

# Regulatory Impact Statement

## Harmful Digital Communications

### Agency disclosure statement

This Regulatory Impact Statement (RIS) was prepared by the Ministry of Justice. It provides an analysis of options to address harmful digital communications by:

- Changes to existing legislation to ensure it responds appropriately to this behaviour and covers technological advances.
- New civil enforcement regime to deal with harmful digital communications.

In August 2012 the Law Commission produced a Ministerial briefing paper entitled *Harmful Digital Communications: The adequacy of the current sanctions and remedies*. This paper will be attached to the Law Commission's report on *The News Media meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age*.

Working from the Law Commission's analysis restricts the range of options that were considered. Also, there are constraints in the analysis, in that the proposal for an approved agency and Tribunal are novel and it is difficult to quantify associated costs.

There will be financial implications of appointing an approved agency. When the regulations are promulgated appointing an approved agency and setting out its functions, precise costs of the agency and any reprioritisation of funding will be finalised.

The preferred policy is likely to impose some minor additional compliance costs on businesses (eg, Internet Service Providers or website hosts may be asked to take down material). The preferred policy options are not likely to:

- Impair private property rights, market competition, or the incentives on businesses to innovate and invest; or
- Override fundamental common law principles (as referenced in Chapter 3 of the Legislation Advisory Committee Guidelines).

Aphra Green  
Policy Manager, Criminal Law  
Ministry of Justice  
Date:

## **Introduction**

1. In August 2012 the Law Commission produced a Ministerial briefing paper entitled *Harmful Digital Communications: The adequacy of the current sanctions and remedies*. This paper will be attached to the Law Commission's report on *The News Media meets 'New Media': Rights, Responsibilities and Regulation in the Digital Age*. Harmful digital communications fall within the ambit of that project and were expedited at the request of the Minister of Justice.
2. The proposals in the Law Commission's Ministerial Briefing can be divided into three areas:
  - 2.1. Changes to existing legislation to ensure it responds appropriately to this behaviour and covers technological advances.
  - 2.2. New civil enforcement regime to deal with harmful digital communications.
  - 2.3. Measures to address cyber-bullying in schools.
3. This Regulatory Impact Statement only deals with the changes to legislation and civil enforcement regime as they fall within the jurisdiction of the Ministry of Justice.

## **Status Quo**

### *Criminal Law*

4. For the most part, harmful digital communications are captured by the current criminal law. Most offences are phrased in technology-neutral language and are able to cover this behaviour. For example, the Crimes Act 1961, Summary Offences Act 1981 and Harassment Act 1997 contain offences for threats and intimidation that apply regardless of how these are conveyed.
5. These offences generally involve a complaint to the Police and the Police then investigate the offence and bring charges. Investigating this type of criminal offending can often involve significant Police time, resources and technical expertise.

### *Civil Law*

6. Alongside the statutorily defined criminal offences, there are also a number of important common law wrongs that can give rise to civil causes of action. The harmful communication giving rise to this action can occur in either traditional or new electronic media. However, it is important to note that civil actions require the aggrieved individual to bring court proceedings and many do not have the means or desire to do so.
7. The civil actions include defamation, invasion of privacy, breach of confidence, breach of copyright and harassment. In addition, while not generally enforceable in the courts, the Privacy Act 1993 and Human Rights Act 1993 offer avenues of redress for certain types of communications. This is via a complaint to the Privacy Commissioner for a breach of privacy; or complaint to the Human Rights Commission.

## Problem Definition

8. Harmful digital communications, cyber-bullying and digital harassment can take a variety of forms, including emails, texts, phone messages, blog sites, forums and social media sites like Facebook or Twitter. These mediums can be used to intimidate, spread damaging or degrading rumours, publish invasive and distressing photographs, and harass people.
9. It is also important to note that the problem of adolescent bullying is wider than harmful online behaviour; international research has found that in many cases the two go hand in hand.
10. What differentiates harmful digital communications and bullying from their offline counterparts is the:
  - 10.1. potential viral nature of the harassment;
  - 10.2. ubiquity and ease of access to technology in modern life;
  - 10.3. ease of dissemination to a global audience;
  - 10.4. persistence of the information and the great difficulty in removing it; and
  - 10.5. facility for anonymity.
11. In other words, the internet has provided a forum for a unique form of harassment that is easy to create and distribute and difficult to remove.
12. There is no precedent for this in the pre-digital world, and the advent of digital communication has brought new ways in which people can cause harm to each other. For example, globally there are 1 billion tweets sent every week, and in New Zealand, Trade Me's forums have 2.8 million users who publish 25,000 new posts every day. The vast majority of which are not harmful.
13. NetSafe estimates that it deals with around 75 complaints of "cyber-bullying" per month. Between April 2009 and June 2011 NetSafe received 1,279 inquiries from members of the public. These inquiries mostly related to text and cyber-bullying and the misuse of social networking sites to victimise, harass, defame or intimidate individuals.
14. In addition, anecdotal evidence from the Police suggests that they are being asked to respond to a "growing number of complaints" relating to this behaviour, although no quantitative data is recorded.
15. Research commissioned by the Law Commission<sup>1</sup> suggests that 1 in 10 New Zealanders have experienced harmful communications on the internet. That number doubles for those aged between 19 and 29. The Law Commission also found that 42% of respondents did not know where to seek help. Research undertaken by Dr John Fenaughty found that 1 in 5 New Zealand school students experienced some form of cyber-bullying or harassment<sup>2</sup>.

---

<sup>1</sup> The Law Commission commissioned independent research company Big Picture to undertake research into a number of issues as part of the Law Commission's review.

<sup>2</sup> John Fenaughty *Challenging Risk: NZ High-school Students' Activity, Challenge, Distress and Resiliency, within Cyberspace* (PhD Dissertation, University of Auckland, 2010).

16. The Courts can take a long time to reach a remedy. In addition, it is often unrealistic for some people to take civil proceedings or lay a complaint with police. These individuals may not have the means or inclination to pursue someone through the courts. Often the material has already done the damage and the person would just like it removed.
17. The Law Commission's Ministerial Briefing makes the point that, often, there is not a lot the Police can do. Further, it can be extremely difficult to get a website, especially those based overseas, to take material down. The Law Commission give an example of it taking months to have a false Facebook page removed; it was only removed once NetSafe became involved.
18. Thus, there are two main problems which arise:
  - 18.1. ensuring that harmful digital communications are covered by the law; and
  - 18.2. providing a range of accessible legal options for people who experience harmful digital communications.

### **Objectives**

19. The proposals in the paper are designed to address concerns regarding the role of digital communications in causing significant harm. This offending on the internet differs in that there is the potential for the information to be very quickly disseminated to a worldwide audience; it can easily be anonymous; and difficult to remove permanently.
20. Options for legislative amendment to address this harm are assessed by the following criteria:
  - 20.1. Ensuring that legislation is effective for a digital age; and
  - 20.2. Ensuring that legislation provides protection for those significantly harmed by this behaviour.
21. Options for providing a remedy to people who experience this harm are assessed by the following criteria:
  - 21.1. Ensuring an effective and accessible remedy for victims;
  - 21.2. Ensuring the response is proportionate to the harm;
  - 21.3. The remedy is cost effective; and
  - 21.4. The remedy is quick.

### **Regulatory Impact Analysis**

22. The regulatory impact analysis below has been separated into three sections – new offences, updating legislation and civil enforcement regime.

## ***New Offences***

### *Status quo*

23. As noted above, harmful digital communications or cyber-bullying are mostly captured by the current criminal law. However, in its analysis, the Law Commission also identified a few areas in which harmful communications fall into gaps in the law.
24. A number of overseas jurisdictions are moving to criminalise communications causing serious distress and mental harm (eg, the United Kingdom, Australia and the United States).

### *Problem*

25. As noted above, the new communications technologies can have effects that are more intrusive and more pervasive, and thus cause greater harm, than many other forms of communication. The potential for emotional harm is greater than in the pre-digital age. There is also a risk that it may lead to self-harm or suicide.
26. The criminal law needs to ensure that communications that cause serious distress and mental harm are captured.

### *Options*

27. Two options have been identified:
  - 27.1. Maintain the status quo; or
  - 27.2. Create new offences to ensure this behaviour is covered.
28. New offences of using a communications device to cause harm in the Summary Offences Act 1981 and incitement to suicide where actual or attempted suicide does not result in the Crimes Act 1961 are proposed to address these gaps.

### *Objectives and considerations*

29. There is a risk with maintaining the status quo that some harmful digital communications will not be captured by the law. In particular incitement to suicide, even if no suicide or attempt results, can cause significant distress.

#### *New communications offence*

30. The new offence is proposed in the Summary Offences Act 1981, of using a communications device to cause harm. This offence would apply to a person who sends a message to another person that is grossly offensive, indecent, obscene, menacing or knowingly false and intends the message to cause substantial emotional distress to the recipient.
31. This new offence applies regardless of how the harmful digital communication is communicated and makes certain that those who are subject to this behaviour have an effective remedy.

32. It is proposed that this new offence be punishable by a maximum of three months' imprisonment or a \$2000 fine.

*Incitement to suicide*

33. Currently, it is only an offence under the Crimes Act (punishable by up to 14 years' imprisonment) if suicide is attempted or occurs as a result of the incitement. Given the distress such behaviour can cause, incitement to suicide should be an offence, without the need for actual or attempted suicide to result.
34. A penalty maximum of 14 years' imprisonment reflects the seriousness of the existing offence.
35. It is proposed to create a separate offence for situations where no suicide or attempt occurs. This new offence (with a penalty of up to three years' imprisonment) will ensure that those subject to this behaviour are protected by the criminal law.
36. Modelling completed by the Ministry of Justice for both new offences indicates that removing this requirement would have virtually no impact on the number of prison beds required. It is expected that there will be a small increase in community sentences given for the new offences, but this is expected to have a very small impact on justice system costs.

*Conclusions and recommendations*

37. To ensure that these types of harmful communications are covered by the criminal law, the Ministry of Justice recommends that the two new offences outlined above be created.

**Updating Legislation**

*Status quo*

38. In their Ministerial briefing, the Law Commission concluded that by and large, existing laws are capable of being applied to digital communications. However, a number of statutes have been identified that should be amended to make them applicable to digital communications or be brought up to date. These include the Harassment Act 1997, the Human Rights Act 1993, and the Privacy Act 1993.

*Problem*

39. There is a risk with this option that some harmful digital communications will not be captured due to definitions of various terms in existing legislation.

*Options*

40. Two options have been identified:
- 40.1. Maintain the status quo; or
- 40.2. Make amendments to the Harassment Act 1997, Human Rights Act 1993 and the Privacy Act 1993.

41. These amendments will ensure that these acts apply to digital communications.
42. There are a number of instances in the Harassment Act, Human Rights Act and Privacy Act where amendments are desirable to remove any uncertainty that existing provisions apply to electronic communications.
43. In addition, explicit references to electronic communications will assist in raising awareness of the law and make it clear to the online community that potential liability may arise from making offensive comments online.

#### *Objectives and considerations*

44. The risk with maintaining the status quo is that some behaviour that would be expected to contravene provisions in current legislation these acts will not do so solely because of the forum in which it is communicated. Amending these provisions will ensure that there is a legal remedy available under these acts regardless of how the communication is sent.

#### *Conclusions and recommendations*

45. The Ministry of Justice recommends that the Harassment Act, Human Rights Act and the Privacy Act be amended to ensure they apply to digital communications.

### **Civil Enforcement Regime**

#### *Status quo*

46. Current forms of self regulation on the internet include user generated feedback and comment in many websites (eg, blog sites or YouTube). In addition, many big internet entities have adopted sophisticated automated systems for dealing with offensive or harmful communications (eg, Facebook).
47. Websites predominantly rely on contractual terms and conditions (users must register and agree to comply to use site), and community moderation to establish and maintain “civil behaviour”. There is also the facility on most social media websites to “flag” or report content that is offensive or transgresses the rules in some way.

#### *Problem*

48. In their Ministerial Briefing the Law Commission notes that it is difficult to gauge the effectiveness of community moderation. The Law Commission does provide a number of anecdotal examples of the difficulty in getting offensive content removed.
49. There are a number of distinct challenges in applying the law in cyberspace. These can include a lack of knowledge about law on the part of the victim, and the time it takes and the cost of pursuing someone through the courts. In addition, in its submission to the Law Commission, Police note that not all harmful communications reach the threshold of criminal offending. However, these communications do cause harm and significant distress and a remedy should be available.

50. The current industry self regulation systems and the court system cannot always provide the type of timely, tailored response required in cases of serious harm.

#### *Options*

51. Four options have been identified:
  - 51.1. Maintain the status quo;
  - 51.2. Establish a communications commissioner;
  - 51.3. Create a new Communications Tribunal; or
  - 51.4. Establish a new civil enforcement regime.

#### *Objectives and considerations*

##### *Status quo*

52. As noted above, maintaining the status quo does not provide an effective, accessible, quick and cost effective remedy for victims. As the Law Commission noted in its Ministerial briefing, it can be very difficult for an individual to have something removed from a website and a large number of internet users do not know where to go for help.

##### *Communications commissioner*

53. This option involves creating an independent commissioner that the public can turn to for information and assistance. The role of this person would be to provide information, and where possible assist in solving problems in an informal manner (eg, through mediation).
54. This would address the concern that many of the harms caused by social media and the internet can be traced back to that fact that there is no clearly accessible place to take complaints, concerns or questions.
55. An independent commissioner would help to provide a quick and accessible remedy for victims. However, a commissioner would not have any ability to order a person to remove a harmful publication if mediation and negotiation failed.

##### *Communications Tribunal*

56. This option involves creating a tribunal at a lower level than the court system that could administer quicker and cheaper remedies to those who have been harmed by communications in media of all kinds. This tribunal could function in a similar way to the Disputes Tribunal, Copyright Tribunal or the Tenancy Tribunal.
57. The benefit of a new tribunal is that it would enhance public access to justice. It would be less expensive, less formal and less intimidating than the court. It would provide quicker remedies than the courts and allow for the development of subject matter expertise in communications harms. In addition, it would provide a single point of entry for complainants seeking remedy.

58. However, there may boundary issues between the new tribunal and other existing entities, such as the Office of Privacy Commissioner. In addition, as a single point of entry for complaints, there is a risk that with no filtering mechanism the tribunal could become overwhelmed by a large number of less serious complaints. There is also a risk of the tribunal becoming a censorship body.
59. A new tribunal and the appointment of members would involve significant costs. Further, with the proliferation of tribunals can lead to fragmentation across the court system.

*New civil enforcement regime (preferred option)*

60. This option involves a tiered approach. The first tier is self regulation (as described above). If that is not effective, the second tier is mediation through an approved agency. If the matter is still unresolved the final tier is a special function of the District Court.
61. Speed and easy access is especially important in the realm of digital communications where pursuing ordinary legal remedies is seen as ineffective as information can be disseminated easily and with little cost.
62. Complaints about harmful digital communications will initially be made to an approved agency. The approved agency could assist those harmed by digital communications to resolve their disputes through negotiation and mediation.
63. A further and final avenue for resolution is needed for cases where the approved agency is unable to resolve the situation. This would be via a new function of the District Court. Specific rules and procedures will be put in place to make this forum as fast, efficient and cost effective as possible. For example, rules around timetabling and processes to deal with urgent applications.
64. Only serious cases that have already been considered by the approved agency will come before the court. In addition, the complainant will be required to show that the communication has caused, or is likely to cause, significant emotional distress.
65. The court will be able to issue a broad range of sanctions and remedies, such as, an order to take down material, an order that the defendant cease the conduct or order the publication of a correction.
66. The court will not have the power to impose criminal or monetary sanctions. However, failure to comply with an order would be an offence punishable by a fine.
67. The Ministry of Justice estimates that the costs of the District Court undertaking a role in the new civil enforcement regime would be \$115,000 per annum. This estimate is based on court staff and judicial time for 100 cases per year. This will be absorbed in Ministry of Justice baselines.
68. In addition, this option will likely have an impact on Internet Service Providers (ISPs) and those who host websites, who may be asked to take down material. In cases where the person conducting the harmful communication cannot be identified, the court may issues an order to an ISP to identify the account using the Internet Protocol address (IP address) at the relevant time. Further, there

may be a cost to ISPs or website hosts if they are required to participate in the approved agency's mediation process. However, this will be rare, as it is intended for the mediation to be between the complainant and the author of the communication.

69. It is not expected that this will be a significant cost. In NetSafe's submission to the Law Commission's issues paper, they note that in around 90% of the complaints they receive the victim knows the identity of the perpetrator.

### *Conclusions and Recommendations*

70. The Ministry of Justice recommends that the new civil enforcement regime outlined above be implemented. This will provide victims of harmful communications with recourse to a quick and accessible regime, with the approved agency dealing with minor complaints and only most serious being considered by the court.
71. The Ministry also notes that further work on the financial implications of appointing an approved agency will be set out in detail in a Cabinet paper seeking approval for regulations appointing and setting out the functions of the approved agency.

### **Consultation**

72. The New Zealand Police, the Crown Law Office, Department of Internal Affairs, Treasury, Department of Corrections, Ministry of Social Development, Ministry of Health, Ministry of Women's Affairs and the Parliamentary Counsel Office, Law Commission, the Privacy Commissioner, the Human Rights Commission and NetSafe have been consulted on the proposals in this paper.
73. In formulating their proposals the Law Commission released a discussion document in December 2011, which received 72 public submissions from academics, the media, organisations (eg, facebook) and individuals. In addition, the Law Commission held public discussion forums on three popular blogs.

### **Implementation**

74. The changes discussed in this Regulatory Impact Statement are to be included in an Omnibus Bill that creates a new act (the Communications (New Media) Act) and amends the Crimes Act 1961, Harassment Act 1997, Human Rights Act 1993, Privacy Act 1993 and the Summary Offences Act 1981. It is intended that this Bill be introduced into the House in 2013.
75. The Bill will contain a regulation making power that allows Cabinet to appoint an approved agency and to specify the function, arrangements and processes for the agency.
76. As the Ministry of Justice is responsible for the pieces of legislation being amended, it is intended that the Ministry of Justice administer the legislation.

### **Monitoring, evaluation and review**

77. A review will be conducted after two years to:

- 77.1. Assess whether the new offences are being used, and whether there are any gaps in either the new offences, or the amendments that have been made to existing legislation;
  - 77.2. Assess the effectiveness of the new civil enforcement regime as to whether it is meeting its aim of being an effective, accessible, low cost and quick option for dealing with harmful digital communications.
78. In addition, the further work on the approved agency will identify who will be responsible for the monitoring of the approved agency's work and performance. As well as further analysis on the potential impact on internet service providers and website hosts.