

Under embargo until 6.00am 15 August 2012



---

LAW·COMMISSION  
TE·AKA·MATUA·O·TE·TURE

---

Wellington, New Zealand | August 2012

## Summary of Ministerial Briefing Paper

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

## 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.<sup>1</sup>
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.<sup>2</sup>
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.<sup>3</sup>
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.

---

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).

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.<sup>4</sup> In this paper we considered the problem of harmful 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

---

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

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 12-18, are:
  - **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.”<sup>5</sup>

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.<sup>6</sup>

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.

---

## 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:

---

<sup>5</sup> Telecommunications Act 2001, s 112(a), s 112(b).

<sup>6</sup> 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.

- 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:<sup>7</sup>

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.

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

---

<sup>7</sup> 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.

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.<sup>8</sup>
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.”<sup>9</sup>
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.”<sup>10</sup>
37. We note that the paucity of quantitative national data on cyber-related communication harms creates challenges for policy makers.
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.<sup>11</sup> Research undertaken

---

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.

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

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.<sup>12</sup>

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.”<sup>13</sup>
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:<sup>14</sup>

[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

---

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.

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.<sup>15</sup>
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.

---

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

## 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.
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:

## Under embargo until 6.00am 15 August 2012

- (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.<sup>16</sup> 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.

#### **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

---

<sup>16</sup> 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.

before they reach the Tribunal.<sup>17</sup> 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.<sup>18</sup> 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”.<sup>19</sup>

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.

### *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

---

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.

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.