available on the site. If the video in question was deemed to be in breach of YouTube's community standards (which prohibit uploading videos showing "graphic or gratuitous violence" among other things)[89] it may be removed by the site's administrators. The user who posted it might receive a strike – repeated violations can lead to various penalties including disabling of the user's ability to post new content for a period, or in the case of persistent offending, account deactivation.

89 YouTube's community standards state as follows:

- Graphic or gratuitous violence is not allowed. If your video shows someone being physically hurt, attacked, or humiliated, don't post it.
- YouTube is not a shock site. Don't post gross-out videos of accidents, dead bodies or similar things intended to shock or disgust.
- Respect copyright. Only upload videos that you made or that you are authorized to use. This means don't upload videos you didn't make, or use content in your videos that someone else owns the copyright to, such as music tracks, snippets of copyrighted programs, or videos made by other users, without necessary authorizations. Read our Copyright Tips for more information.
- We encourage free speech and defend everyone's right to express unpopular points of view. But we don't permit hate speech (speech which attacks or demeans a group based on race or ethnic origin, religion, disability, gender, age, veteran status, and sexual orientation/gender identity).
- Things like predatory behavior, stalking, threats, harassment, intimidation, invading privacy, revealing other people's personal information, and inciting others to commit violent acts or to violate the Terms of Use are taken very seriously. Anyone caught doing these things may be permanently banned from YouTube.

3.38 But as our submitters told us, even when users do utilise the reporting tools provided by websites to alert administrators to the presence of offensive content, it can often be a long and frustrating process. Of necessity these automated reporting systems rely in the first instance on pre-coded templates which do not always provide the appropriate channel for addressing complex human behaviours. In the course of our inquiry we were made aware of many cases where individuals had battled for months to have highly offensive content, including false Facebook pages, taken down.

3.39 These included instances where students had set up "hate pages" on Facebook to publish malicious rumours and content about other students; where individuals had been targeted by anonymous posters creating false online profiles containing damaging content; and where highly defamatory allegations had been disseminated via blog sites.

3.40 NetSafe was very clear in its submission and in subsequent meetings with us that many people who come to them for help feel defeated and distressed by the complexity of complaints systems and the lack of direct communication channels.

3.41 Given the size of these networked platforms it is no surprise that individual complainants should fall through the cracks. This is the case even with highly motivated corporate players such as Google and Facebook but as InternetNZ pointed out in its submission, it is even more of a risk with internet services and content hosts who have no such commitment to standards or concerns about their users' safety.[90]

3.42 In the absence of any centralised body responsible for monitoring complaints about online communication it is difficult to assess how effective New Zealanders consider the self-regulatory tools and laws to be. At this point neither Google nor Facebook produce country specific reports on the use of community reporting tools and the type or volume of content that has been removed as a consequence of such individual user reports. Without this type of information it is difficult to assess how effective users find these tools.

Independent research findings

3.43 As discussed earlier, the Law Commission contracted independent research company Big Picture to survey New Zealanders about a range of issues relating to standards and accountability with respect to both traditional and new media. As part of this research participants were surveyed about:

- their awareness of the "laws, rules or standards" that apply to harmful speech

90 Submission of InternetNZ (12 March 2012) at 9.

online;

- their awareness and assessment of "safeguards which operate within online communities, including the systems of online reporting employed by sites such as Facebook";
- their awareness of where to go for help if they were experiencing "a serious problem with harmful speech on the internet" which they had been unable to resolve themselves.

3.44 On the first point only one in ten respondents was spontaneously aware of the laws, rules or standards which apply to harmful speech on the internet. Among those in the 18-29 demographic, who are much higher users of new media, this rose to one in eight.

3.45 With respect to awareness of online safeguards and reporting tools, less than a third (29 per cent) of the total sample said they were aware of these tools. Among the younger demographic, awareness was higher, at 39 per cent.

3.46 Of those who were aware of the existence of online safeguards and reporting tools, 25 per cent regarded these systems as either "effective or extremely effective" and 63 per cent thought they were "effective some of the time or not at all." Of the younger demographic a third (34 per cent) regarded these safeguards as either "effective or extremely effective."

3.47 Asked where they would go if confronted with a serious problem involving harmful speech on the internet that they had been unable to resolve, a large proportion – 42 per cent – said they did not know.

3.48 Even among the younger demographic, 38 per cent said they did not know where to go for help if they had a serious problem with harmful speech that they could not resolve.

3.49 Of those who nominated a body, 20 per cent said they would go to the Police and 17 per cent said they would go to the website's own complaints system. Just four per cent said they would seek legal advice.

3.50 When asked whether there should be some form of accountability by social media sites for harmful content 45 per cent said "definitely" and a further 37 per cent "maybe". The most common reasons given by those who were *definitely* in favour of some form of accountability for social media platforms:

- Content can be very harmful or damaging;
- Sites need to be held accountable;
- Standards should apply to users and providers.

3.51 Reasons given by those who were either ambivalent or opposed were a mix of principle and pragmatism:

- The individual makes the choice, not the site;
- Free speech/people can say what they want;
- Individuals need to be held accountable;
- Can't control everyone/difficult to regulate.

3.52 Despite the higher incidence of harmful speech exposure within the younger demographic, this group were less in favour than the general population of social media being held accountable with 33 per cent saying they felt social media definitely should be held accountable compared with 45 per cent of the total population.

Submitters' views

3.53 In our Issues Paper we sought feedback from the public about many of these same issues, including the effectiveness of the non-legal remedies that operate within online communities and the adequacy of the existing law.

3.54 As we might expect, those submitters who regarded the problem of digital communication harms as significant tended to be more sceptical about the adequacy of the current legal and non-legal solutions. Conversely, submitters like Google suggested the problem was ill-defined and adequately addressed by the non-regulatory systems already in place online, backed by the law.

3.55 In its submission Trade Me noted that the effectiveness of online safeguards such as reporting tools depended on their "accessibility, responsiveness and ease of use."[91] It noted that some websites make their reporting tools difficult to find or have none. Trade Me also stressed the importance of providing users with direct access to real-time assistance over the phone. In the course of consultation, Trade Me told us they are approached by their members for assistance after being unable to get a response from offshore web operators. At times Trade Me will end up approaching such operators on their members' behalf.

3.56 NetSafe submitted that while technical solutions "are widely touted" as the solution to harmful digital communication "in reality there are limited instances where such solutions are effective".[92]

---

91 Submission of Trade Me Ltd (12 March 2012) at 12, 37.

92 Submission of NetSafe (24 February 2012) at 2.

3.57 It suggested that blocking techniques offer only partial and temporary solutions to prevent abusive content from reaching its target. Reporting systems could be effective if they were easy to access and the host or platform was responsive. NetSafe told us that its experience dealing with the dominant and more mature internet properties such as Facebook and Google indicated these organisations systems and levels of responsiveness to user complaints was constantly improving. However this was often not the case with smaller web-based businesses lacking the resources or "not managed by companies with a strong social responsibility focus."

3.58 Police also questioned whether online reporting and other self-regulatory systems employed by social media sites were adequate, citing an "increasing number of requests for help/advice from members of the public (both young and old) in relation to Facebook issues and other forms of social media harassment."

3.59 "Sweet As Social Media", a New Zealand advocacy group formed to "fight anti-social behaviour and bullying online," reported a lack of awareness and/or utilisation of automated systems for dealing with offensive content. The group submitted that many who had made use of these systems found the process slow and that many were "frustrated by a lack of response or remedy from these sites."[93]

3.60 The Commission also received a number of submissions from organisations and individuals outlining their own personal experiences of attempting to utilise online reporting tools to deal with a range of problems including fake profiles, hate sites and malicious impersonation.

3.61 In its submission the National Council of Women (NCW) outlined a campaign to have Facebook remove pages which it believed were "advocating, supporting and trivialising rape and violence against women."[94] NCW said despite widespread opposition to these pages Facebook had been reluctant to take action, saying that opinion that was outrageous or offensive to some did not necessarily violate the company's policies. Some pages were eventually taken down but NCW pointed out that not all individuals or groups had the time or resources to apply the type of commercial and public pressure that was required before action was taken.

3.62 An individual submitter who had been the subject of defamatory publications on Twitter described her frustration at the lack of remedies available to her:

---

93 Submission of Sweet As Social Media (received 15 March 2012) at 12.

94 Submission of the National Council of Women of New Zealand Te Kaunihera Wahine O Aotearoa (30 March 2012).

> I have reported my case to the police, but they are unwilling to act as direct threats were not made. Twitter claims no rules were broken despite the obvious defamatory content and Google won't even entertain my complaint unless it is backed by a 'law enforcement agency'.
>
> I do feel powerless to act to protect my reputation.

The limits of user choice and the "right of reply"

3.63 As discussed in our Issues Paper, robust communication has been a hallmark of the internet since its inception and for many the facility for users to directly participate in debates and exercise their free speech rights mitigates any harm that might arise. The read/write web[95] is, on this view, a self-correcting system which enables constant scrutiny and correction by users.

3.64 It is also a system that requires users to make active choices. Unlike traditional broadcast media content which is "pushed out" to a mass market, new media relies on people to actively seek out (or "pull in") content and to exercise a level of choice and judgement about what they consume and with whom they engage which is entirely new.

3.65 These characteristics of the new media environment are often seen to be highly significant when considering policy and legal responses to harmful online conduct.

3.66 However, while we agree that these characteristics are significant and that over time users will become increasingly adept at exercising choice and amplifying their own voice online, there are a number of compelling reasons why, for the moment at least, we cannot entirely depend on this new paradigm to protect users from speech harms.

3.67 To begin with, there exist a number of important information and power asymmetries in cyberspace. For example, those who run blog sites and who host interactive forums and websites are not only able to set the terms and conditions which apply to those using these sites but they are also able to determine how much control to exercise over content (e.g. whether or not to monitor user comments), and whether and when to remove content. Website administrators will also often have access to significant information about their users, including email addresses, IP addresses, the search engine query used to find the website and the referring page or link from which the user came to the site.[96]

---

95 The read/write web refers to the set of web tools that allow for conversation, collaboration and creation. See BBC News "Berners-Lee on the read/write web" (online ed, 9 August 2005).

96 David Farrar "Privacy and New Media" (Presention at Privacy Awareness Week forum, 3 May 2012, Wellington) <privacy.org.nz/assets/Files/PAW-privacy-forums/David-Farrars-presentation.pdf>.

3.68 A person who has been targeted by a blog and/or by participants in an online discussion thread certainly has the option of defending themselves and or correcting information that may be factually incorrect by participating in the comments. But a single correcting comment embedded in a long tail of abusive commentary may not have much effect – particularly if the originating blog post continues to assert false or malicious information.

3.69 Also, web-based interactions are mediated by the same sorts of power imbalances that exist offline: mob-like bullying behaviour by cliques of like-minded individuals congregating online is not easily countered by the lone voice of the targeted individual. And while it is possible to comment anonymously online or to adopt a different persona, it will often be the case that participants in online discussions will know each other's real identities.

3.70 Of course, the person who is the subject of the abuse does not have to visit the blog site or engage with their attackers. But given the porous nature of the web, this may prove a less effective solution than it might first appear. As we have discussed, content that appears in one context can quickly go viral as it is linked to or copied by other users. Prominent blog sites are regularly trawled by mainstream media and there are almost daily examples of content published within a quasi-private forum becoming truly public. Trade Me pointed out that New Zealand news media regularly harness the Trade Me message boards in this way.[97]

3.71 The submitter who went to the Police after becoming aware of defamatory statements about her on Twitter provides a good example of why it is not always possible to quarantine or ignore content on the web. This person was not an avid user of new media but her attention was drawn to the defamatory posts by a journalist who had googled her name while researching a business story. The submitter discovered that anyone seeking her out on the web, including prospective employers and business clients, was being directed by the search engine to the offensive content.

3.72 Paradoxically, private individuals with a limited or non-existent online presence can be more adversely affected by malicious communication disseminated via searchable platforms such as Twitter. Damaging content about a high profile individual may be buried in pages of "good" or neutral content, but when there is limited information about the person online the defamatory content rises high in the search rankings.

97 It is worth noting that while those with a Trade Me account can browse message boards the company has chosen to architect the site in such a way as to preclude Google or other search engines from indexing content on message boards.

3.73 The submitter to our review was advised to bolster her online profile by creating relevant and high quality content in an attempt to bury the defamatory content. This worked for a brief period but was ultimately unsuccessful.

3.74 Also, while the relationship between online content hosts and publishers and users is arguably a great deal more dynamic, responsive and egalitarian than the relationship between consumers and traditional news media companies, cyberspace is not a level playing field. Bloggers' motivations, vested interests and relationships with their sources can be every bit as opaque as in the established media.

CONCLUSIONS

3.75 In this chapter we have outlined a three-tiered approach to dealing with harmful communications in cyberspace. The first tier involves what Facebook describes as "user empowerment". This requires educating internet users about their rights and responsibilities in cyberspace and equipping them with the technical knowledge and tools to exercise these rights and responsibilities.

3.76 The second tier involves the self-regulatory systems which have evolved on the internet to support standards and control bad actors. These self-regulatory systems often include terms of use contracts which outline the types of behaviours which are unacceptable and protocols for dealing with breaches of these terms. Commercial entities have developed increasingly sophisticated reporting infrastructures and technologies which allow users to flag content which breaches a site's terms and conditions.

3.77 The third tier is the body of statutory and common law which provides the boundaries for acceptable speech for citizens regardless of what channel they are using to communicate.

3.78 In principle we agree with this approach. Cyberspace is a vital forum for the free exchange of information and ideas among citizens and heavy-handed regulatory intervention is neither defensible from a free speech perspective, nor practically achievable.

3.79 Empowering people to exercise their rights and responsibilities in cyberspace and providing infrastructure and technologies to give effect to these must form the first line of defence against digital communication harms.

3.80 However it cannot be the *only* line of defence. Citizens should have the right to legal protection and meaningful redress when they suffer significant harm as a result of

communication abuses. In this chapter we have identified a number of problems with the existing self-regulatory remedies available to citizens harmed by digital communication. Our research and the information provided to us by submitters indicate there is currently a gap which neither the self-help mechanisms nor the law is adequately bridging. To bridge that gap will require the collaboration of industry, legislators, educators, parents and users. In the following chapter we argue that the law needs to be extended to better protect against some of the serious emotional harms which can be caused by the new forms of communication.

3.81 For the reasons outlined in this chapter we do not believe that the current mix of user empowerment and self-regulatory and legal solutions is always capable of providing that redress.

3.82 User empowerment is a laudable ideal but for the moment there exist a number of important information and power asymmetries in cyberspace. The digital divide applies not only in relation to *access* to technology but also with respect to people's ability to harness the power of technology for legitimate and illegitimate purposes.

3.83 And while we endorse the view that self-regulatory systems must always be a user's first line of defence against harm, we are not convinced that these systems, even at their most sophisticated can provide a total solution. Terms of use contracts are only meaningful if they are enforced by the corporations who impose them and reporting tools are only useful if they result in action.

3.84 Our research indicates awareness of the existence of online reporting tools is relatively low, even among the younger demographic (39 per cent) and of those who are aware of the tools only a third of the younger demographic rated them as "either effective or extremely effective".

3.85 Moreover self-regulation on the web is extremely variable: publishers who have no commercial or other interest in attracting mass participation may choose not to apply any standards or sanctions to their own or their community's behaviour online.

3.86 These conclusions are supported by NetSafe which reports that many of those who turn to their organisation for assistance feel defeated by the lack of responsiveness of website administrators and other content hosts to the existence of harmful content.

3.87 And while it is true that people can exercise considerable choice and control over how they interact on the web and with whom, the porous nature of the internet and the power of search engines means damaging content that has limited exposure in its original form can quickly find its way into much more public spheres after being

indexed by search engines.

3.88 This brings us to the effectiveness of the law as the backstop to these self-regulatory measures and the third prong of the strategy for addressing harmful communication.

3.89 In our Issues Paper we reached the preliminary conclusions the existing criminal and civil law was capable of dealing with many but not all of the new and potentially more damaging harms arising from the use of new technology.

3.90 More critically, we drew attention to a number of impediments to the successful application of the law with respect to harmful digital communication. These included a lack of knowledge of legal rights and responsibilities; difficulties accessing the law; difficulties enforcing the law as a result of inadequate investigative resources and tools; and difficulties in obtaining evidence and identifying perpetrators. There is also a significant problem in providing citizens with quick access to meaningful remedies given the slowness of the court processes and the speed with which harmful content can be disseminated on the internet.

3.91 In short we are persuaded by NetSafe's view that there is currently a gap between where self-regulatory systems end and the law begins and this gap is leaving those who have suffered real harm with no recourse to justice.

3.92 In the following chapters we set out our proposals to bridge that gap.

Chapter 4: Changes in the law

INTRODUCTION

4.1 In this paper we ask whether the technology revolution, and the new forms of communication it has provided us with, requires movement in our legal rules. We conclude that it does.

4.2 The proposals contained in this chapter are focused primarily on the law. But amending the law and introducing new offences will not be enough. Unless the law is understood by citizens, consistently enforced, and its remedies meaningfully applied, it is of limited value. Hence we are as much concerned in this report with putting forward proposals for how to make the law accessible and effective in the age of mass participatory media as we are with the creation of new offences. We address this issue in chapter 5.

4.3 We are not advocating fundamental changes to New Zealand's laws – we propose one new offence, and some extensions and modifications of others. However we are advocating novel solutions for how people access the law and how the law is applied. The internet and the read/write web have brought about a paradigm shift in communications and like all institutions, the justice system must adapt – with respect both to the sanctions and remedies it provides to citizens.

4.4 We believe these proposals are a justified and proportionate response to the problems of harmful digital communication. If implemented, they would more effectively curb certain types of harmful communication. Given the fundamental importance of freedom of expression it is vital that these constraints go no further than can be justified in a liberal democracy. A very large and complex body of legal and philosophical writing has been devoted to the question of what constitutes "expression" in the human rights context, and when the law may be justified in constraining it. In the following discussion we provide a necessarily high level account of how these debates underpin our proposals.

The NZ Bill of Rights Act 1990

4.5 The dynamic relationship between technology and social values is reflected in the law and lies at the heart of this current debate about how we respond to digital communication harms.

4.6 In any deliberative exercise involving the law and communication section 14 of the

New Zealand Bill of Rights Act 1990 (BORA) is a key factor.[98] It provides:

> **Freedom of Expression** – Everyone has the right to freedom of expression, including the freedom to seek, receive and impart information and opinions of any kind in any form.

4.7 Like all Bill of Rights freedoms, it is qualified by section 5, which provides:

> **Justified limitations** – Subject to section 4 of this Bill of Rights, the rights and freedoms contained in this Bill of Rights may be subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

4.8 Section 14 raises several questions about which views may differ. The first question is what 'expression' means. Does it, for example, include conduct? Is posting an obscene photograph on a website 'expression'? We prefer to take the widest possible view of 'expression'. That is probably the legislative intent: 'of any kind in any form' would suggest so. The New Zealand courts have responded similarly: the Court of Appeal has said the word is "as wide as human thought and imagination".[99] Our courts have held that flag burning[100] and lying down in front a car[101] as a protest are forms of 'expression'. So we take the word 'expression' as being wide enough to cover all the types of communication with which we deal in this paper.

4.9 The second question is whether all types of expression, however objectionable or harmful they may be, come within the cover of section 14. This raises the question of the scope of section 14. One view is that each right in the Bill of Rights Act must be interpreted in light of the values it was enacted to protect. On this view it might be argued that speech which has no legitimate value and serves no legitimate purpose, does not fall within the protection of section 14 at all. Thus, for example, images of child pornography, or gratuitously offensive personal comments would not be within the scope of section 14, and laws prohibiting their communication would raise no Bill of Rights Act issues at all.

4.10 The other view is that all expression falls within section 14, in which case the question becomes whether a law prohibiting certain types of expression (for example child pornography or offensive personal comments) is a justified limitation under section

---

98 See the discussions in Paul Rishworth and others *The New Zealand Bill of Rights* (Oxford University Press, Melbourne, 2003) at chapter 12; and Andrew Butler and Petra Butler *The New Zealand Bill of Rights Act : A Commentary* (Lexis Nexis, Wellington, 2005) at chapter 13.

99 *Moonen v Film and Literature Board of Review* [2000] 2 NZLR 9 (CA) at [15] per Tipping J.

100 *Morse v Police* [2012] 2 NZLR 1 (SC).

101 *Police v Geiringer* (1990-1992) 1 NZBORR 331. See however the comment by Paul Rishworth and others *The New Zealand Bill of Rights* (Oxford University Press, Melbourne, 2003) at 313.

5.[102]

4.11 It is very difficult to envisage a case of a truly objectionable message where the end result would be any different, whichever approach was taken. There is at least one New Zealand case (involving contempt of court) when the Judge took both approaches in the alternative and reached the same result.[103] While acknowledging that there is another view, for the purposes of this paper it is convenient to take the second approach and assume that even the most offensive and objectionable communications fall within the ambit of section 14, and that restrictions placed on them by the law must be justified in terms of section 5.

4.12 Having said that, the approach we are taking does not assume that all types of communication are of equal value. International jurisprudence has moved towards a view that these are a number of levels of speech value. The highest value is accorded to political speech, the lowest to hate speech and gratuitously offensive personal comments without any legitimate purpose. Restrictions on speech of high value require much stronger justification under section 5, restrictions on speech at the bottom of the "value pyramid" require minimal justification.[104]

4.13 The third question is, taking all of the foregoing into account, how one applies the section 5 test, i.e. whether the limitation proposed is reasonable, prescribed by law, and such as "can be demonstrably justified in a free and democratic society." The application of section 5 by the courts has led to some of the most complex jurisprudence in our law. That is unfortunate, because it makes understanding of the process very difficult for persons, particularly lay adjudicators, who have to apply it. But for present purposes it may be said the crucial elements are as follows:[105]

(a) The purpose of the proposed limitation on the freedom must relate to "concerns which are pressing and substantial."

(b) The measures adopted to limit the freedom must be rationally connected to that purpose.

(c) The limiting measures must not impair the right more than reasonably necessary.

---

102 See *R v Hansen* [2007] 3 NZLR 1 (SC) at [22] per Elias CJ.

103 *Solicitor General v Radio New Zealand* [1994] 1 NZLR 48 (HC).

104 Jacob H Rowbottom "To Rant, Vent and Converse: Protecting Low Level Digital Speech" (2012) 71 CLJ 355.

105 Based on the Canadian case *R v Oakes* [1986] 1 SCR 103. New Zealand Courts have commonly adopted that test: see *R v Hansen* [2007] 3 NZLR 1 (SC) at [64] per Blanchard J and at [103]–[104] per Tipping J.

(d) The limiting measures must be proportionate to the purpose sought to be achieved. This element is particularly important. One should not "use a sledgehammer to crack a nut".

4.14 As Tipping J summarised it in *R v Hansen*: "Whether a limit on a right or freedom is justified under section 5 is essentially an inquiry into whether a justified end is achieved by proportionate means".[106]

Applying these principles

4.15 In the context of this paper we have had to ask first whether the various kinds of communication we are addressing require legal intervention: whether, in other words, there is a pressing and substantial concern which the law should meet. In this chapter we argue that if such communications cause significant harm then such intervention is needed.

4.16 We also have had to consider what is a proportionate response. In paragraphs 4.72 to 4.76 of this chapter we argue that in some cases, particularly if the communication is grossly offensive and causes real harm, a criminal response is justified. In other cases amendments to the civil law will be appropriate.

4.17 In chapter 5 we turn to the question of remedies. We propose a tribunal which could make orders, the purpose of which is to protect the affected person, for example by requiring that the harmful communication be removed. In each case which comes before it, the tribunal will need to consider whether the order sought is justified in terms of section 5.

4.18 We would also note that several of the reforms we propose merely amend earlier legislation to ensure that it is fit for purpose in the digital age. Some of that legislation was tested against the Bill of Rights in its original form, and our reforms do not really involve any greater limitations on freedom of expression than that legislation already imposed.

4.19 For example, New Zealand's Telecommunications Act 1987 created an offence in connection with the "misuse of a telephone device". It has been re-enacted in the Telecommunications Act 2001. As well as prohibiting the use of a telephone to intentionally offend someone by using "profane, indecent, or obscene language"[107] the Act also makes it an offence to use the telephone "for the purpose of disturbing,

106 *R v Hansen* [2007] 3 NZLR 1 (SC) at [123].

107 Telecommunications Act 2001, s 112(a).

annoying, or irritating any person, whether by calling up without speech or by wantonly or maliciously transmitting communications or sounds, with the intention of offending the recipient".[108]

4.20 The threshold ("disturbing", "annoying", "irritating", "offending") seems low by today's robust standards. There is perhaps doubt whether it would now survive a Bill of Rights vet.

4.21 However there clearly must be legal limits to what is regarded as acceptable speech. There always have been, and we must face the question of the extent to which the limits need to change in the new environment. That is the task we are confronting in this report and the task Parliament will grapple with should it decide to proceed with the changes we are recommending. We are satisfied that the changes we propose are proportionate to the harms that need to be addressed.

4.22 We are not alone in this. Governments elsewhere in the world are similarly reviewing their statute books.

THE CURRENT LAWS CONSTRAINING COMMUNICATION

4.23 In our Issues Paper we set out in some detail the various laws which exist to constrain and remedy such harmful speech.[109] These include a mix of statute and judge-made laws, and include criminal offences and civil wrongs. The current framework is a patchwork of measures that together provide a degree of protection from speech harms, both online and offline.

Criminal Law

4.24 Criminal law is concerned with maintaining law and order and protecting society. A criminal penalty is a more significant fetter on free speech than a civil remedy and expresses condemnation of the action as a wrong against society.[110] Cases are brought by the state and investigated by the Police. Penalties for breaches of the criminal law may involve fines or imprisonment. The standard of evidence required is beyond reasonable doubt.

4.25 Long standing rules of the criminal law, which are for the most part contained in the

108 Telecommunications Act 2001, s 112(b).

109 Law Commission *The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age* (NZLC IP27, 2011), chapters 7-8.

110 See discussion of the New Zealand Bill of Rights Act 1990 above at [4.5] to [4.14].

Crimes Act 1961 and the Summary Offences Act 1981, are capable of addressing certain types of harmful communication. Most of them are phrased in technology-neutral language, and enact basic principles which can do service in the modern world.

Threats and intimidation

4.26 A number of the provisions of the Crimes Act 1961 deal with threats. It is an offence to threaten to kill or cause grievous bodily harm,[111] to destroy property or injure an animal,[112] or to do an act likely to create a risk to the health to one or more people with intent to cause serious disruption.[113]

4.27 The Summary Offences Act 1981 contains an offence of intimidation which is committed by a person who, with intent to frighten or intimidate the other person, or knowing that his or her conduct is likely to cause that person reasonably to be frightened or intimidated, threatens to injure that person or any member of his or her family or to damage any of that person's property.[114]

4.28 The offence of blackmail under the Crimes Act is constituted by threatening to disclose something about a person with the intent of obtaining a benefit.[115]

4.29 The Harassment Act 1997, in addition to providing civil remedies, also creates an offence of harassing another person with the intent to cause them to fear for their own safety or the safety of a family member.[116]

4.30 The Telecommunications Act 2001 offence of misuse of a telephone was set out above at para 4.19. We are aware of this offence being used to prosecute a man who sent text messages threatening to put naked pictures of a woman on Facebook.[117] So, despite a threshold which we have described as low, it is available to deal with deserving cases.

Sexual matters

4.31 The Crimes Act makes sexual grooming an offence. It is an offence for a person to intentionally meet or set out to meet a young person under the age of sixteen, having

111 Crimes Act 1961, s 306.

112 Crimes Act 1961, s 307.

113 Crimes Act 1961, s 307A.

114 Summary Offences Act 1981, s 21.

115 Crimes Act 1961, s 237.

116 Harassment Act 1996, s 8.

117 David Clarkson "Man in court over naked pic threats" Fairfax NZ News (online ed, 31 May 2012) <www.stuff.co.nz>.

met or communicated with them previously, if at the time of doing so he or she intends to engage in unlawful conduct with that young person.[118]

4.32 The Crimes Act provides that it is an offence to publish intimate picture of someone taken covertly without that person's consent.[119] This does not cover the publication of intimate pictures that are taken with consent, but published without consent. However other offences have sometimes been used to cover that situation. For example, it is an offence under the Crimes Act to distribute an indecent object or model.[120] Albeit with a degree of liberal interpretation, this has been used to convict a person who published intimate pictures on the internet even though the pictures were initially taken with the subject's consent.[121]

4.33 It is also an offence under the Films, Videos, and Publications Classification Act 1993 to make or distribute an objectionable publication.[122] A publication is objectionable if it deals with matters such as sex, horror, crime, cruelty or violence in a way that is likely to be injurious to the public good.[123] Publications of children or young persons who are nude or partially nude and are reasonably capable of being regarded as sexual in nature are deemed to be objectionable.[124] A publication is also deemed objectionable if it tends to promote or support the exploitation of children or young persons for sexual purposes.[125]

Incitement

4.34 It is an offence to incite counsel or procure a person to commit suicide if the person in fact commits, or attempts to commit, suicide.[126] It is also an offence to aid or abet suicide. Suicide pacts are also unlawful, but only if one or more participants to the pact

118 Crimes Act 1961, s 131B.

119 Crimes Act 1961, s 216J. See Law Commission *Intimate Covert Filming* (NZLC SP15, 2004).

120 Crimes Act 1961, s 124. The leave of the Attorney-General is required before a prosecution may be brought under this provision.

121 "Naked photo sends jilted lover to jail" Fairfax NZ News (online ed, 13 November 2010) <www.stuff.co.nz>.

122 Films, Videos, and Publications Classification Act 1993, ss 123-124. See *Broekman v R* [2012] NZCA 213.

123 Films, Videos, and Publications Classification Act 1993, s 3(1).

124 Films, Videos, and Publications Classification Act 1993, s 3(1A).

125 Films, Videos, and Publications Classification Act 1993, s 3(2)(a).

126 Crimes Act 1961, s 179.

actually carry out the act of suicide.[127]

4.35 It is an offence to excite racial disharmony.[128] This requires the use of threatening, abusive or insulting language with intent to excite hostility or ill-will against a group of people on the ground of colour, race, or ethnic or national origins.

4.36 It is also generally an offence to incite any person or persons to commit an offence whether that offence is actually committed or not.[129]

Civil Law

4.37 The civil law is concerned with resolving disputes between citizens or organisation, and sometimes between citizens or organisations and the state. Actions are initiated by citizens seeking compensation or other remedies for harms they allege have been caused by the other party. They are not prosecuted by the police and the standard or proof is on the balance of probabilities, rather than beyond reasonable doubt which applies in criminal trials.

4.38 The civil law comprises both common law and statute law. The common law is made up of the legal doctrines that have their genesis in and are developed by case decisions of judges. This can be contrasted with statute law that is contained in legislation (including judicial decisions that interpret the legislation).

4.39 One of the main categories of the common law that is relevant to online speech harms is the law of torts, or civil wrongs, which provide a basis for a private citizen to sue for harm suffered by the actions of another person.[130]

Torts

4.40 The tort of invasion of privacy is a relative newcomer whose existence has been confirmed by the New Zealand Court of Appeal in the case of *Hosking v Runting* in 2004.[131] It provides a remedy for publicity given to facts in respect of which there was a reasonable expectation of privacy, the publication being highly offensive to a

127 Crimes Act 1961, s 180.

128 Human Rights Act 1993, s 131.

129 Crimes Act 1961, s 66(1)(d).

130 In the following chapter we recommend the distillation of the key principles from the relevant torts into a set of principles to provide an accessible summary of this part of the law and to guide the remedies granted by the new tribunal we recommend.

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

reasonable objective person.[132] There is a defence if the material published is of public concern.

4.41 The tort in *Wilkinson v Downton* provides a remedy for the intentional infliction of harm. The case itself involved the communication of maliciously false information which caused nervous shock to the recipient.[133] This tort might be thought to have particular relevance in the internet era. But there are no recent examples of its use; it is virtually obsolete.

4.42 The possibility of a tort of harassment has been postulated by the English Court of Appeal but has gained little traction.[134] Whether it contains any spark of life is open to question. In New Zealand, the Harassment Act 1997 and the Domestic Violence Act 1995 provide certain remedies for harassment, discussed below.

4.43 The tort of breach of statutory duty sometimes provides a remedy in damages for breach of a statute. It is perhaps possible that breach of a criminal statute (say the offence of intimidation) might be able to be remedied by civil action. There is however, no certainty about that.[135] The cause of action is unpredictable and is likely to be seldom available in the kind of situation we are addressing.

4.44 The law of defamation provides a remedy for statements about a person which adversely affect their reputation and cannot be proved true. It is an ancient common law action and is encumbered by complex and time-consuming procedures, but its mere existence remains a powerful deterrent against the publication of false allegations. Defences and some privileges have been codified in the Defamation Act 1992.

4.45 The law of breach of confidence[136] provides a remedy for the publication of information which has been imparted in confidence. There is a defence if the information is of public interest. This area of the law, while still significant, has more limited scope in New Zealand due to the existence of the privacy tort in *Hosking v*

---

132 For discussion of the privacy tort, see Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, 2009) at chapters 6 and 7; (NZLC R113, 2010) at chapter 7.

133 *Wilkinson v Downton* [1897] 2 QB 57. See Stephen Todd (ed) *The Law of Torts in New Zealand* (5th ed, Brookers, Wellington, 2009) at [4.7]. "Nervous shock" is more limited than emotional distress.

134 *Khorasandjian v Bush* [1993] QB 727.

135 See Stephen Todd (ed) *The Law of Torts in New Zealand* (5th ed, Brookers, Wellington, 2009) at chapter 8.

136 Breach of confidence is sometimes classified as an equitable wrong rather than a tort.

Runting.[137]

Statute

4.46 Much civil law is "judge-made" or common law, but another source is the legislation enacted by Parliament to provide redress for citizens who are harmed by unlawful communication. The most important of these Acts for the purpose of this review is the Harassment Act 1997 which provides the remedy of a restraining order in respect of harassing conduct.

4.47 The concept of harassment is defined by the Act.[138] It requires more than one piece of conduct over a twelve month period.[139] A restraining order will not be made unless the conduct causes distress to the victim.[140] Even where the conduct causes distress, a restraining order will generally not be made against a person under the age of 17.[141] Later in this chapter we suggest some amendments to the Harassment Act.

4.48 The Domestic Violence Act 1995 provides for the making of protection orders against domestic violence. "Domestic violence" is defined as including psychological abuse including among, other things, intimidation or harassment.[142] It is a condition of every protection order that the respondent must not engage in or threaten to engage in behaviour which amounts to psychological abuse or encourage any other person to do so, and must not (with necessary exceptions) make contact with the other by any means, including electronic message.[143]

4.49 The Copyright Act 1994 provides that a person has a right not to have a "literary… or artistic work falsely attributed to him as author".[144] This has occasionally been used to provide a remedy to persons who have been parodied, or to whom a false quotation has been attributed.[145] It could perhaps be used in relation to such things as false Facebook

137 For discussion of the relationship between the privacy tort and breach of confidence, see Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, 2009) at [6.16]-[6.21].

138 Harassment Act 1997, s 4.

139 Harassment Act 1997, s 3.

140 Harassment Act 1997, s 16(1)(b).

141 Harassment Act 1997, s 12.

142 Domestic Violence Act, s 3.

143 Domestic Violence Act, s 19(1), (2). Police also have a limited power to make temporary safety orders when that is necessary to ensure the safety of a person: s 124B.

144 Copyright Act 1994, s 102.

145 See for example *Moore v News of the World* [1972] 1 QB 441; *Clark v Associated Newspapers Ltd*

pages. Relief by way of damages and injunction are available.

Regulatory Remedies

4.50 Parliament has also passed Acts to protect people's right to privacy (the Privacy Act 1993) and right to equality (the Human Rights Act 1993). Both Acts provide for regulators (the Privacy Commissioner and the Human Rights Commission) to deal with complaints and both have provisions specifically addressing communications which may breach rights to privacy or which infringe human rights. The Human Rights Review Tribunal hears complaints under both Acts which have not been able to be resolved by the Commissioners.

4.51 The Privacy Act 1993 enacts a set of information privacy principles.[146] Principle 11 provides that an agency must not disclose any personal information about a person unless one of a number of statutory exceptions applies. The news media are exempt from this principle,[147] but communicators which fall outside the definition of news media (such as ordinary citizens) are caught by it. Later in this chapter we point to some targeted amendments to the Privacy Act that the Law Commission recommended in an earlier review of that Act.

4.52 The Human Rights Act 1993 provides that conduct likely to excite racial disharmony is a ground of complaint, and also that sexual or racial harassment are unlawful in so far as they have a detrimental effect on a number of listed matters such as employment or access to services.[148] Later in this chapter we recommend some targeted amendments to the Human Rights Act.

THE NATURE OF OUR PROPOSED REFORMS

4.53 As we noted, much of our present law was settled long before the advent of the new media and new forms of communication and those who framed the law could not have been expected to foresee it. Despite that, much of the law is expressed in terms of flexible principle which is technology-neutral and which can work perfectly well in the new environment. But it would be surprising, given the technological and social changes which have taken place over the last few years, if the law remained entirely

---

[1998] 1 WLR 1558.

146 Privacy Act 1993, s 6.

147 Privacy Act 1993, s 2, definition of "agency".

148 Human Rights Act 1993, ss 61- 63.

satisfactory.

4.54 Another challenge is that the applicable law is widely spread across case law and the statute book. There are relevant provisions in the criminal law that have different consequences to breaches of the requirements of the civil law. The spread of the relevant law creates issues of accessibility. It is not always easy for people to readily appreciate the legal implications of their online activities, or for people who are impacted by the online activities of others to access legal remedies.

4.55 The reforms proposed in this chapter have a number of objectives. Some are simply amendments to existing laws to ensure they can be readily applied in the digital environment.

4.56 But in a number of cases we are proposing new offences to address the specific harms which we have argued are a hallmark of certain types of digitally mediated communication. In doing so we are in effect proposing where New Zealand society might set the legal threshold for offensive communication in the digital era.

4.57 In this chapter we recommend a new communications offence to be placed in the Summary Offences Act. We consider that there is clear justification for a tailored offence that people can look to as a primary mechanism to address egregious communication harms at the high end of the scale. We also recommend targeted changes to the law in the areas of harassment, incitement to suicide and intimate covert filming. We continue to support recommendations the Law Commission has made for changes to the Privacy Act that would also usefully respond to problems identified in this review. And we recommend some targeted amendments to the Human Rights Act to clarify its applicability to online communications.

4.58 As well as these measures to fill apparent gaps in the law, in the following chapter we recommend the distillation into an accessible set of principles of the law that applies to communication harms. The purpose of these principles would be to clearly encapsulate the relevant law (without rigidly codifying it) in a way that could be applied by complaints handling bodies and ultimately by the new tribunal that we recommend in the next chapter. A particular benefit of this approach is to raise awareness in the community of the expectations enshrined in the law that are currently dispersed through case law and the statute book.

Submitters' views

4.59 The majority of submitters were supportive of the proposals to review the statute book to ensure that provisions targeting speech abuses could be effectively applied in the

internet era.

4.60 Where concerns were raised these generally related to whether the specific amendments we were proposing to various statutes were the most appropriate vehicle for achieving the desired objectives. For example the Police questioned whether the Telecommunications Act was the appropriate vehicle to address harmful communications via computer.

4.61 The Human Rights Commission raised concerns about the usefulness of the Commission's proposal to amend section 61 of the Human Rights Act (which prohibits the publication and distribution of material which is threatening, abusive or insulting "if it is likely to excite hostility against a group of persons by reasons of their colour, race, or ethnic or national origins") to make clear it applies to electronic communications. The Commission indicated that the threshold for an offence under this section was so high as to render the provision inoperable, which meant there was little point in simply amending the current section to apply to e-media without first undertaking a more fundamental review of the law itself.

4.62 More fundamentally, some submitters questioned the need for new communication offences either on the grounds that the targeted behaviour was already covered by existing provisions or because they did not believe there was strong enough evidence of actual harms.

4.63 We have taken these views into account in formulating the proposed legal reforms outlined below.

Criminal law reforms

4.64 The long-standing rules of the criminal law which, as we have seen, are for the most part contained in the Crimes Act 1961 and the Summary Offences Act 1981, are capable of addressing many types of harmful communication. Most of them are phrased in technology-neutral language, and enact basic principles which can do service in the modern world.

4.65 We have not identified a large numbers of gaps in the criminal law relating to online communication harms; however the few that we have identified are of significance. We recommend a new communications offence, as well as some clarifying amendments to some existing offences.

Threats, Intimidation and Offensive Messages

4.66 The threats and intimidation with which the criminal law is presently concerned all

relate to the creation of fear of a particular kind: the fear of physical damage, be it to person or property. The infliction of distress or mental harm is not covered unless it relates to potential damage of that very tangible physical kind.

4.67 The only inroad into this is that the courts have indicated that they may be prepared to interpret "grievous bodily harm" in the Crimes Act 1961 as including "really serious psychiatric injury, identified as such by appropriate specialist evidence."[149] Whether this would apply, and if so how it would apply, to *threats* to cause grievous bodily harm is undetermined.

4.68 This reflects the old view that mental distress alone was not something of which the law would take cognisance. In 1973 the editors of *Salmond on Tort* said that mental distress "may be too trivial, too indefinite, or too difficult to prove for the legal suppression of it to be expedient or effective."[150] As late as 2004, Lord Hoffmann said:[151]

> In institutions and workplaces all over the country people constantly say and do things with the intention of causing distress and humiliation to others. This shows lack of consideration and appalling manners, but I am not sure that the right way to deal with it is always by litigation.

4.69 Although these statements were made in the tort context, they convey a sentiment that was once present throughout the law. Nevertheless, we consider that, in the 21st century, it should be an offence to cause serious distress or mental harm even though that distress is not related to fear of physical harm. We take this view for several reasons.

4.70 First, fear which anticipates physical harm is not itself physical harm; it is a state of mind, and may be no more severe or hurtful than other kinds of distress – humiliation and fear of verbal attack, for example. There is no reason in principle why these other sorts of emotional harm should be viewed any less seriously.

4.71 Secondly, the distinction between physical and emotional harm has been broken down over a considerable period of years. In a criminal case in the United Kingdom, Lord Steyn has noted that "the civil law has for a long time taken account of the fact that there is no rigid distinction between body and mind."[152] The new tort of invasion of privacy redresses intangible harm; aggravated damages address injured feelings; in the law of contract damages can lie for emotional distress. A breach of privacy for the

149 *R v Mwai* [1995] 3 NZLR 149 (CA) at 155.

150 RFV Heuston (ed) *Salmond on Torts* (16th ed, Sweet & Maxwell, London, 1973) at 14.

151 *Wainwright v Home Office* [2004] 2 AC 406 at [46].

152 *R v Ireland* [1998] AC 147 (HL) at 156. See also *R v Mwai* [1995] 3 NZLR 149 (CA) at 154-155.

purposes of the Privacy Act 1993 requires damage, which can be constituted by significant humiliation, loss of dignity, or injury to feelings. And the criterion for the grant of a restraining order under the Harassment Act 1997 is distress of the plaintiff. In the criminal sphere, mental harm (caused by work-related stress) is specifically included in the definition of "harm" for the purposes of the health and safety legislation, including its criminal provisions.[153] There are offences relating to invasion of privacy in the Crimes Act, for example the provisions about intimate covert filming.[154] Perhaps most notably, since 1987 the Telecommunications Act has made it an offence to use a telephone device "for the purpose of disturbing, annoying or irritating any person" or to wantonly or maliciously transmit communications or sounds with the intention of offending the recipient.[155] (As we have previously noted the threshold for this offence seems even lower than one might expect.) So the criminal law already penalises some types of conduct causing mental distress.

4.72 Thirdly, as we have demonstrated in the preceding sections of this report, the new communication technologies can have effects which are more intrusive and more pervasive, and thus more hurtful, than many other forms of activity. The potential emotional harm is greater than before. There is a risk that it may lead to self-harm or worse. The prospect is sufficiently worrying to justify extending the law. It is right that the law should be concerned about it.

4.73 Finally, overseas jurisdictions are increasingly moving to criminalise communications causing serious distress and mental harm. In the United Kingdom, it is an offence to send an electronic communication of an indecent, obscene or menacing character, or one which is grossly offensive.[156] In Victoria, Australia, the offence of stalking is committed by a person acting in a way that could reasonably be expected to cause physical or mental harm to a victim.[157] The Australian Criminal Code makes it an offence to use a carriage service (for example a mobile phone or the internet) in a way which is menacing, harassing or offensive.[158] And in a number of American states there are statutes which make it an offence to send electronic communications without legitimate purpose which would cause a reasonable person to suffer substantial

153 Health and Safety in Employment Act 1992, ss 2, 49-50.

154 Crimes Act 1961, Part 9A.

155 Telecommunications Act 2001, s 112.

156 Communications Act 2003 (UK), s 127.

157 Crimes Act 1958 (Vic), s 21A(2)(g).

158 Criminal Code 1995 (Cth), s 474.17.

emotional distress.[159]

4.74 We believe that there should be an offence of sending an offensive message with intent to cause distress. We have had regard to section 127 the Communication Act 2003 (UK). Its provisions, so far as material, read;

> **Improper use of public electronic communications network**
>
> (1) A person is guilty of an offence if he –
>
> (a) sends by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or
>
> (b) causes any such message or matter to be so sent.
>
> (2) A person is guilty of an offence if, for the purpose of causing annoyance, inconvenience or needless anxiety to another, he –
>
> (a) sends by means of a public electronic communications network, a message that he knows to be false,
>
> (b) causes such a message to be sent; or
>
> (c) persistently makes use of a public electronic communications network.

4.75 It is something of this nature that we advocate, although we would prefer the United Kingdom provision to be modified in several ways. The offence in subsection (1) does not explicitly require any specific intent or mens rea, and there is no requirement that the message must in fact result in any distress or other mental harm. That in subsection (2) seems to have too low a threshold for a criminal offence: "annoyance, inconvenience or needless anxiety" are not strong emotions.

4.76 We think the elements of the proposed offence should be:

(a) The message must be grossly offensive, or of an indecent obscene or menacing character, or knowingly false.

(b) The sender must either:

(i) Have an intention to cause substantial emotional distress or,

(ii) Know that the message will cause substantial emotional distress.

(c) The message must be such as would cause substantial emotional distress to a reasonable person in the position of the victim.

159 For example, Rhode Island General Laws §11-52-4.2; Missouri Revised Statutes, Title XXXVIII, §565.090; 2011 Minnesota Statutes, §609.749; Michigan Penal Code 1931, §750.411s; Wisconsin Statutes, Criminal Code, §947.0125; Delaware Code, Title 11, chapter 5, §1311; 2011 Florida Statutes, Title XLVI, chapter 784, §748.048; Massachusetts General Laws, Part IV, Title I, chapter 265, §43A. In some cases a pattern of conduct is required, in others a single act is sufficient.

(d) The message need not be directed specifically at the victim, provided that it is placed in the electronic media and is in fact seen by the victim.

(e) In determining whether a message is grossly offensive, the court should take into account such factors as the extremity of the language employed; the age and characteristics of the victim; whether the message was anonymous; whether the message was repeated; the extent of the circulation of the message; whether the message is true or false (in some contexts truths are more hurtful than falsity, in others the reverse is the case); and the context in which the message appeared (different fora may lead users to expect different levels and styles of discourse).

4.77 Some other jurisdictions have specific offences relating to malicious impersonation. An example is Texas which specifically outlaws online impersonation with the intent to harm, defraud, intimidate or threaten, using the persona or name of another person to create a webpage on a social network site or other internet website or to send messages on such a website.[160] However, we are satisfied that the new offensive communication provision we are recommending is sufficient, without specifically providing for online impersonation.

4.78 The provision would to some extent overlap with the existing offences relating to intimidation and threats. It should be added to this group of offences rather than replace any of them. Each of the existing offences serves wider purposes. The specific nature of the provision we recommend serves as a clear, readily accessible directive to persons about a particular type of activity. It conveys a precise message.

4.79 We considered whether the new offence should replace the relevant offence in the Telecommunications Act as the new offence can be considered to be a more technology-neutral version of the existing offence, although the new offence would have a higher threshold. However we conclude that the Telecommunications Act offences should be retained to deal with the particular problem of nuisance phone calls, but believe that consideration should be given to raising the threshold for the requisite emotional distress.

Incitement

4.80 We have considered whether there should be a specific law of inciting others to harass a person. A problem can be raised by groups of people "ganging up" to send hurtful messages another. However, section 66 of the Crimes Act 1961 provides that everyone

160 Texas Penal Code, chapter 33, s 33.07(a).

is party to and guilty of an offence who incites, counsels or procures any person to commit an offence.

4.81 Section 311 further provides that anyone who incites, counsels or attempts to procure any person to commit any offence, even if the offence is not committed, is liable to the same punishment as if they had attempted to commit the offence. In other words incitement to commit an offence is itself an offence. We think, therefore, that there is no need to create a specific offence of inciting offensive communication. It is caught by the more general provisions.

4.82 We have given considerable thought to the question of incitement to suicide. Presently the Crimes Act penalises incitement to suicide only if suicide is attempted, or in fact occurs. We remain of the view we expressed in the Issues Paper that, given the distress such incitements may cause in themselves, let alone the possibly devastating outcome, there is a strong case for making incitement of suicide in itself criminal.[161]

4.83 Attempted suicide is no longer a criminal offence, but we believe that is no reason for decriminalising incitement. We note that the Canadian Criminal Code criminalises counselling a person to commit suicide "whether suicide ensues or not".[162] We recommend a similar provision in New Zealand. We note that it will extend beyond cyber harassment and catch also a wider range of inciting conduct. The circumstances of the incitement, and the manner in which it was conveyed, would obviously be matters to be taken into account in sentencing.

4.84 We do not anticipate that the provision we recommend would be used very often. "Incite" is a strong word: the Oxford Dictionary defines it as "urge" or "spur on", thus implying a desire in the inciter that the subject should actually commit suicide. The incitement offence would also be limited to inciting a particular person to suicide, rather than a non-specific direction. Most messages referring to potential suicide are not sufficiently specific or do not go as far as actual incitement. Some are intended to hurt and cause distress rather than to induce the recipient to self-harm. Communications of that kind are, we believe, sufficiently covered by the general offensive communication provision which we recommend. However, we consider it appropriate that the small number of very harmful communications that do specifically incite a particular person to suicide should be caught by the offence of incitement.

---

161 Law Commission *The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age* (NZLC IP27, 2011) at [8.31].

162 Criminal Code of Canada RSC 1985 c C-46, s 241.

4.85 There are two forms of communication that the proposed provision will not cover, and which we do not think it should. One is the communication which glorifies suicide. Memorial pages on social media sometimes fall into that category, and there is some evidence that they can lead others to copy what has happened. If memorial pages specify the means of death they are likely to be in breach of the Coroners Act 2006, but it would be neither sensible nor practically possible to go beyond that. One cannot outlaw eulogies on the ground that they might induce some impressionable young people to engage in destructive conduct.

4.86 Nor presently are we inclined to specifically outlaw publications which in general terms describe methods of inducing one's own death. In so far as such publications offend against the public interest they may fall into the category of objectionable publications in the Films, Videos, and Publications Classification Act 1993, and we currently see no need to go beyond that.

Sexual Matters

Grooming

4.87 Presently the sexual grooming provisions in the Crimes Act require that the defendant must have either: met the young person, travelled with the intention of meeting them, or arranged for or persuaded the young person to travel with the intention of meeting them.[163]

4.88 Here too we favour a provision that makes the process of grooming criminal in itself, even though no overt act has been done in preparation for a meeting. There is such a provision in the New South Wales Crimes Act.[164] We recommend that it be an offence if a person:

(a) engages in any conduct that exposes a person under the age of 16 years (the young person) to indecent material; and

(b) does so with the intention of making it easier to procure the young person for unlawful sexual activity with him or her or any other person.

Intimate films

4.89 In the Issues Paper *Invasion of Privacy: Penalties and Remedies* the Law Commission asked whether the publication of intimate pictures of a person without their consent

163 Crimes Act 1961, s 131B.

164 Crimes Act 1900 (NSW), s 66EB(3).

should be an offence, even though the pictures were originally taken with the consent of the person.[165] We were then inclined to think not.[166] This conclusion was in part based on the availability of civil damages for breach of privacy.[167] The Law Commission also recommended changes to the Privacy Act to remove the availability of the "domestic affairs" exception in section 56, where a disclosure is highly offensive to an ordinary reasonable person.[168]

4.90 In the relatively short time since the Law Commission concluded its privacy review however, there have been a number of publicised cases involving the publication of intimate pictures without the consent of the subject of the pictures.[169] Often this behaviour occurs in conjunction with the breakdown of a relationship.[170]

4.91 Prosecutions have been brought against the perpetrators of these acts, under criminal provisions that were not necessarily designed to deal with this issue. It has led a judge in one case to press into service section 124 of the Crimes Act (distribution or exhibition of indecent matter), to which we have referred above, to deal with it despite the rather strained interpretation that that involved.[171]

4.92 Judge Becroft was reported in that case as saying that he was adapting an old print law for the internet age. However section 124 is not particularly suited to this situation. It has been suggested that there may be difficulties with such photographs being considered to be "indecent", given the hyper-sexualisation of the Internet and that the real issue is that the criminal law does not provide an adequate response for the dissemination of images that seriously impinge on the dignity of another person.[172]

---

165 Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC IP14, 2009) at 246.

166 Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC R113, 2010) at [3.32].

167 See *L v G* [2002] DCR 234 where a woman seeking damages when pictures taken of naked body were published in an adult magazine was awarded $2,500.

168 Law Commission *Review of the Privacy Act* (NZLC R123, 2010) at R45. As discussed at [4.125] we continue to support this recommended amendment to the Privacy Act.

169 For example, in 2010, Australian model Lara Bingle threatened to sue a former boyfriend for breach of privacy for selling an intimate picture of her to a woman's magazine after a breakup.

170 Jody Callaghan "Sexting growing issue for Kiwi teens" Fairfax NZ News (online ed, 5 July 2012) <www.stuff.co.nz>.

171 "Naked photo sends jilted lover to jail" Fairfax NZ News (online ed, 13 November 2011) <www.stuff.co.nz>.

172 Jonathan Barrett and Luke Strongman "The Internet, the Law, and Privacy in New Zealand: Dignity with Liberty?" (2012) 6 International Journal of Communication, 127 at 136-137.

4.93 The publication of intimate pictures without the consent of the subject is a form of privacy intrusion. The level of harm and distress that is caused is significant. The criminal law is invoked for privacy intrusions considered serious enough to warrant that response, such as outsiders recording private conversations without consent,[173] peeping and peering into a private dwelling,[174] and intimate covert filming without consent.[175] We consider that the focus of the criminal law should now be on whether the *publication* of the images is without consent, rather than, as now, on whether the images were originally *taken* with consent. This behaviour can be viewed essentially as a form of intimidation.

4.94 In our view, the reported level of online publication of intimate visual recordings now warrants an amendment to the Crimes Act to criminalise the publication of intimate images by the person who made the image, without the consent of the person depicted. Accordingly, we recommend that the covert filming provision of the Crimes Act 1961 be amended to provide that it is an offence for the creator of an intimate picture to publish it without consent even though the picture may have been taken originally with subject's consent.

4.95 We acknowledge that the policy decision in invoking the criminal law in this situation is finely balanced. Other recommendations in this report would provide non-criminal remedies for victims of this behaviour. The tribunal we discuss in the next chapter would have the power to order that offensive material be taken down from websites and online forums. Later in this chapter we discuss the changes to the Privacy Act that are needed so that victims can more readily bring complaints about this behaviour to the Privacy Commissioner and seek a remedy such as an award of damages. A criminal offence would be a further tool in addressing this issue; we consider it is appropriate to provide a criminal law response, given the serious nature of the behaviour and its consequences for the victim.

4.96 We have also taken account of the youth of many people tending to engage in such conduct. One question is whether it is appropriate to criminalise youthful behaviours. We are persuaded, however, that the implications of the more extreme types of behaviour are so serious that a criminal offence is warranted. Prosecutions would no doubt be reserved for the most serious cases; they would not be common among the lower age groups. However, the deterrent effect of a criminal penalty would clearly

173 Crimes Act 1961, Part 9A.

174 Summary Offences Act 1981, s 30.

175 Crimes Act 1961, s 216H.

signal the outer limits of internet freedoms.

4.97 We note that a new offence would be subject to certain limitations. For example an "intimate visual recording" is a recording made in private, rather than a public place.[176] The criminal law would not therefore respond to the publication of an intimate visual recording taken in a public place.

4.98 Another limitation is that the offence would apply only to the publication of intimate images by the person who created them. The offence will not therefore catch behaviours such as "sexting" where teens take intimate images of themselves and share them with others who may on-share the images more broadly than was expected. It will also not catch publication of an intimate image by someone other than the person who created it. For example one scenario might involve a partner of the image's creator posting an intimate image of their partner's lover on the internet to humiliate or intimidate them. While such scenarios could involve substantial harm and distress, we consider that it is appropriate to target the criminal publication offence (in cases where the picture was taken with the consent of the subject) to the creator of the image because of the serious breach of trust involved. Cases of publication without consent by third parties should be dealt through civil law mechanisms such as Privacy Act complaints and the tribunal remedies that we propose in the next chapter.

Threats to publish an intimate or objectionable image

4.99 We have also considered the case of *R v Broekman*, where a young man was prosecuted for making an objectionable publication, namely exploiting a female for sexual purposes.[177] In that case video footage was taken of an intimate sexual act by a 16-year-old girl.[178] Details were published on Facebook which, as we describe in chapter 2 of this report, caused a great deal of distress to the subject of the footage.[179] It is not clear whether it was the footage itself or an account of the incident that was circulated, leading to the devastating impact on the subject of the footage through being ostracised by her family and community.

4.100 The existing criminal offence in the Films, Videos, and Publications Classification Act 1993 proved sufficient in this case to successfully prosecute the offender. However, one issue which the case raises is whether threats to publish intimate or objective

176 Crimes Act 1961, s 216G.

177 Films, Videos, and Publications Classification Act 1993, s 124.

178 *R v Broekman* [2012] NZCA 213.

179 See Chapter 2, at [2.46] –[2.48].

pictures should be prosecuted. In some cases they could be now, but only if they are made to induce sexual activity,[180] or involve blackmail.[181] Possession offences may enable a prosecution to be brought.[182] If the threats are made by electronic communication, they would be caught by the new summary offence of offensive communication we recommend.

4.101 We are reluctant at this stage to recommend that a threat to publish intimate pictures should of itself be criminal, because this would involve considering whether a threat to commit *any* offence should itself be criminal. Currently it is not, and we think that would be to open the door too wide. Threatening conduct which does not fall within any current criminal offence, or the new ones we recommend in this chapter, will often be redressable in the civil courts under the Harassment Act 1997, and presently we prefer to leave matter there.

Recommendations: criminal law

R1 A new communications offence should be created in the Summary Offences Act 1981 as follows:

Causing harm by means of communication device

1. A person **(person A)** commits an offence if person A sends or causes to be sent to another person (**person B**) by means of any communication device a message or other matter that is –

   (a) Grossly offensive; or

   (b) Of an indecent, obscene, or menacing character; or

   (c) Knowingly false.

2. The prosecution must establish that –

   (a) person A either –

      (i) intended to cause person B substantial emotional distress; or

      (ii) knew that the message or other matter would cause person B substantial emotional distress; and

   (b) the message or other matter is one that would cause substantial emotional distress to a person in person B's position; and

   (c) person B in fact saw the message or other matter in any electronic media.

3. It is not necessary for the prosecution to establish that the message or other matter was directed specifically at person B.

180 Crimes Act 1961, s 129A.

181 Crimes Act 1961, s 237.

182 Films, Videos, and Publications Classification Act 1993, s 131; Crimes Act 1961, s 216I.

4. In determining whether a message or other matter is grossly offensive, the court may take into account any factors it considers relevant, including –

(a) The extremity of the language used:

(b) The age and characteristics of the victim:

(c) Whether the message or other matter was anonymous:

(d) Whether the message or other matter was repeated:

(e) The extent of the circulation of the message or other matter:

(f) Whether the message or other matter is true or false:

(g) The context in which the message or other matter appeared.

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

6. In this section, **communication device** means a device that enables any message or other matter to be communicated electronically.

R2 Section 179 of the Crimes Act should be amended so that incitement to suicide is an offence, regardless of whether the recipient proceeds to commit suicide or not, by deleting the words "if that person commits or attempts to commit suicide in consequence thereof".

R3 A new section 131C should be added to the Crimes Act making it an offence to expose a young person to indecent material or provide an intoxicating substance to a young person with the intention of making it easier to procure the young person for unlawful sexual activity with him or her or any other person.

R4 The intimate covert filming provisions in Part 9A of the Crimes Act 1961 should be extended to provide a further offence in section 216J:

A person (person A) who takes a visual recording of another person (person B) with person B's knowledge or consent is liable to [imprisonment for a term not exceeding 3 years] if –

(a) person A publishes the recording without person B's consent; and

(b) the recording is of a kind described in section 216G(1)(a) or (b) and would be an intimate visual recording if taken without person B's knowledge or consent.

Civil law reforms

4.102 Our review of the civil law has led us to conclude that it would be desirable to make certain targeted amendments to the Harassment Act, the Privacy Act and the Human Rights Act, to clarify the application of those laws in online contexts.

The Harassment Act 1997

4.103 The Harassment Act provides for the restraining order.[183] The Act is now 15 years old

183 Harassment Act 1997, Part 3.

and while it has been utilised in cases of harassing electronic communication with some creative interpretation, we think amendments are needed to remove any doubt or uncertainty that it applies to electronic communications. This would ensure that the Act is capable of responding to the challenges of online harassment, and that it is clear on its face that it does so.

4.104 We recommend four changes.

Expressly including electronic communications as a specified act of harassment

4.105 First, one of the items in the list of specified acts in the definition of harassment is:[184]

> making contact with that person (whether by telephone, correspondence or in any other way)

This can doubtless be interpreted as including electronic communications but given that telephone and correspondence are expressly itemised it would be appropriate to add electronic communications to the means of making contact and we recommend accordingly.

4.106 Secondly, paragraph (e) of the definition provides that another specified act is:

> giving offensive material to that person, or leaving it where it will be found by, given to, or brought to the attention of, that person

This phraseology seems particularly appropriate to hard copy. It requires a liberal interpretation to hold that it covers such things as false Facebook pages or comments placed on a blog which has not been directly sent to the subject but may come to his or her attention.

4.107 In a recent District Court case, Judge Harvey was of the view that blog comments can fall within the paragraph where the blogger is *aware* that the material will come to the attention of the victim or it is *reasonably foreseeable* that the victim would access the material.[185] In this case it was reasonably foreseeable that, having become aware of the existence of offending posts, the victims would continue to visit the blog to see if they had been removed, and in so doing would have discovered further offensive posts.

4.108 While the current provision is therefore capable of covering electronic communications such as blog posts, it would be useful, in our view, if the statute was explicit about this. An explicit provision would assist to raise awareness of the law and make clearer to bloggers and to the community the potential liability that may arise in making offensive comments online.

184 Harassment Act 1997, s 4(d).

185 *Brown v Sperling* DC Auckland CIV-2012-004-00925, 15 June 2012 at [204]-[209].

4.109 We recommend a separate paragraph in the section to the following effect:

> Places offensive material in any electronic media and either the victim views that material, or it is reasonably likely that it will be brought to his or her attention.

Continuing acts as a pattern of conduct

4.110 Thirdly, section 3 of the Harassment Act requires that to constitute harassment there must be "a pattern of behaviour", and that this includes "doing a specified act on at least two separate occasions within a period of twelve months".[186] Yet a single internet posting which continues for a lengthy period causes as much, or perhaps even more, damage and distress than two discrete individual acts.

4.111 The Law Commission considered this question as part of its review of the law of privacy, recommending that section 3 be amended so that a pattern of behaviour can be constituted either by a single protracted act, as well as two or more specified acts within 12 months.[187]

4.112 We continue to support that recommendation and consider that just as a single protracted act of surveillance should qualify as a specified act of harassment, similarly a single offensive internet posting that persists over a period of time should also qualify as potential harassment.[188] The implementation of the earlier Law Commission recommendation would address the issue in both contexts.

4.113 We see no need to prescribe any particular length of time that a specified act of harassment must persist. A restraining order can only be made when distress is caused; this is a sufficient criterion.

Effect of restraining order

4.114 Fourthly, section 19 of the Harassment Act prescribes the effect of a restraining order. It provides that it is a condition of every restraining order that the respondent must not:

> Do, or threaten to do, any specified act to the person for whose protection the order is made

While this may be interpreted to cover the cessation of continuing conduct, it is not the most natural meaning of the words. We therefore recommend that the section be

---

186 Harassment Act 1997, s 3.

187 Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC R113, 2010) at R22. The government is due to respond to the recommendations in this report in September 2012.

188 There is precedent in Queensland, where the Criminal Code provides that to constitute of the offence of stalking all that is required is conduct "engaged in on any one occasion if the conduct is protracted": Criminal Code 1899 (Qld), s 359B.

amended to provide that it also be a condition of a restraining order that the defendant must take all reasonable steps not to continue any specified act. The 'reasonable steps' qualifier is necessary because the defendants may not be able to remove the content from all parts of the internet where it may have been cached or archived.

The Privacy Act 1993

4.115 The Privacy Act 1993 regulates the handling of personal information about people, and privacy principle 11 restricts the disclosure of personal information, including online disclosures.

News medium: qualifying conditions

4.116 The Privacy Act's information privacy principle 11 provides that an agency holding personal information about a person should not disclose it to anyone else unless one of a number of exceptions applies. A "news medium" is not an agency for this purpose and therefore does not need to comply with the requirements of principle 11.

4.117 There is presently some debate about the boundaries of that expression. The Law Commission recommended as part of its review of the law of privacy that the term "news medium" should include only those media which are subject to a code of ethics and subject to a complaints body.[189]

4.118 We discussed the question of news media exemptions more widely in part one of the Issues Paper in the present reference,[190] and will return to it in our final report on that reference. If "news medium" is to be defined in this narrower way, disclosures of personal information in the electronic media which fall outside that definition will not have the benefit of the news media exemption. This would mean that such disclosures will need to comply with the requirements of principle 11 and will be subject to the jurisdiction of the Privacy Commissioner. We consider that would be appropriate.

4.119 Even if that issue is resolved however, there remain two further Privacy Act exceptions that can significantly reduce the protections available to persons whose privacy is damaged by internet publications.

---

189 Law Commission *Review of the Privacy Act: Review of the Law of Privacy Stage 4* (NZLC R123, 2011) at R38.

190 Law Commission *The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age* (NZLC IP27, 2011) chapter 4.

Publicly available publication and domestic affairs exceptions

4.120 First, it is an exception to information privacy principle 11 that "the source of the information is a publicly available publication". According to Professor Paul Roth, New Zealand has an extremely broad exemption for "publicly available information".[191] Its effect in an online context is that once personal information, even deeply sensitive personal information, is published once on the internet, no-one can be liable for increasing its circulation by publishing it on other sites.

4.121 Secondly, section 56 of the Privacy Act provides that:

> Nothing in the information privacy principles applies in respect of
>
> (a) the collection of personal information by an agency that is an individual; or
>
> (b) personal information that is held by an agency that is an individual,
>
> where that personal information is collected or held by that individual solely or principally for the purposes of, or in connection with, that individual's personal, family or household affairs.

4.122 This has been described as a "crucial exception":[192]

> It allows a vital "social" space within which individuals may conduct themselves without fear of breaching the strictures of information privacy laws.

4.123 But arguably the breadth of this exception also needs some outer limits. Currently it means that intimate pictures taken in the context of a domestic relationship may be exempt from the Privacy Act principles, including principle 11, even if they are later published on the internet, perhaps on the breakdown of the relationship.[193]

4.124 As part of its review of the Privacy Act, the Law Commission considered the breadth of these exceptions and recommended:

(a) The "publicly available publication" exception should not be available where the use or disclosure of publicly available information would be unfair or unreasonable;[194]

(b) The "domestic affairs" exception should not be available where the personal information has been collected unlawfully, through misleading conduct, or where

---

191 Paul Roth *"Data Protection Meets Web 2.0: Two Ships Passing in the Night"* (2010) 33 UNSW Law Journal 532 at 545.

192 Gehan Gunasekara and Alan Toy "MySpace" or "Public Space" [2008] 23 NZULR 191 at 213.

193 For discussion of the scope of the "domestic affairs" exception see Paul Roth *"Data Protection Meets Web 2.0: Two Ships Passing in the Night"* (2010) 33 UNSW Law Journal 532 at 536-544.

194 Law Commission *Review of the Privacy Act: Review of the Law of Privacy Stage 4* (NZLC R123, 2011) at R10.

the use or disclosure of the information would be highly offensive to an objective reasonable person.[195]

4.125 We continue to support these recommendations and consider that they would be useful in addressing online communication harms that significantly impact on a person's privacy. The "unfair or unreasonable" threshold imposed in relation to the "publicly available publication" exception is lower than the "highly offensive" threshold for the domestic affairs exception. Regardless of the particular threshold however, complaints may only be made if a breach causes "significant humiliation, significant loss of dignity or significant injury to feelings".[196]

The Human Rights Act 1993

4.126 Section 61 of the Human Rights Act 1993 provides that it is unlawful to publish matter which is likely to excite racial disharmony. We have been told by the Human Rights Commission that the threshold for liability under this provision is so high that it is almost never met. Any amendments to this provision would be a matter for review of the Human Rights Act, and is beyond our present scope. But when this exercise is undertaken we recommend that the section, which currently expressly refers to written matter and broadcast matter, should also, to avoid any doubt, refer to electronic communications as well. We also believe that, when such a review takes place, consideration should be given to extending the disharmony provisions to cover insulting or abusive conduct relating to religion, ethical belief, gender, disability and sexual orientation as well as race.

4.127 Sections 62 and 63 deal with sexual and racial harassment respectively. They provide that such harassment must have a detrimental effect on the person in relation to a number of specified benefits including access to goods and services and education. Harassment of the kinds with which these sections deal has the potential to deter individuals, particularly young people, from using social media, thus limiting their interaction with their peers. Perhaps that is covered by the access to goods and services provision,[197] but not clearly and unarguably so.

4.128 We believe the matter is significant enough to justify adding a further item to the list of benefits which can be affected by the harassment "participation in any fora in the electronic media for the exchange of ideas and information".

---

195 Ibid, at R45.

196 Privacy Act 1993, s 66(1)(b)(iii).

197 Human Rights Act 1993, s 62(3)(h), s 63(2)(h).

Recommendations: civil law

R5 We recommend the following amendments to the Harassment Act:

(a) An amendment to section 4(1)(d) so that it is explicit that making contact with a person can include electronic communication;

(b) The addition of a further "specified act" of harassment in section 4 to the following effect:

> "giving offensive material to a person by placing the material in any electronic media where it is likely that it will be viewed by, or brought to the attention of, that person."

(c) An amendment to section 3 to provide that a continuing act over a protracted period is capable of constituting harassment (as recommended in the Law Commission's Invasion of Privacy report).

(d) To make a condition of a restraining order that applies to a continuing act that the respondent must take reasonable steps to prevent the specified act from continuing.

R6 We recommend the following amendments to the Privacy Act:

(a) An amendment to the "publicly available publication" exception in information privacy principle 11 so that the exception is not available where the disclosure of personal information obtained from such a publication would be unfair or unreasonable (as recommended in the Law Commission's Privacy Act report);

(b) An amendment to section 56 so that the "domestic affairs" exception is not available where the disclosure of personal information would be highly offensive to an objective reasonable person (as recommended in the Law Commission's Privacy Act report).

R7 We recommend the following amendment to the Human Rights Act:

(a) Section 62 (sexual harassment) and section 63 (racial harassment) should be amended to include an additional area of application:

> "participation in any fora in the electronic media for the exchange of ideas and information".

(b) Section 61 (racial disharmony) should be amended to refer to electronic communications, in addition to other forms of publication.

CONCLUSIONS

4.129 We have reached the view that changes in the law are necessary and desirable. We note the comment of the Police in their submission to our issues paper:

> Police considers the current law is not always capable of addressing some of the new and potentially more damaging ways of using communication to harm others. This, combined with the practical difficulties of investigating offensive conduct over the Internet, can lead to very real difficulties in enforcing the law against 'new media'.

4.130 No-one believes that creating new law will itself solve the problem of cyber-bullying and harmful communications. The causes of that problem are complex, and the

solutions to them are social and educational as well as legal. Sometimes the offensive communications with which we are dealing are part of a wider pattern of conduct. Enforcement of the law through the courts can also be problematic and unrealistic, particularly in the case of young persons.

4.131 However, the law does have an important part to play. The prosecution of even a few offenders serves as a warning to others. Moreover the law is an authoritative public statement of what is and what is not acceptable in the eyes of society and the mere fact of its existence serves as a deterrent. It is supportive to victims to know that if the conduct to which they are being subjected is serious enough, the law enforcers, namely the Police and the courts, are available at the end of the line. It is also helpful to those dealing with perpetrators, particularly young people, to have the backing of the law. And the law enforcers, the police in particular, welcome clarity in the law.[198]

4.132 Uncertainty as to whether a particular provision covers the case is not conducive to swift action. As context and society change, and the harms to which people are subjected change, the law must change too.

4.133 It may be argued that the threshold for creating a new criminal offence is, and should be, a high one, and that some of the matters for which we recommend criminalisation might be more adequately dealt with through other channels. One commentator, while acknowledging that online communications can have such harmful consequences that criminal sanctions are justified, expresses concern about laws that are overly expansive and catch communications that do not deserve the heavy penalties imposed by the criminal law, suggesting that such laws should be tailored to deal with the most serious and deliberate cases of harassment or bullying, and noting the chilling effect of broadly worded criminal offences.[199]

4.134 We have been mindful of this caution and have been careful to put forward tailored amendments to our laws that include suitably high thresholds so that only those communications that have cause serious harms come within their scope. We have given careful thought to the threshold for criminality, and the requirements of the Bill of Rights Act, in defining the offences. We note that most of our recommendations

198 In their submission to our issues paper the Police supported the introduction of new offences, referring particularly to an "offensive communication" offence, malicious impersonation, publication of intimate photos, and incitement to suicide: submission of the Police (March 2012) at 4.

199 Jacob H Rowbottom "To Rant, Vent and Converse: Protecting Low Level Digital Speech" (2012) 71 CLJ 355.

mirror developments in other jurisdictions.[200]

4.135 We are conscious of the fact that there has been a recent tendency to decriminalise what were formerly speech offences. The abolition of criminal defamation and sedition are recent examples. What we propose is not in conflict with that movement. Sedition was about political speech. Criminal defamation was always an exceptional category in which a prosecution was only authorised if the public interest required that it should proceed. The public as well as the private interest was central to this part of this law.

4.136 As we noted earlier in this paper, overseas jurisprudence increasingly recognises differences in the value of different kinds of speech. Political speech is seen as being of the highest importance, gratuitous personal attacks and "hate speech" the lowest, although even there the reaction of the law must not be disproportionate: freedom of speech is too important.[201] We are concerned about protecting citizens from substantial mental and sometimes physical harm caused by communications of the two latter kinds. We are concerned with creating a safer environment for people. We are satisfied that that objective is serious and important enough to be supported by the criminal law. In terms of the New Zealand Bill of Rights Act 1990, the exceptions to freedom of expression that we advocate are "justified in a free and democratic society".[202]

4.137 Finally we note that the laws controlling harmful communications will be reflected in the principles which will be applied by the new tribunal which we discuss in the next chapter of this report. That body will have no power to impose criminal sanctions, but will be empowered to take remedial measures to protect victims. The availability and accessibility of appropriate non-criminal remedies is important to ensure that there is a balanced approach, and that the criminal law is reserved for the most serious cases. Our objective of creating a safer environment for people will be developed further in the next chapter.

200 See above at [4.73].

201 Jacob H Rowbottom "To Rant, Vent and Converse: Protecting Low Level Digital Speech" (2012) 71 CLJ 355.

202 New Zealand Bill of Rights Act 1990, s 5.

Chapter 5: Enforcement

ISSUES PAPER AND SUBMISSIONS

5.1 As we noted earlier, the law provides a vital anchor for the values and principles by which our society operates. There are many legal rules now which are capable of redressing many of the harms resulting from online communications. From time to time there are successful prosecutions and civil actions. But in order to be truly effective in reinforcing those values and principles the law must be accessible to the public and be capable of providing speedy and meaningful redress.

5.2 This is true with respect to all types of wrong-doing and a number of submitters to our review commented that our discussion about the barriers to accessing justice were not restricted to communication offences. We accept that argument. But as we pointed out in our issues paper there are some unique challenges in applying the law in cyberspace. While the existing criminal and civil law could deal with many types of harmful digital communications, in practice there are a number of obstacles that impede access to justice by those who have suffered harm. These include:

(a) A lack of knowledge of the law and/or the availability of redress, by both victims and enforcement officers;

(b) The complexity of identifying possible defendants in an online situation;

(c) The breadth and speed of spread of information on the internet;

(d) Problems of establishing jurisdiction, where material is hosted overseas.

5.3 Submissions confirmed the themes that had emerged from our preliminary research and consultation as to the problems people encounter in accessing help to deal with cyber offending, and their resulting sense of powerlessness.

5.4 The Police advised that one of the problems they faced in responding to complaints about communications abuses, which increasingly involve social media and online fora, is that not all of the harms reported meet the threshold of a criminal offence, or indeed constitute any sort of offence under the current law. They submitted that nevertheless these harms are frequently significant, and supported the proposal to enhance and strengthen existing laws to make them fit for purpose, as well as introducing a number of new offences.

5.5 But even where there are already appropriate laws to deal with harmful communications, there are still significant flaws in the present system of enforcement.

In summary, these are the cost of bringing proceedings, the time taken by traditional systems of enforcement to deal with the issue, and the complexity of gathering evidence and establishing proof.

5.6 In his submission, Judge Harvey identified the main source of the problem as being one of process, rather than the effectiveness and availability of remedies, and raised three key issues:[203]

(a) legal processes do not operate within "internet time", when information is disseminated virally and globally within minutes:

> Significant damage may be done in the time that it takes to bring civil proceedings to a hearing – even in the case of an injunction.

(b) the cost of civil proceedings and restrictions on legal aid place access to the civil jurisdiction of the courts beyond the reach of many ordinary citizens – and given the evidential and legal complexities that surround litigation of "online" matters, self-represented litigants face a daunting task;

(c) there are difficulties in bringing a criminal prosecution primarily because the evidence gathering process can be complex and multi-jurisdictional, and police investigative resources are limited.

5.7 In its submission, NetSafe also referred to the problems of bringing a criminal prosecution, noting it could be time-consuming and difficult for law enforcement to collect the level of digital evidence required to successfully prosecute the offender, particularly where hosts of harmful communications are based overseas. Even when such evidence can be accessed, prosecution is further complicated by the need to prove that the abuse was produced by the alleged offender (and not someone else who happened to use their IP address or login at that time).

5.8 In NetSafe's experience, the majority of interventions by the law usually occur on an informal, ad hoc basis and involve police officers contacting the alleged offenders and requesting that the threats of harm desist.

5.9 NetSafe also echoed Judge Harvey's concerns about the costs and timeliness of court proceedings in the context of harmful digital communications:

> When it comes to speech abuses that are not covered by the criminal statutes, practical opportunities for the law to produce redress are nearly non-existent for the majority of the public who do not command the financial resources to be able to take the matter through civil proceedings.
>
> The inability of the law to effectively help targets of such abuse mainly centres on the likelihood of action and the time required for such actions to be taken. The longer abusive content remains online

203 Submission from Judge David Harvey at 11.

> the increased chance of distress and victimisation is for targets of such speech abuses. Other than when police officers act informally, it is unlikely the law can produce redress in a time frame that is effective for the targets of such abuse. This issue is particularly salient for targets of abuse that relies on diminishing their social standing, for the longer such material remains online, the more damage it can do to the target's social network.

The proposals in our issues paper

5.10 In our Issues Paper we reached the preliminary conclusion that there was a need for some mechanism by which those who had been harmed by digital communication could be assisted in resolving their disputes and/or be given access to a specialist court capable of administering speedy, efficient and relatively cheap remedies.[204] We sought feedback on two alternate preliminary proposals for achieving these objectives.

A Communications Tribunal

5.11 The first proposal was for the establishment of a Communications Tribunal that would operate like a mini-court dealing with cases where demonstrable harm has resulted or is likely to result.[205] That harm might be financial, or might be psychological harm such as distress, intimidation, humiliation or fear for safety. The tribunal would only deal with cases where it judged the offending content amounted to a breach of the law.

5.12 The tribunal's functions would be protective, rather than punitive. Its job would be to provide remedies for the victim rather than mete out punishment for perpetrators – the power to impose criminal sanctions should be reserved for the courts not a specialist tribunal of this sort.

5.13 However we proposed that the tribunal would have the power to impose a number of sanctions and remedies, including the ability to award monetary compensation up to a prescribed level; to order publication of an apology or correction; to order that a right of reply be granted; to order that the defendant cease the conduct in question (a type of injunction); and (after a fair hearing) to make takedown orders against either the perpetrator or an innocent avenue of communication such as an internet service provider (ISP). It might also make a declaration that statements made about the victim are untrue. Failure to comply with an order would be an offence.

204 Law Commission *The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age* (NZLC IP27, 2011) chapter 8.

205 Ibid, at [8.43]-[8.77].

A Communications Commissioner

5.14 The second option we put forward for discussion was the establishment of a Communications Commissioner, possibly attached to the Human Rights Commission.[206] The Commissioner would not have the enforcement powers of a tribunal but his or her role would be to provide information and where possible assist in resolving problems in an informal manner, for example through mediation. Where appropriate, he or she could also make recommendations to responsible authorities and individuals with the aim of preventing problems or improving the existing situation. In cases of serious harm, the Commissioner may refer a complainant to the police. In other cases, many of the harms that we have discussed could be resolved informally by a person with some authority contacting a website administrator to draw their attention to objectionable material, identifying the harm the post is causing, or how it may be in breach of the law.

What submitters said

5.15 The great majority of submitters supported the proposition that there needed to be some domestically based and authoritative mechanism for assisting people to resolve disputes and address serious harms caused by abusive digital communication.

5.16 Among the few exceptions was Google, which reiterated its belief that harmful speech online was best addressed through existing legal and self-regulatory mechanisms and that a Communications Tribunal would be a "disproportionate response to an as yet ill-defined problem".[207] Its objection to a Communications Commissioner, with lesser powers, was more muted and indeed it accepted that such a body may have some merit "in some limited circumstances". It pointed out that NetSafe, an organisation whose work it strongly endorsed, was already carrying out many of the functions outlined for the proposed Commissioner.[208]

5.17 Facebook shared Google's conviction that "user empowerment" combined with a "robust site reporting infrastructure and technology" were the most effective responses to online communication abuses, but it did not directly oppose the idea of a Commissioner or Tribunal. It was however concerned to ensure any investigative or enforcement powers vested in a tribunal were consistent with its own established

206 Ibid, at [8.78]-[8.85].

207 Submission of Google New Zealand Ltd (14 March 2012) at 30.

208 Ibid, at 27.

protocols for responding to legal requests for account holder information and escalations of serious legal harms or threats which occurred on their platform.[209]

5.18 Google and Facebook's preference for non-regulatory solutions reflect what a submitter described as "the inherent tension between the need for corporate accountability and the right of private commercial sectors to self-regulate within the operation of the law".[210]

5.19 And, as these submitters went on to point out, these tensions have taken on a whole new dimension as a result of the unique place Facebook inhabits: [211]

> In 2011, the official user count for Facebook was reported to be a monumental 854 million (monthly users); more populated that the average nation-state, yet the entity is largely free to determine guidelines and balances considerations for multiple jurisdictions against its own (user) interests. This observation does not purport to be a pretext to suggest active online-forum or corporate regulation, yet it points to an eerie lack of uniform regulatory governance for such online mediums.

5.20 The Equal Justice Project concluded that there would inevitably be tensions between the non-legislative remedies employed by online communities and the judicial and legislative remedies in place within domestic jurisdictions. However, it was clear that "whatever form this coexistence may take, users need a complaint body that is direct and accountable" and that has the "power to demand negotiations".

5.21 The principle that New Zealand users need access to a complaints body that is accessible and that has some teeth to negotiate with global entities was endorsed in the submissions of key stakeholders including Police, the Human Rights Commission, the Post Primary Teachers' Association, the Privacy Commissioner, NetSafe and Trade Me.

5.22 In its submission NetSafe clearly articulated the benefits it saw flowing from the establishment of a tribunal and/or a Commissioner.[212] These included:

(a) Lowering the barrier for victims looking for redress because a tribunal would not require proof "beyond reasonable doubt" and would operate cheaply and on much faster time frames than traditional courts, thereby providing meaningful remedies;

209 Submission of Facebook (14 March 2012) at 9.

210 Submission of the Human Rights division of the Equal Justice Project, Faculty of Law, University of Auckland (received 30 March 2012) at [3.1].

211 Ibid.

212 Submission of NetSafe (24 February 2012) at 4.

(b) Providing a deterrent effect for offenders who currently feel empowered by the barriers to successful prosecution and the very real belief they will not be sanctioned in any way;

(c) Providing an incentive to resolve disputes at an earlier stage to avoid referral to a tribunal – NetSafe argued that if any agency were empowered to work with victims and alleged offenders to resolve complaints though mediation and negotiation this would both incentivise parties to resolve issues, and also provide a filter, ensuring only serious cases were referred to a tribunal for adjudication;

(d) Allowing for the productive engagement of industry partners – NetSafe argued that the pre-tribunal triaging of complaints would allow other agencies and organisations, including schools, to become engaged in the resolution of problems;

(e) Speeding up the responses from content hosts and infrastructure companies by providing a "national contact" point mandated to liaise directly with the influential internet companies and organisations whose co-operation would be required to give effect to notice and takedown orders and obtain information about the identity of anonymous authors etc.

Tribunal or Commissioner model

5.23 In our Issues Paper we presented the proposals for a Communications Tribunal or a Commissioner as alternate options.[213] Some submitters, including NetSafe, saw merit in the two working in tandem – the Commissioner as a mediator and filter for the tribunal. Other submitters expressed a clear preference for one over the other.

5.24 Those who preferred a Commissioner to a tribunal usually did so for two reasons: a belief that the Commissioner model was less legalistic and more flexible, and more likely to be able to mediate solutions and a concern that the alternative tribunal was overly interventionist and risked compromising critical free speech rights online.

5.25 InternetNZ for example argued that in the first instance at least, a Commissioner, with a mandate to educate and mediate, would be a suitably "light touch regulation" with the option of for a "stronger response if the light touch doesn't work over time".[214] It argued that "more empirical evidence of harms and the inadequacy of current redress mechanisms" was required before taking an "expensive and complex step with

213 Law Commission *The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age* (NZLC IP27, 2011) at chapter 8.

214 Submission of InternetNZ (12 March 2012) at 10.

potentially toxic side effects."

5.26 Other submitters were more concerned about how the proposed tribunal would work in practice and whether in order to deliver speedy justice it would inevitably compromise vital legal principles such as the rights of defendants to raise a defence.

5.27 Fundamentally too, some argued whether it was in fact possible (let alone desirable) to short-circuit the necessarily complex legal arguments involved in assessing alleged defamations or privacy breaches. A number also raised concerns about how the tribunal's determinations would impact on the rights of defendants in any future criminal proceedings which may eventuate further down the line.

5.28 In its submission, the Dunedin Community Law Centre cited the concerns expressed by barrister and media law expert Steven Price about the dangers of a parallel legal process and the challenges a tribunal would face:[215]

> Issues around what constitutes free speech and defamation are complex, and will be difficult to establish fairly, speedily and efficiently through a Tribunal process.

5.29 For this reason, these submitters preferred the Commissioner model, arguing that in cases of serious harm the Commissioner could refer the matter to the Police for investigation and prosecution through the courts in the normal manner.

5.30 Some endorsed the suggestion in the Issues Paper that a Communications Commissioner might be attached to the Human Rights Commission, an organisation which was already accustomed to balancing free speech issues against other human rights questions.

5.31 For its part the Human Rights Commission acknowledged that it already had the ability to deal with freedom of expression issues and had good relations with other agencies that have a role in regulating media. However it emphasised that if its mandate were to be extended to deal with more generalised speech harms this would require funding and resources to support this role. The Human Rights Commission also commented that the Commissioner may be cheaper but it was also weaker as it would not have the enforcement powers of the proposed tribunal.[216]

5.32 While the Human Rights Commission said it favoured the tribunal option because it had more teeth, it also expressed concerns about the difficulties the tribunal would encounter in establishing evidence of "demonstrable harm" – the proposed threshold

215 Submission of the Dunedin Community Law Centre (12 March 2012) at 6.

216 Submission of the Human Rights Commission (12 March 2012) at [8.3].

required before it would take action:[217]

> As we have already indicated, this will not always be easy to demonstrate particularly in relation to the relevant sections of the HRA [Human Rights Act]. Humiliation, loss of dignity and injury to feelings, for example, is the head of damages most frequently relied on under the HRA and the most difficult to establish with any precision.

5.33 The New Zealand Police also favoured a tribunal with enforcement powers but no ability to impose criminal sanctions. It emphasised the importance of giving the tribunal the power to require an internet service provider or other content hosts to disclose the details of an account holder, noting that the "co-operation of the ISP cannot always be relied upon".[218] In the view of Police, removal of the infringing material was crucial in order to prevent further victimisation.

5.34 In a similar vein Trade Me argued in favour of a tribunal because it would have investigative and enforcement powers and would play an influential role in establishing the parameters of acceptable behaviour:[219]

> [S]uch a tribunal will build up a strong set of case law about what is "reasonable" and "responsible" which will be useful in indicating where the line of good practice is, delivering better overall behaviour but also less frivolous or unrealistic claims.

5.35 With respect to the alternative proposal for a Commissioner, Trade Me noted that NetSafe already carries out many of the functions proposed for the Commissioner and has already forged many of the critical relationships with intermediaries and content hosts like Facebook and Google. It suggested that "greater resourcing of this function would be preferable to setting up a Commissioner."[220]

RECOMMENDED MODEL: TRIBUNAL PLUS APPROVED COMPLAINTS HANDLING BODY

5.36 We are persuaded by the research we have undertaken, the submissions we have received and the comments of agencies such as NetSafe and the Police, that harmful cyber communications constitute a real problem in today's society, and that the present modes of law enforcement are not adequate to deal with them. The courts are often not a realistic option for people who want swift and effective redress. We believe that there needs to be an appropriate mechanism to provide relief outside the

217 Ibid, at [7.4].

218 Submission of New Zealand Police (12 March 2012) at 5.

219 Submission of Trade Me (12 March 2012) at [46].

220 Ibid at [48].

traditional court system. Such an innovation was supported by many of the submissions we received on the subject.

5.37 This would not be out of place in the New Zealand legal system. The Privacy Act 1993 provides redress outside the court system for invasions of privacy, and the Human Rights Act 1993 for discriminatory behaviour. The Broadcasting Act 1989 provides remedies for people who have been adversely affected by breach of a range of broadcasting standards including the standard that broadcasters must treat people fairly. The harm and distress caused by some online communications is at least as great as, and sometimes greater than, the harms targeted in these statutes. We have outlined some striking instances in chapter 3. We believe that a speedy and informal system of resolving problems in the online environment will support not only victims, but also families, schools and others who have to deal with and advise on harmful online behaviour and its consequences.[221]

5.38 We believe that such a system should have a number of characteristics:

(a) It should be well publicised.

(b) It should be easily accessible.

(c) It should operate as informally as possible.

(d) It should operate quickly.

(e) It should be inexpensive to those using it.

5.39 So what should the new machinery be? Having put forward two alternatives in the issues paper – a tribunal with power to make enforceable orders or a commissioner with persuasive rather than coercive power – we have formed the view that a tribunal is justified. As we pointed out in the issues paper, New Zealand has often resorted to this method of dispute of resolution: the Human Rights Review Tribunal, the Tenancy Tribunal and the Disputes Tribunal are well known examples.[222] The advantages of tribunals are exactly those that we list in paragraph 5.38 above: they provide justice which is accessible, informal, speedy and inexpensive. The tribunal solution has the support of a number of significant organisations including NetSafe, the Police and the Human Rights Commission. When answering the question in the issues paper Trade Me said "absolutely", noting the importance of speed and responsiveness.

---

221 For commentary on a low cost regulatory approach to digital communications, see Jacob H Rowbottom, "To Rant, Vent, and Converse: Protecting Low Level Digital Speech" (2012) 71 CLJ 355.

222 Law Commission *The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age* (NZLC IP27, 2011) at [8.45].

5.40 A tribunal would provide a backstop for other agencies – such as NetSafe – which attempt to resolve issues of this kind. It would also give a legal authority which would be useful to schools, the Police and other agencies. It would have the added value that its determinations would likely be recognised as authoritative by large overseas website hosts and service providers which, even though not resident within our jurisdiction, would regard such these determinations as sufficient reason to take the required action in respect of the offensive communications. In the current absence of such an entity it can be difficult to get such an action.

5.41 But before proceeding to outline the features of the proposed tribunal, a preliminary question needs to disposed of. Given that the main relief which is likely to be sought by most complainants is an order to takedown or discontinue the offensive conduct, might the Harassment Act 1997 as currently applied in the District Court not be enough? It gives power to the District Court to make a restraining order in relation to various forms of harassment. If that Act were to be subject to the minor amendments we have suggested in the previous chapter, it might be argued that it is adequate to be the kind of backstop we are suggesting. We do not favour this solution. As the enforcement authority under the Harassment Act, the District Court acts under the rules of court (adapted for the purpose of the Act)[223] and is subject to all the incidents of its ordinary jurisdiction.

5.42 The advantages of a specialist tribunal will be that it would develop specialist knowledge not just about communications law but also about the developing communications technologies. It would also have the usual advantages of a tribunal over a court in that it could act quickly, informally and relatively inexpensively. It would mitigate the effects of wealth imbalance between the parties. There is the further advantage that orders under the Harassment Act cannot be made against minors under 17;[224] we would anticipate that sometimes a tribunal order might be appropriate against young persons.

5.43 This tribunal would be less formal machinery than the ordinary court system. It would also be able to build up a body of consistent precedent in its specialist field. Nevertheless there might remain cases where a complainant would prefer to use the Harassment Act route. That might be particularly so where the harassment involves a variety of types of conduct or where the harassment reaches the threshold of criminal

223 Harassment Act 1997, s 42; District Court Rules 2009, Part 7.

224 Harassment Act 1997, s 12.

harassment.[225]

5.44 So we support a tribunal model. But the tribunal alone will not be enough. A very large number of cases may not need a tribunal: they may be able to be resolved by some form of alternative dispute resolution. Particularly in the case of young persons this will often be greatly preferable to a hard-hitting judicial resolution. Moreover, if the tribunal were to be the only mechanism it might be flooded with complaints, some of them of a relatively minor kind. There needs to be some way of controlling what reaches the tribunal. So in addition to the tribunal there needs to be a process or machinery to receive, 'filter' and try to resolve complaints before the tribunal's jurisdiction is activated. For a time we were of the view that a Commissioner of the kind we discussed in the issues paper might be the answer. This would in fact involve adopting both of the issues paper options, rather than treating them as alternatives. The Commissioner would attempt to mediate a solution; the tribunal would be activated if those measures failed.

5.45 However, particularly in the present fiscal climate, "the Commissioner plus tribunal" model could involve heavier new machinery than may be necessary or desirable. We are therefore recommending a similar but less formal structure. We think that the preliminary filtering and negotiation functions (which we regard as essential) should be undertaken by an existing body or bodies which would receive formal ministerial approval to undertake them. The non-governmental organisation NetSafe currently does such work and would seem to us to be an outstanding candidate for such approval. So in essence the scheme we recommend is a two-step mechanism whereby:

(a) Complaints about offensive internet communications would go initially to an "approved agency" like NetSafe which would advise complainants and attempt to achieve a resolution by a process of negotiation, mediation and persuasion.

(b) If a complaint cannot be resolved in this way, provided the threshold of seriousness is reached, it might then proceed to a tribunal which can make enforceable orders. To that extent the tribunal would serve as a 'backstop' where dispute resolution procedures have failed or are unsuitable.

5.46 Nothing in all of this, of course, will affect the criminal law. In really serious cases that law should remain as the ultimate sanction, sometimes in parallel with the tribunal process. The purposes served by the two are different.

5.47 We now proceed to discuss the two elements in this scheme. We shall deal with the

225 Harassment Act 1997, s 8.

tribunal first. In what follows we acknowledge the assistance we have derived from the writings and presentations of Steven Price, who commented helpfully on the proposals in our issues paper.[226]

The Tribunal

Who would the tribunal be?

5.48 The tribunal could be a Judge, or other person of legal experience and standing. It would be important for the job description for the position to include, in addition to expertise in communications law, an understanding of the New Zealand Bill of Rights Act 1990. Understanding and empathy with young people would also be an advantage, for some but by no means all of the cases would involve young participants.

5.49 Even more importantly, the tribunal should have an understanding of communications technology. Ideally the tribunal itself should have a degree of expertise in that subject. One of the submitters to our Issues Paper said colloquially that some of people working for the tribunal should be "Gen Y".[227] "They need to demonstrate that they are well versed in different forms of social media". However, it might be enough in an appropriate case for the tribunal to sit with an expert technical adviser.

5.50 Although each case would be heard by a single tribunal member, as for example is the case in the Disputes Tribunal, there might be a number of persons designated for the role to meet the exigency that would otherwise arise if one appointee was unable to hear a particularly urgent case. We are attracted to the idea of designated District Court judges undertaking the task, because there would then be no need to build a new tribunal structure. The support services would already exist. There is a useful precedent in the Victims' Special Claims Tribunal set up under the Prisoners' and Victims' Claims Act 2005.

The type of communication

5.51 The tribunal jurisdiction would extend to all forms of electronic communication. It

---

226 Steven Price, "A heroic – but slightly defective – plan to save the online world" NZ Lawyer (online ed, 18 May 2012) <www.nzlawyermagazine.co.nz>. See also the IT Countrey Justice blog "Dealing with Speech Harms – A Commentary of Steven Price's Answer to the Law Commission" (5 June 2012) <theitcountreyjustice.wordpress.com>.

227 Gen Y or Generation Y is generally considered to be the generation born between about 1983 and 2004, a generation which is marked by an increased use of and familiarity with communications, media and digital technology.

would include comments on websites, message boards and blogs, in social media (e.g. Facebook and Twitter), and also emails and texts. We do not wish to include other forms of communication – for example telephone, hard copy letter or face to face comments. The distinguishing feature of electronic communication is that it has the capacity to spread beyond the original sender and recipient, and envelop the recipient in an environment that is pervasive, insidious and distressing. There are also evidential advantages: a copy of the electronic message will usually be readily available.

5.52 We noted in the previous chapter that the laws of some other jurisdictions make special provision for harmful electronic communications. Similarly in New Zealand, the law on unlawful spam is confined to "commercial electronic messages".[228] In other words there is legislative precedent for giving special attention to electronic communications.

Complainants

5.53 Those entitled to complain to the tribunal should be the victims, the parents or guardians where the victim is a child or young person or a person with a disability, and school principals on behalf of students. We also believe that the Police should have access to the tribunal where a communication constitutes a threat to the safety of any person. We do not envisage that the Crown, or any Government agency, should be able to complain: we do not see the mechanism as one to enable the Crown to address, for example, name suppression breaches or contempt of court. But Government employees and individuals employed by Crown agencies would have rights in relation to harm sustained by them in their individual capacity. For example an employee of a government department, or a school teacher, might complain about conduct towards them in the course of their employment.

5.54 One issue of standing is the position of bodies corporate. Sometimes business enterprises can suffer serious damage as a result of malicious attacks by competitors or disgruntled clients. But bodies corporate are artificial constructs and therefore cannot themselves suffer mental harm or distress. We conclude that the right to complain should be confined to natural persons. However an attack on a small business will often be read as an attack on the proprietor personally, in which case he or she would have standing to complain.

Jurisdiction: the threshold

5.55 We have emphasised previously that only particularly serious cases should come to the

228 Unsolicited Electronic Messages Act 2004. Note also the Electronic Transactions Act 2001.

tribunal. Complainants should have to demonstrate two things:

(a) Firstly, they should show that they have attempted to resolve the matter through other avenues. The tribunal is effectively a backup solution when other approaches have failed. We shall elaborate on this later in the chapter, and explain the prior role of the "approved agency".

(b) Secondly, the harm should be significant before a complaint reaches the tribunal. Complainants should demonstrate that the communication complained about has caused, or is likely to cause, *significant* emotional distress. The whole purpose of this new machinery is to remove or minimise harm to individuals, and not to regulate or enforce community standards. It is a protective jurisdiction. The threshold should be a high one.

5.56 Proof of significant emotional distress may be thought to be problematic. Usually it will be sufficiently demonstrated by the nature of the communication itself: much of the material coming before the tribunal is likely to be of such a kind that it would clearly cause real distress to any reasonable person in the position of the applicant. This blended objective/subjective standard is reflected in the Harassment Act which requires, as a condition of making a restraining order, that the behaviour causes distress to the applicant, and is of such a kind that would it cause distress to a reasonable person in the applicant's particular circumstances.[229] The Privacy Act requirement that an interference with privacy must cause damage including "significant humiliation, significant loss of dignity or significant injury to the feelings of the complainant"[230] appears not to have been problematic.

5.57 Causation of harm is not always straightforward. The complexities of the notion of causation in the law are well known and well documented.[231] In our present context, the fact that cyber messaging is sometimes part of a wider pattern of conduct, and that sometimes it is also part of an exchange of communication in which the "victim" has knowingly participated, renders the question of causation of harm even more difficult. In one case under the Harassment Act the Judge found that the 'victim' was a significant contributor to her own misfortune, and declined to find that the offensive

229 Harassment Act 1997, s 16(1)(b)(ii).

230 Privacy Act 1993, s 66(1)(b)(iii).

231 Todd has said: "In truth, the inquiry into cause is apt to produce perplexing legal and philosophical problems which the courts, not surprisingly, frequently have had difficulty in resolving": Stephen Todd (ed) *The Law of Torts in New Zealand* (5th ed, Brookers, Wellington, 2009) at [20.1].

blog comments complained of caused her distress.[232] We do not think that a legal definition of 'cause', even if it were possible, would be helpful, and are content to leave questions of causation to the judgment of the tribunal in each case.

Jurisdiction: the law

5.58 It will be necessary to specify the types of unlawful communication over which the tribunal has jurisdiction. There are three alternatives:

(a) First, one could require that the tribunal would only have jurisdiction where there had been an alleged breach of the law: that is to say, where a rule of our civil or criminal law had been broken. We have outlined in the previous chapter the groups of offences, civil causes of action, and regulatory rules that make up our body of communications law.

(b) Secondly, one could formulate a specially designed set of ethical standards, the breach of which would give the tribunal jurisdiction. Some but not all of these ethical standards might overlap with the law.

(c) The third is a middle way between the first two. It is a statutory code which derives solely from the existing legal rules but is expressed in plain and accessible language.

5.59 We prefer this third alternative. One advantage is that it ensures that the rules to be applied by the tribunal are accessible in one place, and are easy to understand. That serves an educative function as well as an adjudicative one. A reader can see in one place the prescription of unacceptable internet behaviour. Otherwise the law to be applied by the tribunal would have to be located in its original form, scattered in a variety of places, some of it criminal, some civil, with different standards of proof and different defences.

5.60 Another advantage is that the essential substance of the codified list would reflect the existing law, although of necessity it would not be an exact distillation of it. That has particular attractions in terms of the New Zealand Bill of Rights Act. One of the powers of the tribunal will be to make takedown orders, which are effectively injunctions. It is a requirement of the Bill of Rights Act that limitations on freedom of expression should not only be justifiable in a free and democratic society, but should also be *prescribed by law*.[233] Finally if we were to adopt solution (b) above, it might be

232 *Brown v Sperling* DC Auckland CIV-2012–004–00925, 15 June 2012.

233 New Zealand Bill of Rights Act 1990, s 5.

alleged that we were trying to "regulate the internet."

5.61 In summary, the law to be applied by the tribunal would comprise a set of principles expressed in plain language which derive from the law of New Zealand, both statute law and common law. They could not be accurately described simply as a summary of that law, but it can properly be said that they would be based on it. This technique is not unknown in other contexts. In fact the terms and conditions of some of the large social media websites use a similar methodology.[234]

The Principles

Nature of the Principles

5.62 The principles we recommend below are derived from the criminal law, the civil law and the regulatory rules, both those that currently exist and those which we have recommended should be added.[235] The principles are expressed in a way which draws no distinction between their origins, because the tribunal's powers in respect of them will be the same. The tribunal will have no criminal or punitive jurisdiction and there will be no issues of differing burdens of proof. The tribunal's function will be to prevent and minimise harm caused by breaches of the law. Its powers, which will be outlined in detail in the next section, will include power to make takedown orders, orders to refrain from publishing similar material in the future, and orders to require the publication of apologies.

5.63 Nor are the principles as we state them qualified by conditions or defences. Instead, such matters are recognised as factors to be taken in account in deciding whether to make an order, and if so what kind of order. We emphasise again that the tribunal's jurisdiction will only be invoked where significant harm can be shown: to that extent all the principles must be read as impliedly subject to that qualification. The principles are thus, as it were, "stripped down law".

5.64 It may be said that it is unorthodox to grant what is effectively a civil remedy in relation to a criminal offence. But that is not without precedent. In the days before accident compensation, civil actions would sometimes lie in the tort of breach of statutory duty even where the statute imposed criminal duties: the factories legislation was an example.[236] As we pointed out in the previous chapter, this tort is of uncertain

234 See chapter 3 at [3.29].

235 See chapter 4.

236 See Stephen Todd (ed) The Law of Tort in New Zealand (5th ed, Brookers, Wellington, 2009) at

scope these days. The provisions we propose provide clarity that civil tribunal orders can issue even in relation to criminal activity. It would indeed be illogical if they could not.

5.65 In conclusion, then, the principles derive from the law and are reduced to a form which is accessible to both internet users and victims. Their accessibility will serve both an educational and a deterrent function.

Substance of the Principles

5.66 The principles we recommend are as follows:

> There should be no communications which cause significant emotional distress to an individual because they:

1. Disclose sensitive personal facts about individuals. This derives from the tort of invasion of privacy; from information privacy principle 11 in the Privacy Act;[237] and from the intimate filming provisions of the Crimes Act[238] (both existing and as we recommend they should be amended).
2. Are threatening, intimidating or menacing. This derives from the various intimidation provisions of the Crimes Act and Summary Offences Act, and also from the new summary offence which we recommend in the previous chapter.[239] It extends beyond fear of bodily or property damage: that is one of the features of the new summary offence.
3. Are grossly offensive. This derives from the new summary offence we recommend.[240] If it is thought that this is too vague a test, it must be remembered that the tribunal will also need to find that significant harm has resulted. There will be overlap with some of the other principles, but there will be some cases where no other principle serves the purpose, yet where the message is so disturbing that redress is merited. The *Duffy* case might be an example.[241] The test of grossly offensive should be what is grossly offensive to a reasonable person in the position of the complainant. One does not want the standards of an unusually nervous or sensitive person to be the

---

[8.203(2)].

237 Privacy Act 1993, s 6.

238 Crimes Act 1961, ss 216G – 216N.

239 Chapter 4 at [R1].

240 Ibid.

241 See chapter 2 at [2.52].

touchstone: a reasonable degree of robustness is required. However, the test must to an extent be contextual: if the complainant has voluntarily entered into an online conversation on a chat-room or blog which is known for particularly robust, even extreme, discussion, the complainant's expectations must to some degree affect what another person in their position would regard as offensive.

4. Are indecent or obscene. This derives from the new summary offence we recommend, from the intimate filming provisions,[242] and also from the sexual grooming provisions of the Crimes Act,[243] amended as we propose. The potential harm in the latter instance does not require further demonstration.
5. Are part of a pattern of conduct which constitutes harassment. Such conduct can be subject to a restraining order under the Harassment Act now so long as it causes distress, and there is no reason why the proposed tribunal should have any less power, provided the harm threshold is met. We have recommended that, for the purposes of the Harassment Act, "pattern" may be constituted by a succession of individual acts or one continuing act:[244] the same should apply here.
6. Make false allegations. This derives from the new summary offence we recommend, from the tort of *Wilkinson v Downton*,[245] from the law of false attribution, and also from the law of defamation. It would cover false statements about both the complainant and other matters. It would cover things such as false Facebook pages, and hoaxes intended to cause distress. The requirement to demonstrate harm will ensure that only serious falsehoods are addressed. Though malice is an ingredient of the proposed new offence, it is not of defamation: we have elected to use the defamation standard because the purpose of the new scheme is to mitigate harm, and it is the effect of the statement on the victim rather than the intention of the author which is relevant. When the statement alleged to be false is about the complainant, and is such as to cause reputational damage, we believe that the burden of proof should rest with the defendant to prove truth. Otherwise there is a misalignment with the law of defamation. The overlap between defamation and this proposed principle will not be without difficulty: we deal with that later in this chapter.

242 Crimes Act 1961, ss 216G – 216N.

243 Crimes Act 1961, s 131B.

244 Chapter 4 at R5(c).

245 Chapter 4 at [4.41].

7. Contain matter which is published in breach of confidence. This derives from the law of breach of confidence.[246] While public interest is a defence to the civil cause of action, here the public interest in publication will be a matter to be taken into account by the tribunal in deciding whether to make an order. Given principle 1, this principle is likely to have limited application.

8. Incite others to send messages to a person with the intention of causing that person harm. This derives from the incitement provisions of the Crimes Act.[247] While there appears to be no equivalent principle in the civil law it is appropriate to adopt it in the present context to address, in particular, group bullying. A message inciting harm to another would usually be able to be categorised as "grossly offensive" under principle (3) in any event.

9. Incite or encourage another to commit suicide. This derives from the provision in the Crimes Act,[248] amended as we propose.[249]

10. Denigrate a person by reason of that person's colour; race; ethnic or national origins; religion; ethical belief; gender; sexual orientation or disability. This derives from the Human Rights Act 1993,[250] amended as we propose.[251] Normally such a communication will also fall into the category of "grossly offensive".

5.67 It will be apparent that sometimes a communication may fall under more than one principle. Overlaps are common place in the legal system, and we are not concerned by that.

5.68 The principles must also be read in light of the considerations to be taken into account before an order is made. These considerations are outlined in para 5.80 below.

Procedures and powers

5.69 The rules of procedure of the tribunal should facilitate speedy and relatively informal justice, ensuring however that the rules of natural justice are complied with. Sometimes, particularly in cases where the health and safety of the complainant are at stake, the tribunal might have to move very quickly. The tribunal would have power to

246 Chapter 4 at [4.45].

247 Crimes Act 1961, ss 66(1), 311(2).

248 Crimes Act 1961, s 179.

249 Chapter 4 at R2.

250 Human Rights Act 1993, ss 21, 61, 131.

251 Chapter 4 at R7(b). See also [4.126].

receive evidence which might not be admissible in a court of law, to decide cases "on the papers", and when a hearing is appropriate to conduct it by Skype or videoconference or even by teleconference. In cases which may involve a takedown order, the opportunity for the defendant to be heard would usually be a requirement of natural justice, although there might be cases of such urgency that an ex parte order of an interim nature would be justified. The tribunal would have power to take evidence on oath and to require the supply of information where that was necessary.

5.70 An important procedural issue is how complaints should proceed where harmful communications are made anonymously. Anonymous communications currently pose the following difficulties for complainants: the complainant cannot approach the communicator directly to seek redress; the complainant may experience particular distress in not knowing where the communications originate from; and the extremity of the communication may be intensified under the cloak of anonymity.

5.71 The identity of the communicator may be relevant for the following reasons: so that the communicator can be asked to remove, modify or correct a communication; so that a formal complaint can be made where the communicator does not comply with such a request; or to provide redress to the complainant as revealing a communicator's identity may have an appropriate condemnation value.

5.72 We therefore recommend a three stage process. At each stage it is important to balance the interests of the complainant in exercising their rights to seek a remedy for the harm they have suffered, and the value of protecting anonymous speech from a freedom of speech perspective.[252]

5.73 The first step is a process whereby a complainant can request the source of the harmful communication to remove, modify or correct it. First the request should go to the complaints handling body we recommend later in this chapter. This body would pass the request on to the relevant internet service provider (ISP)[253] or other internet entity (for example Facebook or Google). Finally, the internet intermediary would be required to pass the request to their account holder.[254] If the person receiving such a request responds to it, the complainant may consider the matter sufficiently

252 See Steven J Horowitz "Defusing a Google Bomb" (2007) 117 The Yale Journal Pocket Part 36.

253 ISPs have a similar conduit role under the Copyright Act 1994, Part 6.

254 Of course, there will be situations where this process will not be available where communications cannot be traced to a specific account holder, such as communications made from internet cafes.

resolved.[255]

5.74 The second step would involve an application to the tribunal for a discovery or production order[256] that would require any relevant internet intermediary such as Facebook, Google or an ISP to provide identity details.[257] An application for discovering the identity behind an anonymous communication could be made simultaneously with filing a complaint in the tribunal, or might precede it where identity is a necessary element of the complaint.[258]

5.75 The tribunal should have the discretion to deal with the substance of the complaint in a manner that preserves the anonymity of the respondent. Where the tribunal considers that the respondent's anonymity should be removed, the respondent should be provided with the opportunity either to take steps to address the alleged harm (i.e. through taking steps to remove or moderate the material in question) in lieu of losing their anonymity.

5.76 The third step relates to remedies and would provide for anonymity to be removed where the tribunal is persuaded by a complainant (after hearing arguments on both sides) that this step is appropriately condemnatory and therefore provides a measure of redress to the complainant. The tribunal's powers to make orders (outlined below) should include the power to order removal of the respondent's anonymity.[259]

Order-making powers

5.77 The tribunal should have power to make the following orders:

(a) An order to takedown material. Given that this is a kind of injunction, the requirements of the New Zealand Bill Rights Act would have to be vigilantly

255 However, the complainant may have grounds to proceed with a complaint, even where the material is removed or modified, such as where the complainant seeks further measures such as an apology or acknowledgement, or an order restricting any further such communications.

256 See for example Human Rights Act 1993, s 126A. In the United Kingdom, the process used is a "Norwich Pharmacal" order; see Terri Judd "Landmark ruling forces Facebook to drag cyberbullies into the open" *The Independent* (online ed, 9 June 2012).

257 This would not require the intermediary to assess the nature of the complaint or to takedown the material in question at this stage; it would simply require the intermediary to provide account information under the authority of a tribunal order. As we discuss below however, the tribunal should have the power to order an intermediary to takedown material at a later stage of the process.

258 For example where a pattern of harassment by a particular person is alleged.

259 Compare the Copyright Act 1994, s 122A.

observed: the order would need to be a justified limitation on freedom of expression. Ex parte applications should be granted only in exceptional cases.

(b) An order to cease publishing the same, or substantially similar, communications in future. While similarity is a question of degree, something like this is necessary to prevent a defendant from continuing to attack the complainant using slightly different messages or avenues.

(c) An order not to encourage any other person to engage in similar communication with the complainant.

(d) A direction that the order may apply to a person other than the defendant if there is evidence that the defendant has encouraged that other to engage in offensive communication to the complainant.[260]

(e) A declaration that the communication in question breaches the statutory principles. This would have significant persuasive power, even if not mandatory authority, in relation to websites operating out of the jurisdiction.

(f) An order to correct a factually inaccurate statement in the communication.

(g) An order that the complainant be given a right of reply.

(h) An order to apologise to a defendant, together with such other forms of restorative justice as may be appropriate in the case. We do not, however, think that monetary sanctions are either necessary or appropriate.

(i) An order that the identity of the source of an anonymous communication be released.

(j) An order that the names of any of the parties be supressed.

5.78 Non-compliance with an order of the tribunal would constitute an offence, and would be punishable in the District Court by fine or imprisonment.

5.79 We considered whether in an extreme case termination of an internet account might be appropriate, but concluded that this would be to go too far. To deprive an individual, and perhaps also members of his or her family, of such an all encompassing source of communication and information could not be justified in this digital age.

Considerations to be taken into account in Tribunal orders

5.80 In exercising its functions the tribunal must have regard to the importance of freedom of expression. In deciding whether or not to make an order, and the form that any such

260 There is a similar provision in section 18 of the Harassment Act 1997.

order should take, the tribunal would have to take into account relevant considerations including:

(a) The content of the communication and the level of harm caused by it.

(b) The purpose of the communicator in communicating it. For example, satire or humour, is different from malice.

(c) The occasion, context and subject matter of the communication. For example, a contribution to political debate is a different thing from a gratuitous personal attack with no legitimate motive.

(d) The extent to which it has spread beyond the original communicator and recipient. For example, the size of the audience increases the hurt.

(e) The age and vulnerability of the complainant.

(f) The truth or falsity of the statement. In some contexts truth is more hurtful than fabrication, in others the reverse.

(g) The extent to which the communication is of public interest.

(h) The conduct of the defendant, including any attempt by the defendant to minimise the harm caused.

(i) The conduct of the complainant, including the extent to which that conduct has contributed to the harm suffered. There might be cases where the complainant has voluntarily participated in online conversations which have escalated to the point that the complainant now wishes to call a halt to the other party's excesses. In such cases questions may arise as to the expectations of the complainant when he or she entered the discussion forum, particularly if the forum is well known for robust expression. It might even be held in such a case that the complainant was the effective cause of his or her own eventual distress: in other words that he or she "brought it on themselves".

5.81 We regard consideration (g) (the extent to which the communication is in the public interest) as being of special importance. Such a qualification is present in the common law in relation to invasion of privacy and breach of confidence, and also appears in the official information legislation as an override of the grounds on which information might otherwise be withheld. In our present context, even though a communication might hurt an individual, a countervailing public interest in the subject matter might sometimes be strong enough to outweigh the interests of the complainant. This might possibly be the case if the communication was part of a vigorous debate about a political matter, or a high profile crime, accident or natural disaster.

5.82 The principles we have outlined in paragraph 5.66 must be read in light of these relevant considerations. They serve to qualify their otherwise absolute nature.

5.83 To take an example, principle 6 provides simply that there should be no communication of messages which "make false allegations". On its face, this may seem too simple a proposition, but we have not ignored the complexities of the law from which it is derived. It should be noted:

(a) That the tribunal must take into account the purpose of that communication. Malice and lack of legitimate purpose will be relevant to the making of an order.

(b) That the tribunal must take into account any public interest in publication.

(c) That the tribunal must take into account the occasion and subject matter of the communication.

(d) That the tribunal must take into account the audience to which the message has been communicated.

5.84 In addition the tribunal will only act if the complainant can show significant harm; and if a proposed order limiting freedom of expression can be justified in a free and democratic society.[261] If the defendant pleads that the allegation is in fact true, the tribunal may decide that the case is not suited for the tribunal unless other factors, such as the offensive nature of the communication, justify an interim order to cease publication.

5.85 The tribunal would have no power to impose criminal sanctions. The punishment of breaches of the criminal law is, and should remain, the preserve of the courts.

5.86 The tribunal should give reasons for its decisions, and they should be published. The tribunal should have a web presence and the decisions should appear there. Consideration might also be given to making them available through NZLII. Over time a set of precedents would develop, which would give a degree of certainty as to where the lines of unacceptable behaviour are to be drawn. The requirement to publish reasons brings its own problems. The victim of the message should often be anonymous. Sometimes, too, the facts may need to be stated with careful economy so as not to identify by reference. But the Privacy Commissioner has similar problems, and the case notes from her office manage to provide useful information without identification, and without invading privacy or confidence.

261 New Zealand Bill of Rights Act 1990, s 5.

Defendant

5.87 Usually it will be the creator of the content of the communication who will be the subject of the order, but if the creator cannot be traced, or is out of the jurisdiction, or is unable himself or herself to delete the content of the communication from the website, the tribunal should have power also to make an order against a website host, an internet service provider or other internet intermediary. Those entities will not generally be responsible in law for the communication.[262] But the fact that they may not be legally responsible for the material should not, in an appropriate case, prevent the tribunal ordering them to take it down. Accountability for failure to comply with such an order would arise where:

(a) clear notice has been given to them of exactly where the material is located and the content of it, and

(b) they do not do all that is reasonable to remove the material. (It may not always be possible to remove all traces of material from the various places to which it may have migrated on the internet.)

5.88 We emphasise that there must be no suggestion that the website host or intermediary should be the first point of call when an order is sought. The fact that they are easier to find is not a reason. An order should be made against them only if unsuccessful attempts have been made to seek an order against the content creator. We elaborate on the role of such intermediaries later in this chapter.

5.89 No doubt there will be cases where the tribunal will not be able to act effectively. However there will be many cases where it will. In the great majority of cases that we have in mind the complainant will know who the offenders are, and they will be within the jurisdiction. They will be the main targets of the tribunal's authority. There will doubtless be a few who evade the system. That is so of any law.

Appeals

5.90 Some of the orders the tribunal might make are of a significant nature, especially an order to takedown a communication, or to refrain from future similar conduct. They constrain freedom of expression and involve Bill of Rights Act issues. Conversely, the personal harms which these orders address are serious ones. These considerations argue in favour of a right of appeal. As against that, however, the tribunal is one where

262 We do not elaborate in this report on cases where such entities might be liable to legal sanctions for publishing the material in the first place, but we expect such cases will be exceptional.

specialist knowledge and experience are important, and it is knowledge and experience which will not be possessed by every appeal judge.[263]

5.91 On balance we favour a right of appeal. It should be on the merits. It should lie to an appeal tribunal comprising two District Court Judges. The tribunal and the Judge hearing the appeal should be able to sit with an adviser specialising in information communication technologies (ICT). There should be special procedures to enable the appeal to be dealt with quickly.

Two special cases

5.92 Two special cases of internet harm require separate consideration. First, incitement or persuasion to suicide or self-harm is different from the other harms we have been considering. It is not always directed at a single individual, but can have a wider audience. The same is true of the publication of details of a suicide: that kind of communication is generally prohibited by the Coroners Act 2006.[264] If such publications are generalised and of such a kind that they might influence members of the public at large, there is no specific victim who might bring a case to the Commissioner or the tribunal. In this situation we think there is room for an exception to the general rule that only a victim or a person acting on his or her behalf can complaint. We think that in cases such as these the Chief Coroner should be able to apply to the tribunal for a takedown order or an order to discontinue the conduct.

5.93 Secondly, defamation raises special considerations. Where truth or honest opinion is pleaded there is always the potential for lengthy argument. Defamation cases can become protracted and procedurally complex, and it will probably not be possible for the tribunal in every case to accord them the effective speedy justice we hope it will be able to apply to other sorts of harm. However, we would make two comments. The first is that if, as will often be the case, the statement complained about is extravagant and manifestly untrue, no possible defence of truth or honest opinion will be available. In that sort of case, the tribunal should be able to dispose of the matter quickly. Even now, the courts can sometimes award summary judgment, or grant an interim injunction, restrictive though the rules for those orders are. If, on the other hand, the defendant does plead truth or honest opinion and there is some basis for such a defence, the tribunal may decide that it is an inappropriate forum to determine the case,

263 Legislation Advisory Committee "Guidelines on Process and Content of Legislation" (May 2001) at chapter 13.

264 Coroners Act 2006, s 71.

and that the matter should be remitted to a court. Even then, however, if the tone of the communication is highly offensive, and the distress occasioned substantial, those factors might still justify the award of an interim injunction (or takedown order) pending further investigation by a court. In that case the mental harm caused by the communication and its tone might be more significant than the reputational harm which is the essence of a defamation case.

Relationship with other proceedings

5.94 There are four questions about how the tribunal might relate to other adjudicators or regulatory bodies. The first question is how the tribunal would relate to the converged media regulator that we proposed in part one of the issues paper.[265] Will the news media which are governed by the proposed regulator also be subject to the tribunal? The Commission has not yet finally reported on this matter, and the ensuing discussion is contingent on its continuing to hold the view expressed in the issues paper.

5.95 On one view it could be argued that the news media should be subject to the tribunal because, whereas the regulator applies a code of good practice, the tribunal applies a set of principles based on the law of New Zealand, and those media are bound by the law. On the other hand if the new media regulator is effective, the codes it prepares will cover (among many other things) the sorts of conduct that will be within the tribunal's jurisdiction. If the regulator's powers are rigorously and effectively exercised, in particular its power to require takedowns, it should be able to grant effective remedies for breach. This being so, we think it would be confusing and duplicative for individuals to be able to resort to the tribunal as well as the regulator. If the conduct was demonstrably unlawful, court action would still be available against the offender.

5.96 Secondly, there is a question of whether invasions of privacy on the internet should be dealt with by the Privacy Commissioner or by the new tribunal. Privacy invasions are a small subset of internet harms, but they are one for which there is presently a remedy (unless the communicator is a news medium which is exempt from the Privacy Act principles). The question is whether in such a case the complainant should have a choice of forum or, if not, which of the Privacy Commissioner or the tribunal it should be. We tend towards the option that the complainant should have a choice. Choice of forum is not unknown elsewhere in the law. In some cases the choice would be

265 Law Commission *The News Media Meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age* (NZLC IP27, 2011) at chapter 6.

exercised according to whether the communication in question was part of a wider pattern of conduct which was within the jurisdiction of one regulator or the other, in others according to the remedy desired. Care would be needed, however, to ensure that one route did not become seen as a 'softer' option.

5.97 Thirdly, some of the communications dealt with by the tribunal may involve criminal conduct which is investigated by the police. In very serious cases, criminal prosecutions should remain the ultimate sanction. We do not see any objection in principle to such parallel processes. Their purposes are quite different. The recourse to the tribunal is to remove or mitigate a serious harm to the complainant; the fact that the harm has occurred, and has been addressed by the tribunal, does not determine whether criminality has been established and whether the communicator should incur a criminal penalty. Just as civil and criminal proceedings can both lie in respect of the same act, so we think criminal proceedings and a complaint to the tribunal should be able to co-exist.

5.98 Fourthly, the existence of the commissioner or tribunal process does not mean that the victim is deprived of his or her rights to seek justice in the courts instead. If he or she wishes to seek substantial damages for, say, defamation or invasion of privacy, he or she must continue to have a right to take a civil action in the courts. Likewise if the offensive communication in question is part of a much wider pattern of victimisation and harassment, as it might well be for example on the breakup of a relationship, the victim may elect to go to the District Court for a restraining order under the Harassment Act or to the Family Court for a protection order under the Domestic Violence Act 1995. But the complainant would have to elect between the two avenues. He or she could not pursue both.

5.99 It would be different, however, if a complainant went directly to the court to seek no more than an order which could have been granted by the tribunal. We are alive to the fact that there may, however rarely, be a well-resourced complainant who brings a claim to court with a view to exploiting a resource imbalance between the two parties. In such a case we believe that the defendant should have the right to request, and the court to order, that the matter be transferred to the tribunal. There is such a power in section 37 of the Disputes Tribunal Act 1988.

The "approved agency"

5.100 It is clear that the tribunal cannot be the sole machinery to resolve difficulties of the kind with which we are dealing. This is so for two reasons.

5.101 The first reason is that there will need to be a high level of seriousness before a matter proceeds to the tribunal. Freedom of expression must not be constrained except for very good reason. Moreover, a flood of insubstantial complaints could burden the tribunal to the extent that its workload would be unmanageable. So there has to be a means of controlling, or "filtering", what comes to the tribunal.

5.102 Some such avenues already exist independently of anything that we might recommend. Many websites have their own internal system of moderation and censorship. Complainants should be required to try there first. In the same way, complainants who are school children should be required to approach the school first, the school referring matters on only where internal resolution fails. Schools, with the assistance of the Ministry of Education, should adopt consistent and effective policies for the handling of such matters. Then, perhaps most importantly, education and user awareness are key. Good "digital citizenship" should be the aim, and already large responsible providers are promoting it. As this develops the pressures on a complaints mechanism should decrease. Nonetheless it is clear that there will need to be some mechanisms for 'filtering' complaints.

5.103 The second reason is that the tribunal should be a backstop. Many complaints will be much better handled by less formal means: by techniques of mediation, negotiation and persuasion. In the case of young people in particular recourse to a judicially imposed solution in a tribunal should indeed be a last resort. Persuasion, with the possibility of tribunal proceedings in the background, should be an effective tool in many cases. That is a model which has been employed in New Zealand: the Privacy Act and the Human Rights Act are notable examples which bear an analogy with the present situation.

5.104 On this basis we believe there needs to be an agency through which complaints must pass before they reach the tribunal. There are a number of possible ways of achieving this end. One would be for the tribunal itself to have support staff who would receive all complaints and refer them to mediation in the first instance, rather in the way the Tenancy Tribunal works. This, however, would involve creating a new structure. It could be cumbersome. The same may be said of the office of a Communications Commissioner. We were initially attracted to this as a possibility, although as an alternative rather than as an adjunct to a tribunal. But given that there is a degree of speculation as to how great a load of work there will be, we would prefer at least in the early stages to utilise and build on structures which already exist. We therefore support the concept of an "approved agency", in other words an existing person or entity which

is appointed by the Minister by Gazette notice as a body entitled to perform the relevant functions.

5.105 There are analogies elsewhere in our law. Among them are approved dispute resolution schemes under the Financial Service Providers (Registration and Disputes Resolution) Act 2006 and approved organisations under the Animal Welfare Act 1999.

5.106 In this context the functions of that agency would be:

(a) To advise persons on steps they may take to resolve a problem caused by an electronic communication and whether they may have a ground of complaint. In some cases this may involve the agency in advising the enquirer to go to the police. Helping inquirers to select the appropriate recourse will be a proper function. There should be an online platform for receiving complaints and providing information. An 0800 telephone number should be employed.

(b) To receive complaints about electronic communications.

(c) To decline some complaints because the matter complained about is unlikely to cause harm, or is otherwise inappropriate for investigation.

(d) To investigate substantial complaints and attempt to achieve settlement between the complainant and the person responsible. The settlement might include such things as an apology, an undertaking to takedown the offending material and an undertaking to refrain from such content in future.

(e) To liaise with website hosts and ISPs and request them to takedown or moderate posts which are clearly offensive.

(f) To liaise with other agencies such as schools, the Police, Commissioners such as the Privacy Commissioner, the Children's Commissioner and the Human Rights Commission, the Ministry of Social Development and InternetNZ in attempts to resolve wider issues surrounding the communications complained about.

(g) To advise the complainant to seek an order from the tribunal requiring a website host, ISP or internet intermediary to identify the author of an offensive communication.

(h) To advise the complainant to refer to the tribunal:

(i) any complaint which meets the appropriate level of seriousness and which has proved incapable of resolution by other means;

(ii) any complaint which is so serious, and resolution of which is so urgent, that it should be referred directly to the tribunal without mediation;

(i) To certify that it has recommended a referral of such a complainant to the tribunal.

5.107 We envisage that an agency would be approved to exercise these functions by the Minister of Justice by Gazette notice. It may be that there could be several agencies so approved, although if the workload is manageable we think one would be preferable. The idea of a well-publicised single point of entry has clear advantages.

5.108 Presently, one organisation which is clearly suited to the task is NetSafe. NetSafe is a non-governmental organisation, partly funded by government, which performs many of the tasks already. It advises people who are upset by electronic communications. It has formed good relationships with other agencies such as the Police, the Ministry of Education and ISPs. It knows and has dealings with big offshore operations such as Google and Facebook and commands their respect. As Google noted in its submission to our issues paper, "NetSafe's work has been praised by government, who have described its programme as 'world leading'."

5.109 We believe that NetSafe should be an 'approved agency' for the purposes we have outlined.

5.110 However, this would inevitably involve an increase in its workload. The quantum of that increase is difficult to estimate in advance, but, particularly in the early stages before the threshold for complaints is clearly delineated and understood, it could be significant. It is imperative that NetSafe has appropriate systems in place, and that it be appropriately resourced. The state should provide necessary additional funding.

Wider functions

5.111 In addition to the complaints function which we have described, there is a clear need for a body with more general oversight functions.

5.112 They would include the following:

- *Education and publicity* – Education about appropriate online conduct and safety on the internet is becoming increasingly important for users young and old. Just as the Privacy Commissioner performs a range of education and guidance functions, so would such a function be desirable in the context we are addressing. The development of good digital citizenship is a priority.
- *Research* – Related to this last point, some agency needs to keep abreast of developments in technology and patterns of internet use and abuse. Currently we lack sufficient hard, detailed, statistical data.
- *Policy oversight* – It would be desirable, too, to have an agency with the function of

providing advice to the government about the need for change or updating of legislation or government policy.

5.113 It is not absolutely necessary that the complaint-handling "approved agency" should be the same one which performs these wider functions. But there are clear advantages in its being so. The combination of similar functions in the Privacy Commissioner in the Privacy Act works well. It means that a single body becomes expert and authoritative in the subject matter. The wider oversight activity would benefit the complaints-handling function, and vice versa. Co-location in one agency is also clearer for the consumer and makes it more cost effective to promote the organisation and its services. We strongly support all functions being combined in one agency. This is another reason for NetSafe being the approved agency. It already performs some of the wider functions.

5.114 We have noted previously that cyber-bullying is sometimes part of a wider and complex set of issues. It is important that the approved agency maintains a close working relationship with other agencies, such as the Police, the Children, Young Persons and their Families Service (CYPFS) and the Ministry of Education, which also deal with bullying and relationship issues, so that coordinated responses can be developed.

The role and responsibilities of internet intermediaries and content hosts

5.115 In their submissions to our review a number of internet based businesses, including Google and Trade Me, emphasised the need for clarity and consistency in the treatment of Internet Service Providers (ISPs) and other internet intermediaries in any legislative reforms we propose.

5.116 In our Issues Paper, and in earlier reviews conducted by the Law Commission, we have adopted the widely supported position that entities which act as conduits or intermediaries for the publication of content, such as ISPs and content hosts, should not be legally liable, in the first instance, for the innocent dissemination of content created by their users.

5.117 As Trade Me pointed out in its submission:[266]

> … everyone can be a publisher on the internet, and …online content hosts are often not in a position to know, let alone pre-vet, all the content that appears on their websites. Nor is there an effective technology filter for the truth, or for offensive or illegal content.

5.118 However, as we discussed in chapter 3, many of these companies do employ various

266 Submission of Trade Me (12 March 2012) at [54].

self-regulatory tools, including terms of use contracts and community moderation and reactive reporting to support the responsible use of their services.

5.119 How far these entities are prepared to go in terms of proactive policing and enforcing their own terms of use contracts, and how responsive they are to users' complaints varies considerably. Alongside the considerable resourcing implications of enforcing standards, there can be difficult commercial and ethical issues to balance.

5.120 These interests include the companies' own legitimate rights as private entities to run their businesses as they see fit; the interests of their customers to privacy; the wider public good in supporting the free flow of information on the internet and the legitimate interests of governments and law enforcement agencies in upholding the law and protecting the interests of their citizens.

5.121 One of the important features of our proposed reforms is to provide an authoritative, locally based, mechanism for mediating on behalf of complainants, and, in cases where mediation fails, securing remedies for those affected by harmful digital communication.

5.122 As we have stated, as a matter of principle, the target of these actions should be the person responsible for the content. But identifying that target, and providing them with the opportunity to respond to a complainant will sometimes require the active co-operation of intermediaries, whether they be a locally based ISP or website administrator or a global entity such as Facebook.

5.123 Similarly, there may be occasions when an intermediary or content host is compelled by an order of the tribunal to take certain steps, such as removing content after the author has failed to do so. Once content has been removed from a site it may also be necessary to request that cached versions of the old content be removed from search engines' indexed caches in order to make takedown more effective.

5.124 Large corporations like Google, Trade Me and Facebook have well developed protocols for how they respond to authoritative requests from governments and law enforcement agencies for information about users or to notice and takedowns. However in other cases these protocols may not be easy to access, or implement, even for law enforcement agencies – particularly when the entity has no physical presence in New Zealand. And, as we discussed earlier, internet intermediaries and content hosts vary hugely in size and complexity and it is by no means the norm for all to have clear and transparent policies for how they will respond to complaints or to legitimate requests for user information.

5.125 As Trade Me pointed out during consultation, to maximise the effectiveness of the tribunal and NetSafe's work it will be important to develop clear protocols with content hosts and intermediaries, both New Zealand based and overseas, to ensure consistent and speedy responses to notice and takedown orders and other information.

5.126 In its submission Trade Me emphasised the important role these entities can play in upholding the law and facilitating its enforcement:[267]

> In our experience, the architecture of the internet can help facilitate maintenance of the law in a way that was not previously possible. However it requires a co-operative approach.

5.127 Trade Me proposed the development of a code for content hosts and intermediaries, a requirement of which would be adherence to the notice and takedown principle that is already enshrined in other legislation.

5.128 We agree that critical to the effectiveness of our proposed tribunal will be the development of consistent, transparent, and accessible policies and protocols for how intermediaries and content hosts interface with it and with NetSafe. We recommend that NetSafe work with these private sector agencies, including New Zealand's telecommunications companies to develop such guidelines and protocols. Trade Me, an organisation which has both considerable technical and regulatory expertise, would be an invaluable partner in that process.

CONCLUSIONS

5.129 We are persuaded that there are serious harms resulting from electronic communications which require addressing. The concerns exposed by organisations such as the Police, some coroners, NetSafe, and the Human Rights Commission are evidence enough of that. The harms often go unaddressed. Some of the alleged harms are so serious (suicide and self-harm, for instance) that even the risk they might occur justifies remedial measures.

5.130 Something can be done by educating users in good digital citizenship, and by improved self-regulation and moderation by website hosts and intermediaries. Cyber-bullying and other kinds of harmful speech are also symptomatic of wider social problems which require address, as far as that is possible, by extra-legal techniques.

5.131 However, the law has an important part to play. In chapter 4 we recommended some changes to existing legal rules, and the creation of some new legal rules. These range from a new criminal offence (the top of the pyramid) to changes in some of our

267 Ibid, at [44].

regulatory statutes. These new legal provisions (in particular the criminal offences) will have an important deterrent, even if cases seldom reach the courts, and will serve to delineate the limits of the community's tolerance for the misuse of communications tools.

5.132 In this chapter we propose a new regime for addressing the harms suffered by individuals. The purpose is to provide a more accessible mechanism than now exists for addressing individual hurt. It comprises an approved agency or agencies, with persuasive power, to receive complaints and attempt to resolve them, backed by a tribunal which can make enforceable orders, including takedown orders, when efforts at settlement fail. The proposals have the following features.

5.133 First, they are not disproportionate in terms of resource. If the tribunal consists of District Court judges, and if NetSafe becomes an approved agency, there will be no new structures required, although some of the existing structures are likely to require extra resource. Our proposals build on what is presently there.

5.134 Secondly, the set of principles, based on the law, which will be applied by the tribunal will serve an educational and awareness function as well as a deterrent one. Internet awareness is a critical objective of this project.

5.135 Thirdly, the new agency/tribunal structure will be a well-publicised point of entry which will enable remedies to the obtained informally, relatively cheaply and (above all) quickly. In other words the remedies will be accessible. Access to justice represents what a society and its legal systems stand for.

5.136 Finally, the new system will not compromise other legal sanctions. The criminal law will be available for serious cases, and the right to sue in a court of law, for example for defamation, will still be an option. It is impossible to predict the exact level to which the new structures will be used, but there is ample evidence of need to justify the reform. Currently the avenues available are simply not enough to address the problems which exist. There is a gap that needs to be filled, and the proposals aim to do so. If we do not try this, nothing will improve. The reform is a package, the parts of which are inter-dependent. The package needs to be seen as a whole.

Recommendations

R8 Complaints about offensive internet communications should go initially to an "approved agency" which would advise complainants and attempt to achieve a resolution by a process of negotiation, mediation and persuasion.

R9 If a complaint cannot be resolved in this way, it may then proceed to a tribunal which can

make enforceable orders, provided the threshold of seriousness is reached.

R10 The tribunal should consist of a District Court judge drawn from a panel of District Court judges designated for the purpose. The tribunal may sit with an expert in information communication technology.

R11 The tribunal's jurisdiction should extend to all forms of electronic communications.

R12 Those entitled to complain to the tribunal should include the victims (other than non-natural persons), the parents or guardians where the victim is a child or young person or a person with a disability, school principals on behalf of students, and, where the communication constitutes a threat to the safety of any person, the Police.

R13 Only particularly serious cases should come to the tribunal. Complainants should have to demonstrate two things:

(a) that they have attempted to resolve the matter through other avenues; and

(b) that the communication complained about has caused, or is likely to cause, significant harm, including significant emotional distress.

R14 The tribunal must not make an order unless it is satisfied that there has been a breach of one of the principles in R15.

R15 There should be no communication of messages which cause significant harm to an individual because they:

1. Disclose sensitive personal facts about individuals.
2. Are threatening, intimidating or menacing.
3. Are grossly offensive.
4. Are indecent or obscene.
5. Are part of a pattern of conduct which constitutes harassment.
6. Make false allegations.
7. Contain matter which is published in breach of confidence.
8. Incite or encourage others to send messages to a person with the intention of causing that person harm.
9. Incite or encourage another to commit suicide.
10. Denigrate a person by reason of his or her colour; race; ethnic or national origins; religion; ethical belief; gender; sexual orientation or disability.

R16 The rules of procedure of the tribunal should facilitate speedy and relatively informal justice, ensuring however that the rules of natural justice are complied with. In particular:

(a) The tribunal should have power to receive evidence which might not be admissible in a court of law, to decide cases "on the papers", and when a hearing is appropriate to conduct it by videoconference or teleconference.

(b) The tribunal should have power to take evidence on oath and to require the supply of information where that was necessary.

(c) The tribunal should have the discretion to deal with the substance of the complaint in a manner that preserves the anonymity of the respondent. Where the tribunal considers that the respondent's anonymity should be removed, the respondent should be provided with the opportunity either to take steps to address the alleged harm in lieu of losing their anonymity.

R17 The tribunal should have power to make the following orders:

(a) An order to takedown material from the electronic media.

(b) An order to cease publishing the same, or substantially similar, communications in future.

(c) An order not to encourage any other person to engage in similar communication with the complainant.

(d) A direction that the order may apply to a person other than the defendant if there is evidence that the defendant has encouraged that other to engage in offensive communication to the complainant.

(e) A declaration that the communication in question breaches the statutory principles.

(f) An order to correct a factually inaccurate statement in the communication.

(g) An order that the complainant be given a right of reply.

(h) An order to apologise to a defendant, together with such other forms of restorative justice as may be appropriate in the case.

(i) An order that the identity of the source of an anonymous communication be released.

R18 The tribunal should have the power to make an order against a defendant, an internet service provider, a website host, or any other relevant internet intermediary requiring material to be taken down from the internet.

R19 The Chief Coroner should be able to make an application to the tribunal for an order that material relating to suicide that is prohibited by the Coroners Act 2006 be taken down from the internet.

R20 In exercising its functions the tribunal must have regard to freedom of expression. In deciding whether or not to make an order, and the form that any such order should take, the tribunal would have to take into account relevant considerations including:

(a) The content of the communication, its offensive nature and the level of harm caused by it.

(b) The purpose of the communicator in communicating it.

(c) The occasion, context and subject matter of the communication.

(d) The extent to which it has spread beyond the original communicator and recipient.

(e) The age and vulnerability of the complainant.

(f) The truth or falsity of the statement.

(g) The extent to which the communication is of public interest.

(h) The conduct of the defendant, including any attempt by the defendant to minimise the harm caused.

(i) The conduct of the complainant, including the extent to which that conduct has

contributed to the harm suffered.

R21 The tribunal should not have the power to impose criminal sanctions or monetary sanctions.

R22 The tribunal should give reasons for its decisions, and they should be published.

R23 There should be a right of appeal on the merits from decisions of the tribunal to an appeal tribunal consisting of two District Court judges. The judges hearing the appeal should be able to sit with an adviser specialising in information communication technologies. There should be special procedures to enable the appeal to be dealt with quickly.

R24 The tribunal or an appeal tribunal may refer a complaint to a court if it considers the complaint could be more approximately dealt with by a court.

R25 If a matter comes before a court which could be dealt with by the tribunal, the court may refer the matter to the tribunal.

R26 A person or organisation may be appointed by the Minister as an "approved agency".

R27 The functions of an approved agency should be:

(a) To advise people on steps they may take to resolve a problem caused by an electronic communication and whether they may have a ground of complaint.

(b) To receive complaints about electronic communications.

(c) To decline some complaints because the content of the communication is unlikely to cause harm, or is otherwise inappropriate for investigation.

(d) To investigate substantial complaints and attempt to achieve settlement between the complainant and the person responsible.

(e) To liaise with website hosts, ISPs and other internet intermediaries and request them to takedown or moderate posts which are clearly offensive.

(f) To liaise with other agencies such as schools, the Police, the Privacy Commissioner, the Ministry of Social Development and InternetNZ in attempts to resolve wider issues surrounding the communications complained about.

(g) To advise the complainant to seek an order from the tribunal requiring a website host, ISP or internet intermediary to identify the author of an offensive communication.

(h) To advise the complainant to refer to the tribunal:

- any complaint which meets the appropriate level of seriousness and which has proved incapable of resolution by other means;
- any complaint which is so serious, and resolution of which is so urgent, that it should be referred directly to the tribunal without mediation;

(i) To certify that it has recommended a referral of such a complainant to the tribunal.

R28 NetSafe should be an approved agency.

R29 The approved agency should also have general oversight functions including education and publicity, research, and policy oversight.

R30 The approved agency should work with intermediaries and content hosts to develop guidelines and protocols regarding their relationship to the approved agency and the tribunal.

Chapter 6: The education sector

INTRODUCTION

6.1 In chapter 3 we discussed the nature of cyber-bullying, and how it presents particular threats to victims, and particular challenges to those attempting to prevent it. As we noted, while cyber-bullying is by no means limited to relationships between adolescents, it is becoming an increasing issue in schools.

6.2 Cyber-bullying has recently come into sharp focus in the context of a *New Zealand Herald* campaign highlighting the impact of violence and bullying on New Zealand adolescents. In the context of this campaign, the Chief Coroner, Judge Neil MacLean, expressed his concern about the emergence of bullying, and cyber-bullying in particular, as a "background factor" in New Zealand's high youth suicide rate. He also noted that bullying featured as one of the factors researchers found when investigating incidences of self-harm among adolescents.[268]

6.3 In 2011, the Prime Minister John Key called for a "national conversation" on how to reduce bullying in our schools after mobile phone videos of children being bullied became prominent on the internet.[269]

6.4 In this report we have argued that from a policy point of view cyber-bullying should not be divorced from the wider social problem of harmful digital communication. That said, we also recognise that there are compelling reasons for prioritising resources and tailoring solutions for adolescents who as a group are both the highest users of new media and the group most vulnerable to some of the harms associated with its misuse.

6.5 The impact of new media and digital technology were considered as part of a wide ranging report on the challenges confronting New Zealand adolescents commissioned by Prime Minister John Key in 2009 ("the PMCSA report").[270] The authors emphasised the need for policy and law makers to understand the radically changed

268 Helen L Fisher and others "Bullying Victimisation and Risk of Self Harm in Early Adolescence: Longitudinal Cohort Study" British Medical Journal (26 April 2012).

269 Audrey Young "PM Tells Schools to Act Against Bullies" *The New Zealand Herald* (online ed, New Zealand, 29 March 2011).

270 A Report from the Prime Minister's Chief Science Advisor *Improving the Transition: Reducing Social and Psychological Morbidity During Adolescence* (prepared for the Prime Minister by the Office of the Prime Minister's Science Advisory Committee, May 2011).

environment in which young New Zealanders were growing up:[271]

> The nature of peer pressure and role models has been radically altered by exposure to electronically connected social networks and to very different media content. Young people have far greater freedom, engendered by more ready access to funds. While the exact impact of these changes is difficult to ascertain, it is clear they have radically affected the social pressures that influence adolescent behaviour. This creates challenges for parents and society in establishing boundaries and acceptable behaviours.

6.6 The PMCSA report also emphasised the importance of evidence-based policy when tackling problems such as New Zealand's high youth mortality rates, alcohol and drug related problems, violence, and the spectrum of mental and behavioural disorders.

6.7 Reviewing the effectiveness of education policy is well beyond the scope of the Law Commission's original terms of reference for this project and we make no claim to expertise in this area. Our task is to assess the adequacy of the law with respect to harmful digital communications, of which cyber-bullying is an example. However, cyber-bullying must be addressed within the broader context of strategies for combatting adolescent aggression and bullying. The law performs a critical part in anchoring educational strategies for combatting bullying, but it can only go so far when dealing with minors.

6.8 In this chapter, we provide an overview of the legal framework which operates in the education sector. We discuss how the law and existing strategies can respond to bullying and cyber-bullying, and consider whether changes to that framework are required.

6.9 In preparing this report we reviewed some of the most significant reports and inquiries that have been produced in response to bullying in New Zealand over the past decade, including the two-part report produced by Dr Janis Carroll-Lind on behalf of the Children's Commissioner in 2009/2010, *School Safety* (2009) and *Responsive Schools* (2010).[272]

6.10 We met with staff from the Ministry of Education[273] and also sought the views of Chief Human Rights Commissioner, David Rutherford, who played a pivotal role in advocating for the victims and their families in relation to an inquiry into the response

---

271 Ibid, at 2.

272 Dr Janis Carroll-Lind *School Safety: An Inquiry into the Safety of Students at School* Office of the Children's Commissioner, 2009 (*"School Safety"*); Dr Janis Carroll-Lind *Responsive Schools* Office of the Children's Commissioner, 2010 (*"Responsive Schools"*).

273 We sought to meet with the Education Review Office, but it has not proved possible to do so.

to bullying at Hutt Valley High School,[274] and who is taking a close interest in bullying as a human rights issue.[275] We consulted with NetSafe, which works closely with schools in relation to cyber-bullying. We also met with the Chief Coroner, Judge Neil MacLean.

APPROACHES TO PREVENTING BULLYING

6.11 Although the precise relationship between online and offline aggression is not yet well understood, there is a general consensus that the two are related. People who are respectful, tolerant and aware of their legal rights and responsibilities in relation to their fellow citizens in their physical interactions are unlikely to adopt an entirely different way of relating to others in cyberspace.

6.12 Similarly experts argue that cyber-bullying and other forms of abusive digital communication among adolescents needs to be understood in the broader context of interpersonal and relational aggression and bullying behaviour.[276]

6.13 It is clearly accepted in New Zealand that bullying should be viewed as a whole school problem, requiring a whole-school solution. When anti-bullying initiatives are being developed in a school, all those affected – teachers, boards, parents, students and administrators – should be involved in the full process.[277] There is no shortage of anti-bullying approaches and programmes available, and a number have been successfully trialled and evaluated in New Zealand schools over time.[278]

6.14 The view of the Chief Human Rights Commissioner, David Rutherford, is that it is

274 Office of the Ombudsmen *Report of David McGee, Ombudsmen on Complaints Arising Out of Bullying at Hutt Valley High School in December 2007* (2011).

275 See Human Rights Commission *School Violence, Bullying and Abuse: a Human Rights Analysis* (March 2009).

276 For example a 2005 study by Massey University researcher Juliana Raskauskas found that young people who experienced text-bullying were also likely to be victimised by verbal bullying or relational aggression. Similarly a 2010 study by Otago University researcher Louise Marsh found students involved in text bullying were significantly more likely to be involved in traditional forms of bullying and were less likely to feel safe at school. However the precise relationship between on-line and off-line bullying behaviours is not fully understood.

277 Dr Janis Carroll-Lind *School Safety* Office of the Children's Commissioner, 2009 at 85.

278 These programmes were described in detail in the reports by the Office of the Children's Commissioner: ibid, at 97, and Dr Janis Carroll-Lind *Responsive Schools* Office of the Children's Commissioner, March 2010 at 28.

vitally important that the programme adopted be evidence-based.[279] *School Safety*, the 2009 report by the Office of the Children's Commissioner, concluded that no matter which programme is introduced, to maximise success, schools must first have effective policies and procedures in place.

6.15 In relation to schools' reporting of incidents of violence and abuse, the report found that there was no consistency in the way that schools across New Zealand deal with issues around safety. While recognising the individuality of each school to make its own informed decisions, it proposed that schools should follow the same broad guidelines wherever possible.[280]

6.16 In 2009 the Government introduced the Positive Behaviour for Learning programme (PB4L),[281] led by the Ministry of Education. PB4L adopts a whole school approach to promoting positive behaviour. The Ministry of Education provides a variety of tools and resources on its website for schools in this regard,[282] and additional funding was provided in this year's budget to support the PB4L programme, and the implementation and piloting of other evidence-based programmes.[283]

6.17 In April 2012, the Prime Minister also announced a Youth Mental Health package, including funding for a range of initiatives aim to improve prevention and treatment services for young people with or at risk of mental health problems. The Ministry of Education says a number of school-based initiatives will be delivered as a result of this funding, including making schools more responsible for student well-being, and creating indicators to measure student well-being.[284]

---

279 The Commissioner cites the KiVa anti-bullying program developed in Finland that is being trialled in the United States: see Antti Karna and others "A Large-Scale Evaluation of the KiVa Antibullying Program: Grades 4-6" (2011) 82 Child Development 311 One of the important components of the programme is procedures for handling acute bullying cases that come to the attention of the school.

280 Carroll-Lind *School Safety* at 65.

281 Ministry of Education, Te Kete Purangi website <pb4l.tki.org.nz/About-PB4L/What-is-PB4L>.

282 Ibid <pb4l.tki.org.nz/Deter-bullying/Positive-behaviour-to-deter-bullying>.

283 Ministry of Education <www.minedu.govt.nz/theMinistry/Budget/Budget2012/SpecialEducation.aspx>.

In 2010 the Government provided $45 million of initial funding for the PB4L Action Plan for the first five years of implementation. Budget 2010 provided $15 million additional funding over two years, and Budget 2012 provided a further $15 million of additional funding for 2012/2013 year.

284 Ibid.

LEGAL FRAMEWORK

6.18 At the outset we acknowledge the difficulties created for teachers, principals and Boards of Trustees by increasing public expectation that schools can and should address the myriad social problems that students bring to the classroom each day. As the Post Primary Teachers' Association pointed out in their submission, cyber-bullying presents particular challenges in this respect because it "occupies the blurred space between home and school so it is not always clear whose responsibility it is."

6.19 However, from an educational point of view, student achievement can be detrimentally impacted by both bullying and cyber-bullying behaviours. Where students generally feel safe and positive in the school environment, this is likely to have a key influence on learning outcomes. Schools therefore have a role in promoting positive psychosocial development, in addition to fostering academic achievement. As ERO notes:[285]

> Students cannot learn effectively if they are physically or verbally abused, victims of violence, racial or sexual harassment, discrimination or bullying, or if their school surroundings are unsafe….
>
> Providing a safe physical and emotional environment (including safety on the Internet) for students at school is one of the basic responsibilities of each board of trustees. However, it is also one of the requirements that is most difficult for boards to address, both because there are so many factors that impact on student safety, and because safety issues do not always have clear solutions.

6.20 From a legal point of view it is clear that the boards of trustees of New Zealand state schools are required to provide a safe physical and emotional environment for their students, and comply in full with any legislation developed to ensure the safety of students and employees.[286]

6.21 The National Administration Guidelines (NAGs) issued by the Ministry of Education set out statements of desirable principles of conduct or administration.[287] NAG 5

285 Education Review Office *Guidelines for Board Assurance Statement and Self-Audit Checklists* (2011) at 23.

286 National Administration Guidelines 5(a) and (c). Section 60A of the Education Act 1989 provides that the Minister may publish these guidelines by notice in the Gazette, as part of the National Education Guidelines (NEGs). The National Administration Guidelines (NAGs) set out the administrative framework that Boards of Trustees must use to work towards the NEGs. There should be policies and procedures in place in each school to achieve the NAGs.

287 There may be a case for considering whether the overarching obligation on schools to provide a safe environment for students should be placed on a stronger legislative footing, for example in the Education Act itself rather than remaining in a subordinate instrument such as the Guideline. Possible advantages of elevating the requirement into legislation might include confirmation of the importance and priority to be

provides as follows:

> Each board of trustees is also required to:
>
> (a) provide a safe physical and emotional environment for students;
>
> (b) promote healthy food and nutrition for all students; and
>
> (c) comply in full with any legislation currently in force or that may be developed to ensure the safety of students and employees.

6.22 The Education Act 1989 also requires the principal of a state school to take all reasonable steps to ensure that students get good guidance and counselling, and to tell a student's parents of matters that in the principal's opinion are preventing or slowing the student's progress through the school, or are harming the student's relationships with teachers or other students.[288] Teachers and Boards of Trustees must report to parents any matters that may put a student at risk of not achieving.[289] Registered teachers also have an ethical obligation to promote the physical, emotional, social, intellectual and spiritual wellbeing of learners.[290]

6.23 These Education Act obligations apply only to state schools. There are no equivalent legislative obligations that apply to private schools. In 2009, the Law Commission recommended that the registration criteria set out in legislation for private schools should contain a requirement that a school must provide a safe and supportive environment that includes policies and procedures that make provision for the welfare of students.[291] This recommendation has not been implemented.

6.24 The Education Review Office (ERO) evaluates and reports on the education and care of students in schools and early childhood services, and the implementation of government education priorities in these sectors. Most schools are reviewed every three years.

6.25 As part of a review of an individual state school, ERO asks the Board of Trustees to attest to compliance with a range of legislation and regulation. It specifically investigates the following areas of compliance: students' physical and emotional safety

---

given to student safety, and giving greater prominence to student safety in the overall legislative framework. In the time available to prepare this report however, we have not had the opportunity to carry out the necessary investigation and consultation on this option to be able to reach any particular conclusions.

288 Education Act 1989, s 77.

289 National Administration Guideline (1).

290 New Zealand Teachers' Council *Code of Ethics for Registered Teachers* (2004) at (1)(f).

291 Law Commission *Private Schools and the Law* (NZLC R108, 2009).

(including prevention of bullying and sexual harassment); stand-downs, suspensions and exclusions; teacher registration; and student attendance.[292] ERO follows up on items where the school reports non-compliance or says that it is "unsure."

6.26 ERO highlighted issues of bullying in a 2007 report which sets out its expectations of good practice by schools in both the prevention and management of bullying. ERO expects that, as a matter of good practice, schools will:

(a) monitor incidents of bullying;

(b) develop, update or review anti-bullying policies and procedures;

(c) include in existing policies ways to deal with text bullying;

(d) report self-review findings to the board of trustees and wider school community;

(e) provide professional development for teachers related to particular anti-bullying programmes or strategies;

(f) implement or extend anti-bullying programmes for students; and offer workshops and support for parents.

6.27 In relation to private schools, during the Law Commission's 2009 review of private schools, ERO expressed concern that the existing criteria for registration for private schools did not give it sufficient power to comment on matters such as a tolerance for bullying, unless it could fit them under some other head such as "standard of tuition" or "suitable staffing".[293]

6.28 The responsibilities of schools to provide a safe environment are reinforced by other statutes including the Health and Safety in Employment Act 1992.[294] This statute primarily protects staff from harm as it regulates workplaces, but indirectly provides students as people "in the vicinity of a workplace" with some protection from

---

292 Education Review Office *Framework for Schools* (2011) at 6. <www.ero.govt.nz>.

293 Law Commission *Private Schools and the Law* (NZLC R108, 2009) at [2.54].

294 See Ministry of Education *Health and Safety in Schools: Guidelines to the Health and Safety in Employment Act and the Health and Safety Code of Practice for State and State Intergrated Schools* <www.minedu.govt.nz>. The Code has been notified under section 70 of the Education Act 1989, which allows the Secretary of Education to specify terms and conditions including such matters as minimum safety and health requirements by notice in the New Zealand Gazette, and so state and integrated schools are obliged to comply with it (but not private schools). Separate codes for State Schools and State Integrated Schools were merged into one code in 2003. While the Code deals with particular matters of health and safety such as construction work, noise, heating, and first aid, it does not refer specifically to bullying. The Code requires schools to keep a register of accidents and serious harm (affecting staff and students); however, "serious harm" is limited to physical injury or hospitalisation.

hazards.[295] The Act requires a register to be kept of accidents and near miss incidents.

6.29 Finally it is worth noting obligations under international instruments such as the United Nations Convention on the Rights of the Child.[296] Article 19 provides:

> (1) States Parties shall take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any person who has care of the child.
>
> (2) Such protective measures should, as appropriate, include effective procedures for the establishment of social programmes to provide necessary support for the child and for those who have the care of the child, as well as for other forms of prevention and for identification, reporting, referral, investigation, treatment and follow-up of instances of child maltreatment described heretofore, and, as appropriate, for judicial involvement.

6.30 Bullying and violence in schools is an issue that has arisen in New Zealand reports under articles 16 and 17 of the International Covenant on Economic, Social and Cultural Rights.[297]

EFFECTIVENESS OF LEGAL FRAMEWORK

6.31 How effective is the current legal framework in operation? Despite the legal obligations that exist, the 2009 *School Safety* report by the Office of the Children's Commissioner found that a minority of schools either had no systems in place, or those systems were not robust enough to cope when things go wrong. It proposed that schools should follow the same broad guidelines wherever possible.[298] NetSafe has also told us that many of the schools it deals with do not have effective policies in place.

---

295 Health and Safety in Employment Act 1992, s 5, s 16. "Hazard" is broadly defined in the Act as any activity or event (whether arising or caused within or outside a place of work) that is an actual or potential source of harm, and includes a situation where a person's behaviour may be an actual or potential source of harm to another person. But while the definition of "harm" includes both physical and mental harm, the latter must be caused by work-related stress.

296 For other relevant instruments, see Human Rights Commission *School Violence, Bullying and Abuse: A Human Rights Analysis* (2009) at [10].

297 Human Rights Commission *Consideration of New Zealand's third periodic report on the implementation of the International Covenant on Economic, Social and Cultural Rights* (submission to Committee on Economic, Social and Cultural Rights, March 2012) at [3.11]. See [6.53] below.

298 Carroll-Lind *School Safety* at 132.

Ombudsman's inquiry

6.32 An example of that kind of situation can be found in the events that occurred in December 2007 at Hutt Valley High School, when a number of violent assaults took place. Both the victims and the perpetrators were students of the school. A group of parents laid complaints with the Office of the Ombudsmen, prompted by the school's refusal to retract a public statement made about it having handled the incidents reasonably and responsibly.

6.33 Ombudsman David McGee investigated and presented a report on the matter to the House of Representatives in September 2011.[299] The investigation covered how the incidents were handled by the School, Child Youth and Family (part of the Ministry of Social Development), the Education Review Office, and the Ministry of Education.

6.34 The Ombudsman made a number of findings and suggestions for change. When the events in question occurred, the school did not have any targeted anti-bullying programmes or policies in place. The Ombudsman concluded that if there had been a mandatory obligation on the school to implement an anti-bullying programme, the events that occurred in December 2007 are less likely to have happened. He considered that the national framework needed to be strengthened, and that it should be compulsory for all schools to implement an anti-bullying programme.

6.35 In the Ombudsman's view, the most appropriate vehicle for effecting this change was an amendment to National Administration Guideline 5, to require each board of trustees to implement an effective anti-bullying programme. Inclusion of the requirement in the Guideline would emphasise the pivotal importance of student safety in this area.[300]

6.36 Monitoring of the anti-bullying policies would continue to be undertaken by Education Review Office in accordance with procedures it already had in place.[301]

6.37 The Ombudsman also suggested that to complement the requirement for mandatory anti-bullying programmes, schools should be given more specific guidance on the levels of punishment that should be given for various infringements.[302]

---

299 Office of the Ombudsman *Report of David McGee, Ombudsman, on Complaints arising out of Bullying at Hutt Valley High School in December 2007* (2011).

300 Ibid, at 39.

301 Education Review Office *Safe Schools, Strategies to Prevent Bullying* (May 2007).

302 Ibid.

Research findings

6.38 As we have noted, the Children's Commissioner's *School Safety* report found there was no consistency in the way that New Zealand schools deal with issues around safety.[303] The Australian Government has commissioned research into covert and cyber-bullying. Two studies investigated the prevalence and impact of covert bullying (including cyber-bullying) and made a number of recommendations to address the issue in Australian schools.[304]

6.39 A recent comparative study found some significant differences in the content of anti-bullying policies between schools in New Zealand and schools in Victoria, Australia. In Victorian schools, bullying policies have been mandatory since 2003, and resources have been provided to support schools in developing such policies. In relation to the approach taken by New Zealand schools, the researchers noted:[305]

> While the Board [of Trustees] sets goals and policies, the governance structure allows for variation in how schools might develop and implement policies. Some schools take a zero tolerance perspective on problem behaviours, using suspensions and expulsions, whereas other schools look for more innovative ways to keep students attached to school, through restorative practices and other processes.

6.40 14 of the 267 responding New Zealand schools did not have an anti-bullying policy. Of the remainder, one-third of the New Zealand schools had a specific anti-bullying policy separate from other policies, as opposed to 75 per cent of the Australian schools. Most of the New Zealand schools embedded their anti-bullying policies in their behaviour management or discipline policies, whereas those of the Victorian schools were more likely to be found in their student engagement documents.[306]

6.41 The review suggested that the differences between New Zealand and Victorian policies

303 Carroll-Lind *School Safety*.

304 D Cross and others *Australian Covert Bullying Prevalence Study* (Child Health Promotion Research Centre, Edith Cowan University, Perth, 2009) [ACBPS]; B Spears and others, *Behind the Scenes: Insights into the Human Dimension of Covert Bullying* (Hawke Research Institute for Sustainable Societies, Centre of the Analysis of Educational Futures, University of South Australia, 2008).

305 L Marsh and others "Content analysis of school anti-bullying policies: a comparison between New Zealand and Victoria, Australia" (2011) 22 Health Promotion Journal of Australia 172 at 173. The researchers randomly selected 640 New Zealand schools (out of a possible total of 2582) towards the end of the 2009 academic year, and asked each for their anti-bullying policy. 42 per cent of the schools replied. The sample therefore included 267 schools (or 10 per cent of the total schools in the country). The researchers noted that additional policies could not be obtained from websites, as it seemed rare for schools to place their policies online.

306 Ibid at 174.

might indicate that more comprehensive anti-bullying policy formation by schools requires an element of necessity (schools must have a policy) and adequate government resources to develop a separate policy.[307]

6.42 The review also noted that many New Zealand schools lacked an inclusive description of what constitutes bullying behaviours:[308]

> Clearly defining bullying communicates to the whole school community what behaviours are not acceptable, and makes the implementation, enforcement, and monitoring of the policy more successful.

6.43 One of the main differences between schools in Victoria and New Zealand was the relatively low number of New Zealand schools that included cyber and mobile phone bullying in their definition.[309] Bullying outside school was infrequently mentioned overall.

6.44 The study concluded:[310]

> As in England and Victoria, NZ schools may benefit from Ministry of Education provision of clear guidelines on how to develop effective policies and what the minimum standard should be for these policies, while at the same time allowing schools the autonomy to develop a policy that specifically suits each school's needs. By developing a comprehensive policy which details what bullying behaviour involves, how the school will respond to incidents of bullying, recording and maintaining data on bullying incidents, having a comprehensive strategy for bullying prevention and periodically evaluating the policy, schools are more likely to reduce bullying in their schools.

Human Rights Commission

6.45 The Human Rights Commission (HRC) has expressed the view that the prevalence of peer to peer violence and abuse in schools shows that the current legislative and regulatory framework fails to provide enough protection for children and young people.[311] Building on the suggestions made in the Ombudsman's 2011 report, the HRC proposes that legislation be enacted to require all schools (public, private and integrated) to:

(a) implement school safety programmes and policies on a whole-school basis;

---

307 Ibid at 175.

308 Ibid.

309 Ibid at 176.

310 Ibid.

311 Human Rights Commission *Consideration of New Zealand's third periodic report on the implementation of the International Covenant on Economic, Social and Cultural Rights* (submission to Committee on Economic, Social and Cultural Rights, March 2012) at [3.10].

(b) appoint and train safety officers who will facilitate responses to violence, abuse and bullying;

(c) institute a process to respond to complaints of violence, bullying and harassment; and

(d) report annually to the Education Review Office on whole-school approaches to school safety; the number of incidents of violence, abuse and bullying; and complaint outcomes.

6.46 The HRC has expressed its commitment to advocating for and monitoring progress in implementing a national response to bullying, violence and abuse in schools including legislative, policy and/or practice changes required to improve students' safety at school.

Law Commission's view

6.47 Based on the research findings noted above and the views put forward by the Ombudsman, the Human Rights Commission and NetSafe, we support the introduction of a mandatory requirement for the adoption of anti-bullying policies in all schools. Specifically, we support Ombudsman McGee's suggestion of an amendment to National Administration Guideline 5 to require public schools to implement anti-bullying policies.

6.48 When it considered Ombudsman McGee's report on incidents at Hutt Valley High in 2007, the Education and Science Select Committee was persuaded by the submission of the Ministry of Education that it was not necessary to take such a step, and that a number of the issues raised in the report are being adequately addressed. The Ministry was not in favour of the proposed amendment to NAG 5 to require anti-bullying programmes:[312]

> It considered that in the several years since the incidents, it has come to be expected that all schools will have systems and processes to manage bullying. The ministry was concerned that the processes used in some schools might not constitute "anti-bullying programmes," although they might be effective in a particular school's circumstances. The change might thus impose obligations on some schools without significantly improving the environment for children.
>
> The ministry also said that guidance material for boards of trustees on applying Guideline 5 is being developed. The ministry's Core Governance Knowledge Base is designed to equip boards of trustees and principals to manage health and safety issues appropriately, and one section focuses on creating a positive school environment to reduce bullying.

312 Education and Science Committee *Report from an Ombudsman, Complaints Arising out of Bullying at Hutt Valley High School in December 2007"* (NZ House of Representatives, 3 May 2012) at 3.

6.49 Despite the reservations expressed by the Ministry of Education in response to the Ombudsman's report, we consider there must be a clear requirement for schools to have specific anti-bullying policies and procedures in place. For state schools, this could be implemented by an amendment to National Administration Guideline 5, as Ombudsman McGee suggested in his report. Evidence we received from NetSafe indicates that bullying is a major issue in schools, that many schools still do not have effective anti-bullying policies in place, and that there is a lack of awareness and resourcing in schools to manage the issue effectively. We consider it is vitally important to ensure that *all* schools have appropriate policies and procedures in place. We note this is the expectation of the Minister of Education.[313] At present that is not the case.

6.50 In our view, an equivalent requirement should extend to private schools. It should be a criterion for registration that the school provide a safe and supportive environment that includes policies and procedures that make provision for the welfare of students.[314] Private schools are subject to a different regulatory system and are not subject to the Guidelines. It will be necessary to ensure that management of this issue can be monitored by ERO and reported on to parents as part of any private school review.

MEASUREMENT

6.51 The comparative Victoria/New Zealand survey discussed above notes the importance of recording and maintaining data on bullying incidents, and periodic re-evaluation of bullying policies.

6.52 In 2007, the Education Review Office found that schools' measurement of the effectiveness of their anti-bullying initiatives was often anecdotal in nature, or was measured more broadly against analyses of incident reports and decreases in the number of detentions or stand-downs. ERO recommended that schools evaluate the effectiveness and impact of their anti-bullying initiatives through a regular self-review programme. ERO provided some questions to support schools in this process, which were endorsed and extended by the Office of the Children's Commissioner in its report

313 Hon Anne Tolley, former Minister of Education, Letter to all Boards of Trustees (4 April 2011) <www.minedu.govt.nz>.

314 This is consistent with an earlier recommendation: Law Commission *Private Schools and the Law* (NZLC R108, 2009) at R14.

into school safety.[315] The report also referred to a range of school climate surveys available to assist schools in measuring the safety of their physical and emotional environment.

6.53 Collation and management of data on violence and bullying in schools continues to be an issue. In May 2012, the United Nations Committee on Economic, Social and Cultural Rights released its conclusions on the consideration of reports submitted by State parties under articles 16 and 17 of the International Covenant on Economic Social and Cultural Rights. In relation to New Zealand, the Committee noted with concern that violence and bullying were widespread in schools, and endorsed the Human Rights Commission's proposals for New Zealand to:[316]

(a) systematically collect data on violence and bullying in schools;

(b) monitor the impact of the student mental health and wellbeing initiatives recently introduced in schools on the reduction of the incidence of violence and bullying; and

(c) assess the effectiveness of measures, legislative or otherwise, in countering violence and bullying.

6.54 In Australia, the emergence of new technologies has led to covert and cyber-bullying becoming an issue for many schools. The Australian Government commissioned two research projects to better understand these issues and the impact on Australian schools.

6.55 The first study, the Australian Covert Bullying Prevalence Study (ACBPS), investigated the prevalence and impact of covert bullying (including cyber-bullying) in Australian school communities. Covert bullying was broadly defined as any form of aggressive behaviour that is repeated, intended to cause harm and characterised by an imbalance of power, and is 'hidden', out of sight of, or unacknowledged by adults.

6.56 Cyber-bullying was defined by young people as cruel covert bullying used primarily by young people to harm others using technology such as: social networking sites, other chat-rooms, mobile phones, websites and web-cameras.[317]

6.57 The resulting report made a number of recommendations to address covert and cyber-

315 Carroll-Lind *School Safety* at 79-80.

316 Human Rights Commission "Commission welcomes UN Committee recommendations on social, economic and political rights" (media release, 25 May 2012).

317 D Cross and others *Australian Covert Bullying Prevalence Study* (Child Health Promotion Research Centre, Edith Cowan University, Perth, 2009) (ACBPS) at xxi.

bullying in Australian schools. Recommendations for national policy and practice included:[318]

(a) Establish an Australian Council for Bullying Prevention that reports to the Prime Minister to lead the review of the National Safe Schools Framework and the concurrent development of a strategy that considers the other recommendations made in the report.

(b) Revise the National Safe Schools Framework and its implementation in schools to explicitly encourage schools to address covert and overt bullying and provide the necessary resources to support schools to minimise this bullying through their policy and practice.

(c) Establish ongoing and routine data collection systems with standardised methods for defining and measuring covert and overt forms of bullying.

6.58 The second study also recommended a review of the National Safe Schools Framework and the Bullying No Way website[319] to address and include more on the issues of covert and cyber-bullying.[320]

Law Commission's view

6.59 We note that in his 2011 report, the Prime Minister's Chief Science Advisor emphasised the importance of evidence-based policy. In order to develop evidence-based policy in the area of bullying and cyber-bullying, and assess its effectiveness, New Zealand needs reliable data relating to incidents of inappropriate student behaviour and complaints received about bullying. The development of measurable objectives and performance indicators for activities intended to improve school safety is also critical.

REPORTING

6.60 One of the key concerns of the Human Rights Commissioner, is the lack of a clear framework for schools around the reporting of violence and bullying by schools internally and to parents (of both bully and victim) and external agencies such as ERO,

318 Ibid, at xxxi.

319 Bullying No Way website <www.bullyingnoway.gov.au>.

320 B Spears and others, *Behind the Scenes: Insights into the Human Dimension of Covert Bullying* (Hawke Research Institute for Sustainable Societies, Centre of the Analysis of Educational Futures, University of South Australia, 2008).

Child Youth and Family and the Police. In his view there needs to be clear guidelines about reporting procedures, particularly in serious cases.

Law Commission's view

6.61 We agree that it is highly desirable for schools to be equipped with clear models that provide processes for informing the relevant personnel within schools, including the Principal, as well as parents and external agencies as appropriate in the circumstances of any particular incident. In particular, we suggest that there needs to be a clear integration of schools' anti-bullying policies with the right of parents to be informed.

ANTI-BULLYING LEGISLATION

6.62 A number of overseas jurisdictions have opted to take a legislative approach to the problem of bullying, including cyber-bullying. In Canada, Nova Scotia, Ontario and Quebec have all introduced anti-bullying legislation,[321] and New Brunswick and British Columbia have indicated their intentions to do the same.

6.63 The Ontario and Quebec Bills both contain definitions of bullying, which include cyber-bullying, and require schools to adopt and implement anti-bullying and anti-violence policies or plans. Both Bills amend education legislation, but do not amend the criminal code.

6.64 In Nova Scotia, a recent report recommended amendments to the Education Act relating to jurisdiction over bullying that occurs off-site, mandatory reporting by principals, and ensuring that schools have appropriate policies in place. [322] The report also recommended that the Education Act be amended to include a provision requiring parents to take reasonable steps to be aware of their children's online activities, at least to the extent that such activities may detrimentally affect the school climate, and to report relevant information to the school principal or other relevant staff.

6.65 Bill No 27, a private member's Bill, was also introduced into Nova Scotia's General Assembly in April of this year.[323] The Bill provides that any youth who cyber-bullies

321 Bill No 56 (Quebec) (an Act to prevent and deal with bullying and violence in schools) was introduced in early 2012.

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

323 Bill No 27, Cyberbullying Intervention Act (An Act to Promote Cyberbullying Intervention and Parental Responsibility) The Bill defines cyberbully as meaning to use the Internet or any other form of electronic communication, including social media, emails and text messages, deliberately or recklessly, to cause,

commits an offence, and that parents also commit an offence if they knew or ought to have known the youth was Cyber-bullying.

6.66 In the United States, state legislation relating to bullying has grown rapidly in the last 13 years.[324] A flurry of legislative action was triggered by the Columbine High School shootings in 1999, and later fuelled by a number of highly visible suicides among school-aged children and teenagers that were linked to bullying.[325] This is particularly noteworthy in a country in which freedom of speech is a fiercely protected value.

6.67 Out of the 46 states with anti-bullying laws in place, 36 have provisions that prohibit cyber-bullying and 13 have statutes that grant schools the authority to address off-campus behaviour that creates a hostile school environment. The most commonly covered key components in state legislation are the development and implementation of district policies, the scope of jurisdiction over bullying acts, definitions of prohibited behaviour, and disciplinary consequences.[326]

6.68 In Australia, the National Safe Schools Framework (NSSF) is strengthened by legislation that requires all schools to align their policies with the guiding principles of the Framework.

6.69 In June 2011, a Joint Select Committee on Cyber-Safety tabled its report on the Inquiry into Cyber-Safety entitled *High-Wire Act: Cyber-Safety and the Young*. Among its recommendations, it proposed the development of an agreed definition of cyber-bullying to be used by all Australian government departments and agencies, and encourage its use nationally. It also recommended that a legislative approach be developed to enable schools to deal with bullying incidents out of school hours.

6.70 New South Wales explicitly criminalises bullying and cyber-bullying in relation to school children. Section 60E of the Crimes Act 1900 (NSW) makes it an offence punishable by imprisonment to assault, stalk, harass or intimidate any school student or member of staff of a school while that student or staff member is attending a school, whether or not any actual bodily harm occurs. The section does not cover bullying outside school premises.

---

directly or indirectly, harm to another person. Under the Bill "harm" means physical or emotional harm to a person that would also harm a reasonable person in those circumstances.

324 V Stuart-Cassel, A Bell and JF Springer *Analysis of State Bullying Laws and Policies* (US Department of Education, Washington DC, 2011).

325 Ibid, at ix.

326 Ibid, at 79.

Law Commission's view

6.71 Beyond the recommendations we make in relation to the amendment of National Administration Guideline 5 and changes required for private schools, we do not presently support specific legislation relating to cyber-bullying or bullying in New Zealand.

6.72 Cyber-bullying and bullying may of course be dealt with under existing New Zealand law, subject to restrictions around the age of criminal responsibility.[327] For example, some instances of physical bullying may constitute an offence, such as assault. The same would apply with the new communications offence that we recommend in chapter 4 for inclusion in the Summary Offences Act 1981. That offence may well apply to some cases of cyber-bullying, where the offender is 14 or older.

6.73 We also envisage that children, parents and schools may apply for orders to the new tribunal that we recommend in chapter 5 of this report.

6.74 However we think it is the new approved agency which we recommend in chapter 5 that will be of the most practical assistance to students, parents and schools when issues related to cyber-bullying arise. We note in this regard that NetSafe is already very active in this area, and has strong established relationships with many schools, with the Ministry of Education, the Police, and companies like Facebook and Google. NetSafe has a dedicated cyber-bullying website offering advice to parents, schools and young people.[328]

6.75 One of the practical recommendations NetSafe makes for schools and teachers is the development of a class contract, that includes appropriate behaviour "online and on mobile" both inside and outside of school time. NetSafe also recommends that all schools have a suitable ICT Use Agreement (for which it provides templates) and ensure that students understand the terms of those agreements. We endorse the value of this practice. We suggest that further work could be done to develop the educative potential of ICT Use Agreements, for example by adopting the set of principles discussed in chapter 5 as an educative tool.

---

327 In New Zealand, the minimum age of criminal responsibility is 10, but children under the age of 14 cannot be prosecuted except for the offences of murder and manslaughter. In all other cases, the matter must be dealt with by way of a Family Group Conference and if necessary, an application can be made to the Family Court that the young person is in need of care and protection. The Youth Court deals with young persons aged 14 or over but under 17. A young person 17 or over who commits offences is dealt with as an adult in the District Court or, if the offence is serious, in the High Court.

328 NetSafe, Cyberbullying Website <http://www.cyberbullying.org.nz>.

6.76 The recent Australian inquiry into cyber-safety commented on the importance of "Acceptable Use Agreements" and supporting policies covering the use of the technology supplied to students. However it found that these agreements are not always backed by procedures that are followed consistently, or even widely known and understood:[329]

> For such Agreements to be effective, they must be:
>
> - clear about the rights and responsibilities of users, especially penalties for breaches of conditions of use;
> - signed by students and parents/carers;
> - preceded by information sessions on cyber-safety, perhaps presented wholly or partially by the young people themselves, and
> - supported by policies that are known and understood by all staff and students, so that they can be implemented promptly, effectively and consistently.

6.77 NetSafe has developed the concept of Digital Citizenship in New Zealand schools, a model which aims to produce confident, capable digital citizens with a combination of technical and social skills that enable them to be successful and safe in the internet age. If the tribunal that we recommend in chapter 5 is established, we anticipate that the terms of future ICT Use Agreements in schools could refer to the statement of principles which form the basis of the tribunal's jurisdiction. This would help confirm the legal basis of digital citizenship in New Zealand schools, setting out a clear statement of what is and is not acceptable conduct on the internet.

CONCLUSIONS

6.78 The weight of international and New Zealand evidence supports the view that cyber-bullying should not be approached as a discrete practice but as a manifestation of intentionally harmful acts perpetrated and experienced by adolescents within the context of individual and peer relationships. However, it is critical that policy makers are alert to the very real differences between covert and overt forms of aggression, and in particular the unique challenges created by digitally mediated bullying and harassment which crosses over the boundary between school and home life.

6.79 Similarly, it is important that the risks associated with bullying generally and cyber-bullying specifically, including the association with suicide, are understood within the wider broader context of adolescent health and wellbeing. In this respect the PMCSA

329 Joint Select Committee on Cyber-Safety, Parliament of the Commonwealth of Australia *High-Wire Act Cyber-Safety and the Young* (interim report, 2011) at 261-262.

report provides an invaluable resource for policy makers attempting to understand the complex personal, social and environmental factors which are contributing to a range of poor outcomes for New Zealand adolescents.

6.80 We consider that the package of reforms we recommend in this report will be of real assistance in relation to dealing with cyber-bullying by or among adolescents. In particular, the approved agency we recommend, which may be a body such as NetSafe, will be able to assist schools, parents and students by providing advice as to their options, guiding them towards appropriate self-regulatory remedies where those are available, and investigating substantial complaints and liaising with website hosts to request material to be taken down or moderated.

6.81 In particularly serious cases which cannot be otherwise resolved, a school Principal, student or parent may have recourse to the tribunal that we recommend in chapter 5. Principals, along with the Police and Coroners, would be one group provided with direct access to the new tribunal in serious cases involving threats to safety. School Principals will be able to seek the Tribunal's assistance in cases where there is a risk to life including potential contagion effects with respect to youth suicides.

6.82 In addition to these wider reforms, we make some specific comments and recommendations in relation to bullying and cyber-bullying.

6.83 We recommend that National Administration Guideline 5 be amended, to require each board of trustees to implement an effective anti-bullying programme.

6.84 We also recommend that it should be a criterion for registration of a private school that the school provide a safe and supportive environment that includes policies and procedures that make provision for the welfare of students. The last National Report by ERO into school safety and strategies to prevent bullying was published in 2007.[330] That report presented the findings of an analysis of 297 ERO education review reports that included information about what schools were doing to prevent bullying. Given the developments in this area both in New Zealand and overseas in the last five years, we suggest it would be timely for ERO to revisit the subject by way of a national report.

6.85 We encourage the Ministry of Education to consider the following matters that our research and consultation indicate are on-going issues in New Zealand's response to bullying and cyber-bullying:

330 Education Review Office *Safe Schools: Strategies to Prevent Bullying* (May 2007).

(a) the development of an agreed definition of bullying behaviour, including cyber-bullying, and encouraging schools to use it in anti-bullying policies;

(b) the need to establish ongoing and routine data collection systems with standardised methods for defining and measuring covert and overt forms of bullying;

(c) the need for the development of measurable objectives and performance indicators for activities intended to improve school safety;

(d) the need for the development of reporting procedures and guidelines.

Recommendations

R31 National Administration Guideline 5 should be amended, to require each board of trustees to implement an effective anti-bullying programme.

R32 It should be a criterion for registration of a private school that the school provide a safe and supportive environment that includes policies and procedures that make provision for the welfare of students.

R33 The Ministry of Education should consider further work in the following areas:

(a) the development of an agreed definition of bullying behaviour, including cyber-bullying, encouraging schools to use it in anti-bullying policies;

(b) the establishment of ongoing and routine data collection systems with standardised methods for defining and measuring covert and overt forms of bullying;

(c) the development of measurable objectives and performance indicators for activities intended to improve school safety;

(d) the development of guidelines for the reporting of serious incidents of bullying and cyber-bullying.

R34 Consideration should be given to further developing the educative potential of Information and Technology (ICT) contracts to inform students about their legal rights and responsibilities with respect to communications, using for example, the set of principles developed in chapter 5 as an educative tool.

APPENDIX

Communications (New Media) Bill