Legislating for E-Manners: Deficiencies and Unintended Consequences of the Harmful Digital Communications Act

STEPHANIE FRANCES PANZIC*

This year, Parliament passed new legislation as an attempt to improve legal protection against online "speech harms". Unfortunately, although the motives behind the Harmful Digital Communications Act 2015 are to be commended, the end result is not. A number of deficiencies mean that the Act is unlikely to provide quick and efficient redress to victims. Its complaints process is poorly drafted and may cause legitimate complaints to fall through the gaps, while frivolous or vexatious complaints reach the District Court. Ultimately, the Act is too far-reaching and may result in a number of unintended consequences.

I INTRODUCTION

It seems that not a day goes by without witnessing, experiencing or reading about harmful communication in the digital world. Stories abound in the media of suicide triggered by bullying via popular social medial platforms such as Twitter and Facebook. Some blogs — and their accompanying comments sections — are festering cesspits, harbouring offensive retorts and personal attacks. Examples of such communication are not difficult to come by:[1]

> ... go root another married man then cry about how you are not good enough for anyone to love, then do your fake suicide crap while you don your sexy black nightie to get his attention again ....

Arguably, a reasonable person would ignore messages like this or perhaps contact the author, website host or administrator to remove them. But when none of these options succeed, the victim's last resort is legal action. Unfortunately, this has also been prone to failure, typically due to cost and evidential issues. As a result, New Zealanders have suffered from the harm caused by digital communications with no easily accessible means of redress.

---

* BSC/LLB(Hons). I would like to thank Judge David Harvey for his invaluable input.

1 *Brown v Sperling* DC Auckland CIV-2012-004-925, 15 June 2012 at [115]. Extracts from the case are reported at *Brown v Sperling* [2012] DCR 753.

Parliament has recently attempted to resolve this issue by enacting the Harmful Digital Communications Act 2015 (the Act). However, instead of creating an efficient system offering remedies, the Act provides regulation that may displace existing law and result in a large number of unintended consequences. Partners breaking up via text message, political satirists, whistleblowers, Internet trolls and others who never expected harm to be suffered because of their communication may all find themselves subject, with no defence, to a civil enforcement regime. The messily drafted complaints procedure means that frivolous or vexatious complaints may clog up the courts, while legitimate complainants struggle to navigate the system.

II PROTECTION FROM HARMFUL DIGITAL COMMUNICATION

The Problem

The adage "[s]ticks and stones will break my bones, but names will never hurt me!" is frequently uttered,[2] but is often inaccurate as a description of law.[3] For thousands of years, society has used law to limit what can be communicated to cause harm. A very early example can be taken from ancient Rome, from a praetorian edict issued in approximately AD 130, which declared that an action could be brought against someone who shouted at another "contrary to good morals".[4] Closer to home, New Zealand has developed an arsenal of laws that, for many years, have successfully constrained both written and spoken word. This collection of criminal and civil statutes and common law principles spans from threats to kill,[5] to the disclosure of private information.[6]

But today's digital world requires us to revisit this previously effective arsenal of laws. Differences between traditional and digital communication mean that what once worked no longer does.[7] Many of these differences are a matter of degree; characteristics that were present in the pre-digital era may be transformed by technology.[8] Taken together, their effects arguably make modern digital communication qualitatively different from non-digital communication, to the extent that special legislative intervention is now required.[9]

---

2 An early recorded instance of which appears in GF Northall *Folk-Phrases of Four Counties* (Oxford University Press, London, 1894) at 23.

3 It often does not hold true in a literal sense, either: see Adrienne Nishina, Jaana Juvonen and Melissa R Witkow "Sticks and Stones May Break My Bones, but Names Will Make Me Feel Sick: The Psychosocial, Somatic, and Scholastic Consequences of Peer Harassment" (2005) 34 Journal of Clinical Child & Adolescent Psychology 37.

4 Jill Harries *Law and Empire in Late Antiquity* (Cambridge University Press, Cambridge, 1999) at 3.

5 Crimes Act 1961, s 306.

6 Privacy Act 1993, s 6.

7 Law Commission *Harmful Digital Communications: The adequacy of the current sanctions and remedies* (NZLC MB3, 2012) at [2.96].

8 David Harvey "Collisions in the Digital Paradigm II — Recorded Law" (20 January 2014) The IT Countrey Justice <theitcountreyjustice.wordpress.com>.

9 Law Commission, above n 7, at [2.96].

The Internet provides greater opportunity for apparent anonymity, as illustrated by Peter Steiner's famous cartoon in *The New Yorker*, captioned: "On the internet, nobody knows you're a dog."[10] There are a number of ways to achieve anonymity.[11] At the simplest level, a pseudonym may be used, such as forging an email header or creating a fake profile on social media. Certain websites even use anonymity as a drawcard, like Ask.fm, a social question-and-answer website.[12] Anonymity may also be achieved through remailers, which strip identifying information from emails and make them appear to have been sent from a different email address.[13]

The main consequences of anonymity are two-fold. First, it may have a disinhibiting effect on communicators, who may say or do things they never would in person.[14] A number of additional factors contribute to disinhibition. These include the absence of face-to-face real-time communication and people's tendency to think of their online behaviour as fictional and separate from the offline world.[15] Secondly, anonymity may exacerbate the victim's feeling of powerlessness.[16] This is amplified by the fact that a single perpetrator can attack from multiple platforms at once — or from multiple accounts on the same platform — creating the illusion that there is more than one assailant.[17]

The ease of disseminating information is another unique property of the digital world.[18] It has never been truer that a lie can travel halfway around the world while the truth is still putting on its shoes.[19] The Internet is not essential for information to "go viral"; information has been doing this for centuries. For example, in 1955, an estimated 40,000 African American people heard about the arrest of Rosa Parks within three days.[20] This information spread via phone, pamphlets and word of mouth, resulting in a boycott of the bus system in protest.[21] However, the Internet undoubtedly increases the speed, reach and frequency of viral events; it enables a "many to many" communication flow where virtually anyone can republish the information.[22] Thanks to digital technology, an embarrassing video of a 15-year-old pretending that a golf ball retriever is a lightsaber can reach tens of

10 Peter Steiner "On the internet, nobody knows you're a dog." *The New Yorker* (New York, 5 July 1993) at 61. The anonymity is only apparent, as in many cases it may be possible to identify someone using Internet Protocol numbers or metadata.

11 David Harvey *internet.law.nz: selected issues* (3rd ed, LexisNexis, Wellington, 2011) at 351.

12 The website has been linked to cyberbullying and suicide: Lizette Alvarez "Girl's Suicide Points to Rise in Apps Used by Cyberbullies" *The New York Times* (online ed, New York, 13 September 2013).

13 Harvey, above n 11, at 351.

14 John Suler "The Online Disinhibition Effect" (2004) 7 CyberPsychology & Behaviour 321 at 321. According to Suler, there are two contrasting types of disinhibition — "toxic disinhibition", exemplified by offensive communication or deviant behaviour, and "benign disinhibition", which is the sharing of personal information and the exhibition of unusual acts of kindness and generosity.

15 At 322–323.

16 Law Commission, above n 7, at [2.42].

17 At [2.42].

18 At [2.42].

19 A saying that was described in the mid-19th century as being an old proverb: CH Spurgeon *Sermons delivered in Exeter Hall, Strand; By the Rev. C.H. Spurgeon during the Enlargement of New Park Street Chapel, Southwark* (Alabaster & Passmore, London, 1855) at 130.

20 Karine Nahon and Jeff Hemsley *Going Viral* (Polity Press, Cambridge (UK), 2013) at 1.

21 At 1.

22 Harvey, above n 8.

millions of viewers within a few days; content no longer needs a pressing cause in order to reach large audiences.[23] The ease with which bystanders can contribute to the harm and the ability for "mob mentality" to emerge only exacerbates this condition.[24]

Unlike traditional bullying, the ubiquity of technology means that it is far more difficult for a victim to "walk away" from cyberbullying.[25] Furthermore, digital information has a high degree of permanence. Information stored on the Internet is never forgotten; it can resurface at any time by virtue of powerful search engine technology.[26]

The media overflows with stories of both children and adults experiencing serious emotional harm as the result of online behaviour.[27] A number of organisations, including NetSafe, the New Zealand Police Association and the New Zealand Post Primary Teachers' Association, claim that such harm is a significant problem.[28] Independent research instigated by the Law Commission suggests that up to one in 10 New Zealanders has experienced harmful digital communication.[29] This rate increases to 22 per cent among 18 to 29-year-olds, who are more frequent users of digital technology than the population as a whole.[30]

In 2011, the Law Commission released an Issues Paper exploring the adequacy of existing law for speech harms in the digital environment.[31] The Law Commission coined the term "harmful digital communication" in a subsequent Ministerial Briefing Paper.[32] The resulting Act defined digital communication as "any form of electronic communication", including "any text message, writing, photograph, picture, recording, or other matter that is communicated electronically", while the Act defined "harm" as "serious emotional distress".[33] The Law Commission found that there were gaps in how the law protected individuals from harmful digital communication,[34] which was true of both the criminal and civil law.[35] According to the Law Commission, the need for additional legal coverage stemmed from how the

23 Daniel J Solove "Speech, Privacy, and Reputation on the Internet" in Saul Levmore and Martha C Nussbaum (eds) *The Offensive Internet: Speech, Privacy and Reputation* (Harvard University Press, Cambridge (Mass), 2010) 15 at 15.

24 See Andrew Murray *Information Technology Law: The law and society* (2nd ed, Oxford University Press, Oxford, 2013) at 144.

25 Law Commission, above n 7, at [2.42]. See also Murray, above n 24, at 157.

26 At [2.42].

27 See, for example, Alecia Bailey "Cyber-bullying blamed for death" *The New Zealand Herald* (online ed, Auckland, 24 February 2013). See also Murray, above n 24, at 157.

28 NetSafe "Submission to the Justice and Electoral Committee addressing the Harmful Digital Communications Bill" at 1; New Zealand Police Association "Harmful Digital Communications Bill: Submission of the New Zealand Police Association" at 3; and New Zealand Post Primary Teachers' Association "Submission to the Law Commission review of the adequacy of the regulatory environment in which New Zealand's news media is operating in the digital era" at [2.1].

29 Law Commission, above n 7, at [2.23].

30 At [2.23].

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

32 Law Commission, above n 7, at [1.21].

33 Harmful Digital Communications Act 2015, s 4.

34 Law Commission, above n 7, at [55].

35 At [55].

digital environment gave individuals unprecedented power to affect others' reputation and wellbeing.[36] It is from this background that the Act emerged.

The Supposed Solution

The purpose of the Act is to:[37]

> (a) deter, prevent, and mitigate harm caused to individuals by digital communications; and
> (b) provide victims of harmful digital communications with a quick and efficient means of redress.

The Act purports to achieve these aims through a civil enforcement regime — which will be the focus of this article — and a new criminal offence. The Act also amends the Crimes Act 1961, Harassment Act 1997, Human Rights Act 1993 and Privacy Act 1993 in order to tailor them to the developing digital world. These amendments are comparatively uncontroversial and will be considered elsewhere in the article where relevant.

1 The Civil Enforcement Regime

The Act is intended to provide a system whereby complaints about harmful digital communications are first considered by an "Approved Agency".[38] The District Court serves as a further avenue if the Approved Agency is unable to resolve the complaint.[39] The Act is unclear on how this process works.[40]

The regime relies upon ten "communication principles":[41]

> *Principle 1*
> A digital communication should not disclose sensitive personal facts about an individual.
>
> *Principle 2*
> A digital communication should not be threatening, intimidating, or menacing.
>
> *Principle 3*
> A digital communication should not be grossly offensive to a reasonable person in the position of the affected individual.
>
> *Principle 4*
> A digital communication should not be indecent or obscene.

36 At [2.96].
37 Harmful Digital Communications Act, s 3.
38 Sections 7 and 8.
39 Section 12(1).
40 For example, it is unclear how the complaint initially reaches the Approved Agency.
41 Section 6(1). See also Law Commission, above n 7, at [5.62]–[5.68].

> *Principle 5*
> A digital communication should not be used to harass an individual.
>
> *Principle 6*
> A digital communication should not make a false allegation.
>
> *Principle 7*
> A digital communication should not contain a matter that is published in breach of confidence.
>
> *Principle 8*
> A digital communication should not incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual.
>
> *Principle 9*
> A digital communication should not incite or encourage an individual to commit suicide.
>
> *Principle 10*
> A digital communication should not denigrate an individual by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation, or disability.

The Approved Agency is to be appointed by the Governor-General by Order in Council.[42] The Law Commission recommended that NetSafe should be appointed to this role, due to its existing function of protecting individuals from harm online.[43] However, the matter is far from decided, with legislators preferring an Order in Council to select any person, organisation, department or Crown entity.[44] The Approved Agency's proposed functions are:[45]

> (a) to receive and assess complaints about harm caused to individuals by digital communications:
> (b) to investigate complaints:
> (c) to use advice, negotiation, mediation, and persuasion (as appropriate) to resolve complaints:
> (d) to establish and maintain relationships with domestic and foreign service providers, online content hosts, and agencies (as appropriate) to achieve the purpose of this Act:
> (e) to provide education and advice on policies for online safety and conduct on the Internet:
> (f) to perform the other functions conferred on it by or under this Act, including functions prescribed by Order in Council made under section 7.

42 Section 7(1).
43 Law Commission, above n 7, at [65], n 17.
44 Section 7(1)(a).
45 Section 8(1).

The Approved Agency may refuse to investigate a complaint in the following circumstances: if it considers it to be trivial, frivolous, or vexatious; if its subject matter is unlikely to cause harm; or if its subject matter does not contravene a communication principle.[46]

Once the Approved Agency has received a complaint and has had a reasonable opportunity to consider and decide what action (if any) to take, then the complainant, a parent or guardian, or a professional leader of a registered school (or his or her delegate) may apply to the District Court for an order under ss 18 or 19.[47] The court may only make such an order if it is satisfied that there has been a serious, repeated or threatened breach of one or more communication principles and that the breach is likely to cause harm to an individual.[48] Like the Approved Agency, the court may dismiss frivolous or vexatious applications.[49] The police,[50] and the chief coroner,[51] may apply directly to the District Court and do not need to use the Approved Agency or satisfy the requirements for harm or breach of a communication principle.[52] The court may dismiss an application from the police but not from the chief coroner.[53]

Section 19 sets out a wide variety of orders that the court may make against a defendant, online content host or another person.[54] Under subs (1), the court may order a defendant to take down or disable material, cease the conduct concerned, not encourage other persons to engage in similar communication towards the victim, publish a correction, give a right of reply to the victim or publish an apology. Further, under subs (2), the court may order an online content host to:

(a) Take down or disable public access to material that has been posted or sent;
(b) Release the identity of the author of an anonymous or pseudonymous communication to the court;
(c) Publish a correction; or
(d) Give a right of reply to the affected individual.

The court may also: make any of the above orders in respect of any other persons;[55] order an Internet protocol address provider (IPAP) to release the identity of an anonymous communicator to the court;[56] make a declaration

46 Section 8(3).
47 Sections 11(1) and 12(1). Section 18 provides that the court may grant any interim orders pending the determination of an application for orders under s 19.
48 Section 12(2). "Harm" is defined in s 4 as "serious emotional distress".
49 Section 12(3).
50 If the digital communication constitutes a threat to an individual's safety: s 11(1)(d).
51 If the communication contravenes a provision of the Coroners Act 2006: s 11(2).
52 Section 12 only sets these requirements for the complainant, a parent or guardian, or a school leader.
53 Section 12(4).
54 An "online content host" is defined in s 4 as "the person who has control over the part of the electronic retrieval system, such as a website or an online application, on which the communication is posted and accessible by the user".
55 Section 19(4)(a).
56 Section 19(3). Internet protocol address provider (IPAP) is defined in the Copyright Act 1994, s 122A.

that a communication breaches a communication principle;[57] and give name suppression.[58] The court may appoint a technical adviser to assist its determination of an application,[59] and must do so in some circumstances.[60]

In deciding what order (if any) to make, the court must take into account the following factors:[61]

(a) the content of the communication and the level of harm caused or likely to be caused by it:
(b) the purpose of the communicator, in particular whether the communication was intended to cause harm:
(c) the occasion, context, and subject matter of the communication:
(d) the extent to which the communication has spread beyond the original parties to the communication:
(e) the age and vulnerability of the affected individual:
(f) the truth or falsity of the statement:
(g) whether the communication is in the public interest:
(h) the conduct of the defendant, including any attempt by the defendant to minimise the harm caused:
(i) the conduct of the affected individual or complainant:
(j) the technical and operational practicalities, and the costs, of an order:
(k) the appropriate individual or other person who should be subject to the order.

Non-compliance with an order under ss 18 or 19, without reasonable excuse, is an offence punishable by imprisonment for a term not exceeding six months or a fine not exceeding $5,000.[62]

2 The Criminal Offence

This article's focus is the civil law elements of the Act. However, the new criminal offence is a significant — and arguably overreaching — component and therefore deserves attention too.

Section 22 introduces the offence of causing harm by posting a digital communication, which carries the penalty of imprisonment for up to two years or a fine of up to $50,000. The offence is committed by posting a digital communication with the intention to cause harm where posting would cause harm to an "ordinary reasonable person in the position of the victim" and posting does indeed cause harm to the victim.[63] In determining whether a post would cause harm, the court may consider any relevant factors,

57 Section 19(4)(b).
58 Section 19(4)(c).
59 Section 17(1).
60 When considering whether or not to make an order against a person other than the defendant, an order against an IPAP or an order for an online content host to take down or disable material or release the identity of its author: s 17(3).
61 Section 19(5).
62 Section 21. For a body corporate, non-compliance is punishable by a fine not exceeding $20,000.
63 Section 22(1).

including a list that is similar, but not identical, to those of the civil enforcement regime.[64]

III DEFICIENCIES OF THE HARMFUL DIGITAL COMMUNICATIONS ACT

Legislators intended to produce a statute that would provide quick and efficient redress against harm.[65] This denotes a clear focus on access to justice. However, the problems identified in this part mean that these objectives are unlikely to be achieved; that is, the Act is insufficient to combat harmful digital communication.

The Complaints Process on Paper

The Act's civil enforcement regime is confusing and omits important information. To begin with, the Act does not provide a mechanism for commencing a complaint. It is clear from supporting material that the Approved Agency was intended as the front line for complaints.[66] Despite specifying that an applicant may only apply for a court order after the Approved Agency has considered his or her complaint,[67] at no point does the Act specify how an applicant may make this complaint. This procedure may be added later in regulations,[68] but it is unusual to omit the first step of a process in an Act that is otherwise very detailed.[69]

The Approved Agency's statutory powers of referral to the District Court are also poorly conceived. As the Act currently stands, application to the court is primarily left to the individual,[70] which will be a significant barrier for many complainants.

The judges of the District Court proposed a better system.[71] They submitted that all applications under the civil enforcement regime should be sent to the Approved Agency, which could then refer them (as appropriate) to the District Court.[72] This would give full effect to the Agency's purpose as a filter for the District Court, preventing meritless claims from reaching

64 Google was critical of these two lists being different: Google "Google NZ Supplementary Submission on the Harmful Digital Communications Bill" at 36–37. Their concern was noted but not addressed in the advice from the Ministry of Justice in its report *Harmful Digital Communications Bill: Departmental Report for the Justice and Electoral Committee* (April 2014) at [234.1].

65 Harmful Digital Communications Act, s 3(b).

66 See Office of the Minister of Justice *Harmful Digital Communications* (21 March 2013) at [38].

67 Section 12(1).

68 Under ss 7(1)(b) and 26.

69 Such as in the various orders available and factors for consideration in s 19.

70 The police, a guardian, a professional leader of a registered school or his or her delegate, or the chief coroner may also apply, at their discretion: s 11(1).

71 Jan-Marie Doogue "Before the Justice and Select Committee in the Matter of the Harmful Digital Communications Bill: Submission on Behalf of the Judges of the District Courts" at [53]–[58].

72 At [56].

the court.[73] It would also remove the applicant's burden of taking a claim to the District Court himself or herself. The Approved Agency should also be able to directly refer a complaint to the District Court without considering it.[74] This is the same power that the police currently have under the Act; their complaints are fast-tracked to the District Court without the need for consideration by the Agency. In many cases, a victim may approach the Approved Agency before, or instead of, the police. It does not make sense for complaints with similar subject matter to be subject to different procedures depending on where the complaint commenced.

Given the absence of direct referral, one would expect the Act to ensure that complainants are made aware of their right to obtain an order from the District Court. Indeed, the Ministry of Justice seems to have expected that the Approved Agency would give clear directions to the complainant — the Ministry envisioned that regulations could include functions:[75]

> 40.7. To advise the complainant to seek an order from the court requiring a website host, ISP or internet intermediary to identify the author of an offensive communication.
>
> 40.8. To advise the complainant to refer appropriate matters to the court.
>
> 40.9. To certify that it has recommended a referral of such a complaint to the court.

The Justice and Electoral Committee amended the original Harmful Digital Communications Bill 2013 to require the Approved Agency, upon refusal to take further action, to notify the complainant of the right to apply for an order from the District Court.[76] This gives the impression that, in all other cases, the agency need not notify the complainant of this right.[77] Although regulations may be added, it is inapt to include some of the information provisions in primary legislation and others in secondary legislation. These are important functions that would be better placed in primary legislation where they will attract greater Parliamentary scrutiny.

---

73 According to the submission, the Approved Agency should only refer to the court if it has used its best efforts to resolve the matter and further attempts would not be constructive or be in the public interest: at [56].

74 At [57].

75 Office of the Minister of Justice, above n 66, at [40.7]–[40.9].

76 Harmful Digital Communications Bill 2013 (168-2), cl 8(4). The Human Rights Commission's recommendation triggered this amendment. It recommended that the Approved Agency's functions be similar to the Human Rights Commission's in respect of the requirement, upon a decision to take no further action in relation to a human rights complaint, to notify a complainant of his or her right to take further action: see Human Rights Commission "Harmful Digital Communications Bill" at [3.6].

77 For example, where the Approved Agency investigates the incident and takes action but the applicant is not satisfied with the result.

The Approved Agency was intended to act as a filter for the District Court.[78] However, gaps in its information responsibilities mean that legitimate complaints may fall through the gaps. Furthermore, because application to the courts is left in the hands of the complainant, illegitimate complaints can still reach the District Court. Therefore, the Approved Agency is not really operating as a filter at all.

The mishmash of instructions provided by the Act can be contrasted with a similar, but more comprehensive, consumer complaints system: the Health and Disability Commissioner Act 1994. The Health and Disability Commissioner Act clearly sets out the mechanism by which a person may complain to the Commissioner and the way in which that complaint is processed.[79] Section 31, in pt 4 of the Act, establishes a general right to complain and identifies to whom complaints should be made. The rest of the part methodically details the complaint process. This includes the detailed process, and factors to be considered, for: the Commissioner's preliminary assessment;[80] direct referral to a number of agencies;[81] a decision to take no action;[82] and an official investigation of a complaint by the Commissioner.[83] The Health and Disability Commissioner Act enables a reader to sequentially follow the steps of its complaints system.[84] Conversely, a reader who wants to understand the complaints system of the Act will find himself or herself jumping backwards and forwards between the sections in no particular order.[85]

The purpose and overarching objectives of the Health and Disability Commissioner Act are strikingly similar to those of the Act:[86]

> The purpose of this Act is to promote and protect the rights of health consumers and disability services consumers, and, to that end, to facilitate the fair, simple, speedy, and efficient resolution of complaints relating to infringements of those rights.

It is strange, therefore, that these two complaints systems, with similar aims for protection and awareness, are so divergent in their approaches. If

78 See Law Commission, above n 7, at [5.44] for the description of the Approved Agency as a "filter"; and see Office of the Minister of Justice, above n 66, at [43] for the intention that only complaints that cannot be resolved by the Agency should be able to reach the court.

79 See Health and Disability Commissioner Act 1994, pt 4. Part 4 is bolstered by Right 10 of the Code of Health and Disability Services Consumers' Rights 1996. These rights were created by the Health and Disability Commissioner to establish the rights of consumers and duties of providers in the health sector: Health and Disability Commissioner Act, s 20(1).

80 Section 33.

81 Sections 34–37.

82 Section 38.

83 Sections 40–49.

84 In fact, it is unnecessary to understand the system, as once a complaint is dispatched, everything is taken care of for the consumer. Comparatively, under the Act, the complainant is responsible for bringing a claim to the District Court.

85 For example, a complainant may establish his or her eligibility to bring proceedings in the District Court from s 11 and then move on to s 12: the threshold for proceedings. Next, the complainant may realise that he or she cannot actually bring proceedings until the Approved Agency has investigated the complaint. Thus, he or she must refer to ss 7 (Approved Agency) and 8 (Functions and powers of Approved Agency) to work out how to complain to the Agency. This is problematic, however, because the Act does not specify how to instigate the complaint.

86 Health and Disability Commissioner Act, s 6.

legislators had been given more time to consider and draft a complaints system for harmful digital communications, perhaps the Act would have borne greater resemblance to the Health and Disability Commissioner Act.

The Complaints Process in Reality

1 The Capacity of the District Court

In their submission, the District Court Judges noted that at least initially — when there are no precedents — a large number of complaints would require an oral hearing.[87] This would involve expert evidence, a technical adviser and, potentially, representatives from service providers.[88] An estimated 0.5 full-time-equivalent judges are required just to deal with the referrals needing a full oral judgment.[89] Although hearings on the papers are likely to increase after the relevant jurisprudence is established, the judges believe that the extra workload will still be a considerable burden.[90]

The Ministry of Justice noted the judges' concerns, stating that although judicial resourcing was beyond the scope of their considerations, it would be "taken into account as part of the full implementation of the Bill".[91] Arguably, it would have been far more valuable for the Ministry to modify procedures so as to avoid increasing the workload of judges. At the very least, the Ministry ought to have given greater consideration to implementing more significant amendments that might relieve the courts of their burden.

The key culprits behind the increase in the courts' workload are the poorly drafted complaints process and the decision to allow independent complaints before the court. Another culprit is the courts' limited power to refer or dismiss complaints. The court may dismiss an application from an individual and his or her parents, guardians and teachers,[92] or refer the matter back to the Approved Agency.[93] The Justice and Electoral Committee also added that the court can dismiss an application from the police "if satisfied that, having regard to all the circumstances of the case, the application should be dismissed".[94] However, a similar provision was not added for applications from the chief coroner.[95] The court also has no express power to refer a complaint from the police to the Approved Agency where they consider that the agency would be the best body to deal with it. Another factor increasing the courts' workload is the Select Committee's

87 Doogue, above n 71, at [71].
88 At [71].
89 At [74]. This is not taking into account the judicial resources needed to deal with referrals on the papers: at [75].
90 At [76].
91 Ministry of Justice, above n 64, at [45].
92 Harmful Digital Communications Act, s 12(3).
93 Section 13. However, this still takes up court time, as courts would need to consider the complaint to determine whether or not to take this action. Those complaints that the court refers back to the Approved Agency should arguably not have reached the court in the first place.
94 Harmful Digital Communications Bill, cl 11(4).
95 Section 19 seems to imply that the court can choose not to make an order no matter who the complainant was. The Act should be clearer about this; it currently singles out some parties but not others.

amendment to include a *threatened* breach of one of the Act's communication principles, which widens the pool of potential complainants.[96]

The Ministry of Justice could have substantially decreased the workload of the District Court under the Act. A simple method would have been to remove the right to apply directly to the court, instead requiring cases to be referred by the Approved Agency. A more significant change would have been to remove the entire court component from the Act and only use the Approved Agency and existing legal avenues — such as harassment or defamation — to combat harmful digital communications. A case could also be made for a Communications Tribunal, as the Law Commission recommended.[97] Indeed, it is conceivable that cases under the Act would be assigned to specific judges who would operate as a de facto tribunal.[98]

2 *Ineffective and Infeasible Remedies*

Even if the District Court does find time to investigate complaints, the remedies it grants may be ineffective or infeasible. This may be particularly true of the remedies available against online content hosts.[99]

Section 19(2)(a) could be read as requiring the online content host to find and take down all future re-postings of the communication.[100] This is an entirely unworkable obligation. Although it is hoped that the court would clarify that this is not the case, the alternative would create issues for the complainant who would bear the burden of tracking down re-posted material. He or she would then have to initiate new complaints to remove them. Therefore, there would be either an entirely infeasible burden on the content host, or an entirely ineffective remedy for the complainant. Even if it were possible for a content host to ensure the offending material was not re-posted, a new complaint would be required if that content was reposted with a new content provider. Given the abundance of social media websites — and the tendency of individuals to frequent more than one — this situation will likely be common. The potential for multiple complaints regarding the same material is a strong incentive to remove the availability of this remedy. Take-down orders should be reserved for the author of the material.

---

96 Section 12(2)(a). This is another hasty addition that has not been thought through. It does not fit with wording used elsewhere in the Act and may make it redundant. For example, s 11 states that only an individual and other representatives who have suffered harm as a result of digital communication may apply to the District Court. Therefore, someone who anticipates being harmed by a threatened digital communication technically cannot apply. Likewise, s 8 only gives the Approved Agency the power to investigate harm caused (and not harm anticipated to be caused) to individuals by digital communications. Additionally, the orders that can be made by the court in s 19 do not include an order against doing something that has not yet been done.

97 Law Commission, above n 7, at [5.39].

98 The Law Commission envisioned that the Communications Tribunal could be entirely comprised of District Court judges: Law Commission, above n 7, at [5.133].

99 Google, in its submission to the Justice and Electoral Committee, commented that the Bill did not reflect the Government's intention for orders against an online content host to only be used as a "*last resort and when the author of the communication cannot be identified*": Google, above n 64, at 32 (emphasis in original).

100 At 33.

An online content host is also unlikely to be able to comply with an order under s 19(2)(b) to reveal the identity of the author of an anonymous or pseudonymous communication.[101] Some online content hosts, such as the administrators of websites where communication may be made anonymously, would only be able to reveal the Internet Protocol address from which harmful material was posted.[102] An Internet Service Provider can then match this address number with a subscriber to its services. But where the subscriber shares his or her Internet connection with one or more people (as is often the case), it will be difficult to pinpoint the exact offender.[103] The courts will, therefore, be issuing impossible orders and will be left to decide how to find a defendant for the purposes of s 19(1). Perhaps the courts will need to impose a strict liability system whereby the subscriber or joint household will be responsible for ensuring compliance with the court's order.[104] It would be unsatisfactory for the courts to make such a significant ruling without any statutory backing.

Finally, an order for an online content host to publish a correction, or to give a right of reply, is likely to be infeasible for many content hosts.[105] It would be both unusual and disproportionate for a host such as Facebook, for example, to be tasked with publishing a correction or responding to something that only a small proportion of its users would have seen. Ironically, such an action may even amplify the damage, particularly if the harmful content has been re-posted elsewhere on the Internet. A less restrictive alternative could be to publish a declaration against the content on a government-hosted website.[106]

IV UNINTENDED CONSEQUENCES OF THE HARMFUL DIGITAL COMMUNICATIONS ACT

The Act is too far-reaching and inadequately protects the rights and freedoms of both individuals and online content hosts. This part draws together issues that contribute to this unintended consequence.

The District Court can only grant an application where there is a "threatened serious breach, a serious breach, or a repeated breach" of a communication principle that causes, or is likely to cause, serious emotional distress.[107] Even then, the court does not have to award a remedy to an undeserving complainant. The court may dismiss frivolous or vexatious

101 At 33.

102 An Internet Protocol address is a unique identifier for a machine connected to a network (such as the Internet). For domestic Internet use, these identifiers are usually assigned by the Dynamic Host Configuration Protocol to a household's router. This router may be shared by a number of computers. Furthermore, the address is dynamic, meaning that it can change automatically: Stephanie Crawford "What is an IP address?" <computer.howstuffworks.com>.

103 Under s 19(3), Internet Service Providers may also be ordered to reveal an anonymous communicator.

104 For an example of such a system, see the Copyright Act, ss 122A–122U.

105 See the Harmful Digital Communications Act, s 19(2)(c)–(d). See also Google, above n 64, at 34.

106 Google, above n 64, at 35.

107 Harmful Digital Communications Act, s 12(2)(a) and (b).

applications,[108] refer matters back to the Approved Agency,[109] or decide not to make an order after considering all of the factors in s 19(5).[110] Therefore, the issue is not with undeserving individuals obtaining remedies. Instead, the overarching concern is clogging up the District Court. This would be inconsistent with the Act's objectives of providing quick and efficient redress.[111]

Two types of cases will be responsible for wasting court time:

(a) Cases that technically meet the threshold for complaints but are unlikely to have been intended to attract coverage by the Act; and
(b) Cases that do not meet the threshold but may still be brought before the courts due to individuals thinking they have an arguable case.

In either event, the wording of s 16 suggests that the court will have to consider the application and publish a decision, with supporting reasons. This is a significant amount of work to resolve complaints that the Act could have filtered out itself.

Examples from both of these types of cases will be addressed in order to illustrate the overreach of the Act. The potential for the Act to displace existing legal principles will also be explored as an unintended consequence.

Displacement of Existing Legal Principles

The New Zealand Productivity Commission criticised official advice on the Harmful Digital Communications Bill for not considering the risks arising from "overlapping, cumulative regulation" and for ignoring opportunities for synergy.[112] A key foundation for these criticisms is likely the overlap between the civil enforcement regime and existing law. Even if the regime were effectively identical to existing law, having different agencies consider identical issues could cause financial inefficiencies and result in conflicting decisions.[113] For example, the Privacy Commissioner and the District Court would both oversee privacy issues. But the Act is not identical to current law. This creates the potential for it to completely displace existing legal principles.[114]

The lack of defences in the Act is a key cause of this danger. The Act does not include any of the defences available under the current,

108 Section 12(3).
109 Section 13.
110 Under s 19, the court "may" make an order.
111 See s 3(b).
112 New Zealand Productivity Commission *Boosting Productivity in the Services Sector* (May 2014) at 194. The Commission does not give any evidential support for these assertions or suggest where "synergies" may be obtained.
113 Google, above n 64, at 24.
114 This is despite the Law Commission stating that the purpose of the communication principles would be "to clearly encapsulate the relevant law": Law Commission, above n 7, at [4.58].

equivalent laws, including truth,[115] satire, political opinion,[116] public interest, consent, honest opinion and lawful purpose. Under this regime, in situations like *King v Taylor*, where a defendant is providing valuable consumer information about a fraudulent salesman (a lawful purpose), he or she will only be able to rely upon the contextual factors from s 19(4) coming out in his or her favour.[117] As the court is not expressly required to consider traditional defences, this provides little comfort.[118] Indeed, claimants seem likely to choose the Act over other actions if they are worried that these may fail due to a defence.

Differences between the Act and existing law in respect of their definitions and tests are also likely to result in the displacement of the latter. In many cases, this may simply be due to the fact that the Act provides remedies for serious emotional distress where the equivalent legal principle does not. A more specific example is the potential for two definitions of "harassment". The Act's harassment principle (principle 5) does not cross-reference the Harassment Act 1997, which means that there is no reason for the District Court to take that Act into consideration when making the order.[119] Instead, courts may opt to take the plain and ordinary meaning of the word, which could impose a lower standard of conduct than the Harassment Act. For example, the New Zealand Oxford Dictionary defines "harass" as to "trouble and annoy continually or repeatedly".[120] This sets a much lower threshold, as a complainant does not have to prove that his or her purported harasser has engaged in a specified act. Instead, the complainant could allege that posts on a message board were simply "annoying", even if the author had not drawn his or her attention to them.[121]

A Right to Be Forgotten

The Act could also be responsible for introducing a controversial "right to be forgotten" to New Zealand. The European Court of Justice recently bolstered this right in *Google Spain SL v Agencia Española de Protección de Datos*

115 Doogue, above n 71, at [45].

116 The New Zealand Police Association, above n 28, at 3, submitted that opinion in a political or satirical context should not be covered by the Act. The Ministry of Justice disagreed: Ministry of Justice, above n 64, at [264]–[265].

117 *King v Taylor* DC Auckland CIV-2014-004-122, 24 April 2004.

118 There are examples of courts refusing to refer to the similar law when considering new legislation. See *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (Admin), [2013] 1 WLR 1833 at [29], where the High Court of England and Wales declined to consider other threat offences in determining the meaning of sending a message of "menacing character" for the purposes of s 127 of the Communications Act 2003 (UK).

119 Section 5(1) of the Interpretation Act 1999 provides that the meaning of a provision is to be ascertained "from its text and in the light of its purpose", which makes it difficult to import another Act's definition where no express mention of it is made. The District Court judges recommended that express reference to the Harassment Act 1997 should be made: Doogue, above n 71, at [33]–[34]. The Ministry of Justice rejected this recommendation because they believed it would undermine the Act's objective for the principles to be simple and accessible to the layperson. However, they acknowledged that they could "see value in clarifying the effect of this principle" and would explore ways to simplify the wording with Parliamentary Counsel: Ministry of Justice, above n 64, at [110].

120 Tony Deverson and Graeme Kennedy (eds) *The New Zealand Oxford Dictionary* (Oxford University Press, Oxford, 2005) at 490.

121 This is a requirement for statutory harassment: Harassment Act, s 4(1)(e) and (ea)

(AEPD).[122] In that case, the Court held that European law should be interpreted to require a search engine operator to, upon request, erase data that is "inadequate, irrelevant or no longer relevant" from its search results.[123] This right to privacy could only be outweighed by the "preponderant interest of the general public", which sets a very high threshold.[124] The decision has imposed a considerable burden on search engines. For example, on the first day that Google launched its "right to be forgotten" service, it received over 12,000 requests from European citizens for content to be removed.[125] The backlash against the *Google Spain* ruling was overwhelming.[126] One commentator observed that:[127]

> It is a decision that, while carrying out a balancing exercise between competing rights, leans firmly (almost to the point of falling over) on the side of the right of privacy of the individual.

Jimmy Wales, the founder of Wikipedia, described the decision as "wide-sweeping internet censorship".[128] Representatives of the Prime Minister of the United Kingdom, David Cameron, also expressed concern over the fact that the ruling does not distinguish between inaccurate material and factually correct material.[129] A court in the Netherlands has attempted to take some of the sting out of the *Google Spain* judgment, holding that the European Court of Justice only intended to provide protection "against being pursued for a long time by irrelevant, excessive or unnecessarily defamatory expressions".[130]

Search engines would easily fit within the broad definition of "online content host" contained in s 4 of the Act. Under the Act, where a person wants "inadequate, irrelevant or no longer relevant" information to be removed, he or she could form a case based on principle 1 (disclosing sensitive facts). The applicant would have to prove that he or she had suffered serious emotional distress, which may be difficult to prove for pure reputational damage.[131] However, the test is subjective and there are conceivable situations in which reputational damage could be found to cause

---

122 Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos (AEPD)* [2014] QB 1022.

123 At [94].

124 At [99].

125 Rose Powell "Google receives 12,000 requests to be 'forgotten' on first day" *The Sydney Morning Herald* (online ed, Sydney, 1 June 2014). Google expressed disappointment at the ruling and issued a statement bemoaning the consequence that it must "make difficult judgments about an individual's right to be forgotten and the public's right to know".

126 See David Harvey "Back to the Future — Google Spain and the Restoration of Partial and Practical Obscurity" (22 May 2014) The IT Countrey Justice <theitcountreyjustice.wordpress.com> for a more detailed exploration of the adverse consequences of the decision.

127 Steven James "The right to privacy catches up with search engines: the unforgettable decision in *Google Spain v AEPD*" (2014) 20 CTLR 130 at 132.

128 "UK reacts to Google 'right to be forgotten' ruling" *BBC News* (online ed, United Kingdom, 21 May 2014).

129 James, above n 127, at 132.

130 Joran Spauwen and Jens van den Brink "Dutch Google Spain ruling: More Freedom of Speech, Less Right To Be Forgotten For Criminals" (26 September 2014) Media Report <www.mediareport.nl>.

131 This will depend on how broadly the term is interpreted by the courts. It may be found that "serious emotional distress" is not much different to "distress" in the Harassment Act, in which case reputational damage at the level in *Flannagan v Sperling* [2013] DCR 567 could be sufficient.

serious emotional distress; in particular, where the communication is seriously damaging to the applicant's reputation.[132]

Indirect and Unexpected Harm

Two scenarios will be used to relay my concerns about the Act's application to indirect or unexpected harm.

The first scenario, involving indirect harm, is where a digital communication is intended for recipients who will not suffer harm. Person A is not an intended recipient but accesses the communication and suffers harm as a result. Children who access online pornography, for example, fit into this category. They have accessed a communication, which is a serious or repeated breach of principle 4 ("[a] digital communication should not be indecent or obscene") and it should be easy to prove that serious emotional distress has resulted.[133] Although the Act gives little attention to the fact that the website was intended for adults, the court will likely take this matter into account under s 19(5) in deciding whether or not to make an order. But by then the damage is done. The court has already had its time wasted by having to entertain a vigilante parent's attempt to censor the Internet.[134] Scenarios like this are particularly unfair for a defendant due to the apparent anonymity of the Internet. A person cannot possibly know the identity or disposition of all individuals accessing his or her digital communication.

The second scenario, involving unexpected harm, occurs where a digital communication is intended for person B, who is not expected to suffer harm but does. An extreme example of this scenario, admittedly outside the digital context, is the suicide of Jacintha Saldanha following a prank call from an Australian radio station.[135] Although the actions of the radio deejays could be considered stupid or even deplorable, it is not the law's place to punish serious but unforeseeable harm resulting from freedom of expression. However, the Act can apply to this type of harm. The civil enforcement regime's threshold for proceedings merely requires harm or likely harm to an individual, without consideration of whether a reasonable person would also suffer harm.[136]

Unknowingly False Allegations

Unknowingly false allegations may also be subject to the Act because principle 6 merely states: "A digital communication should not make a false allegation."[137] The intention or knowledge of the defendant is irrelevant in

132 See, for example, *King*, above n 117, at [31]. King's distress was related to reputational harm. His claim failed, however, due to the fact that a restraining order was not justified — a requirement under the Harassment Act, s 16(1)(iii).

133 The threshold for proceedings in s 12(2) is therefore met.

134 The court may also dismiss the application under s 12(3) for being frivolous or vexatious but even having to do this is a waste of time.

135 Dominic Gover "Kate Middleton Prank Death Call: No Charges over Jacintha Saldanha" *International Business Times* (online ed, London, 28 December 2012).

136 Harmful Digital Communications Act, s 12(2).

137 Section 6(1).

determining whether or not the court can grant an application.[138] Provided that the "serious emotional distress" threshold is passed, a number of communications could needlessly concern the courts. For example, the Act could apply to a person who breaks up with his or her partner via digital communication, with the reason for ending the relationship being a mistaken belief that the partner was cheating.[139] The Act could also apply to someone posting condolences on a Facebook page, mistakenly thinking that someone had died. The District Court Judges suggested that a better version of principle 6 would be: "A digital communication should not *knowingly* and *deliberately* make a false allegation."[140] The Ministry of Justice merely countered that "issues such as intent will be considered later on in the civil process".[141] However, this does not resolve the fact that the courts' time is wasted with cases that should never have reached them in the first place.

Ridiculously False Allegations

Principle 6 also fails to adequately acknowledge false allegations that no reasonable person would believe. Such allegations are unlikely to be considered "serious" for the purposes of s 12(2)(a) but if they are repeated or threatened they will be covered by the Act. Therefore, if I sent out more than one tweet asserting that someone is an apple tree and for some reason that person suffers harm,[142] I could find myself subject to the civil enforcement regime.[143] The same could result if I merely threatened to tweet this message.[144]

Political Satire

Satire is currently governed by defamation law, which, for a long time, has been a mixed bag in terms of success for the plaintiff.[145] Courts have held that a person cannot be too thin-skinned and will generally not grant an order where a reasonable person would laugh off the incident.[146] In addition, satire can often be considered an expression of honest opinion, which provides

138 Section 12(2).

139 Google, above n 64, at 20, gave the example of a break-up via text message due to personal health reasons.

140 Doogue, above n 71, at [38] (emphasis in original). See also Tech Liberty "Submission: Harmful Digital Communications Bill" at 8, which proposed similar wording of a "knowingly false allegation".

141 Ministry of Justice, above n 64, at [112].

142 A "tweet" is a message posted on Twitter, a social media website.

143 Perhaps that person had some traumatic childhood experience involving apple trees which caused him or her nervous shock upon the metaphor being drawn.

144 The "threatened breach" option was likely added in order to allow the court to put in place preventative measures: see Steven Price "Submission on Harmful Digital Communications Bill" at 3. However, in many instances complaints could come before the courts for conduct that was never going to occur in the first place.

145 Ursula Cheer and John Burrows "Defamation" in Steven Todd (ed) *The Law of Torts in New Zealand* (6th ed, Brookers, Wellington, 2013) 809 at 818–819. Note that, in many cases, satire could also be considered to involve ridiculously false allegations, as described in the previous part.

146 At 818.

further protection.[147] Conversely, courts have found satire to cross the line in a number of cases.[148]

The Act is likely to make it more accessible for easily offended people to attack satirical content about them. For example, in 2013, Colin Craig, the leader of the Conservative Party, threatened to sue The Civilian, a satirical website, for defamation over a fictitious quotation that the website had attributed to him.[149] Steven Price, a well-known media lawyer, was reported as saying that Colin Craig did not have a strong case.[150] However, under the Act, Craig may be more likely to succeed in obtaining a remedy. The satire would fall under principle 6, as it essentially made a false allegation by falsely attributing the quotation. Craig would have to prove he had suffered "serious emotional distress". This may be difficult but could be supported with evidence that he cared deeply about his political credibility.[151] Because the Act does not focus on whether or not people will take the communication seriously, this is a far easier process than defamation. It is hoped that courts will view their obligation to act consistently with the New Zealand Bill of Rights Act 1990 as a ground for not making an order against political satire.[152] However, it would be more reassuring and efficient for the Act to provide its own safeguard.[153]

Robust Debate and Internet Trolls

Offensive retorts or false allegations make up a significant portion of online communication. Where this content emanates from an individual intending to cause disruption or to trigger or exacerbate conflict for his or her own amusement, the behaviour is termed "trolling".[154] However, individuals who are genuinely involved in robust debate can also cause disruption and conflict. Both of these behaviours may attract undesirable attention from the Act.

Trolling occurs on a spectrum. At one end, trolls can be described as mildly irritating or even funny.[155] At the other end, trolling can be seriously

147 Defamation Act 1992, s 9. Another protection, which will also operate in respect of the Harmful Digital Communications Act (see ss 6(2)(b) and 19(6) — the latter of which is redundant in light of the former), is the court's obligation to take into account the provisions of the New Zealand Bill of Rights Act 1990 and thus the right to freedom of expression contained in s 14.

148 Cheer and Burrows, above n 145, at 819.

149 Claire Trevett "Colin Craig warns on satirical quote" *The New Zealand Herald* (online ed, New Zealand, 24 April 2013). See also "Maurice Williamson looking pretty stupid after floods" (22 April 2013) The Civilian <www.thecivilian.co.nz>.

150 Sophie Speer "Conservative Party withdraws legal action over satire" *The Dominion Post* (online ed, Wellington, 24 April 2013).

151 Google, above n 64, at 22.

152 In addition to the contextual factors in s 19(5). See, for example, s 14 of the New Zealand Bill of Rights Act, which protects freedom of expression.

153 Perhaps by including defamation defences.

154 Claire Hardaker "Trolling in asynchronous computer-mediated communication: From user discussions to academic definitions" (2010) 6 Journal of Politeness Research 215 at 237.

155 Indeed, the first examples of trolling were for humour rather than provocation: Sarosh Khan "Can the trolls be put back under the bridge?" (2013) 19 CTLR 9 at 9–10.

offensive and legitimately distressing.[156] Legislation to deal with the latter is arguably warranted, although some believe that self-regulation is the best answer.[157] But the Act goes further than this. Any troll that repeatedly posts mildly offensive or false content could be subject to the regime if a single, sensitive individual suffers harm. While reasonable people would ignore or report trolls, some may unwisely choose to engage and as a result contribute to their own distress.[158]

Similarly, the Act overreaches when it comes to robust debate online, which may resemble trolling but is fuelled by a genuine intention to prove a point or discredit a proponent of an alternative viewpoint.[159] For this reason, robust debaters could be said to deserve even more protection than trolls. As such, it is hoped that a judge would be less likely to make an order for offence caused to prove a point (debate) rather than for amusement (trolling).[160] Nonetheless, the damage is already done. As one writer observes: "Two decades ago, ill-judged remarks made in the heat of the moment or poor taste jokes among friends were unlikely to be on the radar of law enforcers."[161] Now, the Act may be brandished as a weapon by the easily offended.

Self-Disclosure and the Ability to Revoke Consent

Principle 1 (disclosing sensitive personal facts) can apply where a person discloses sensitive facts about himself or herself. This means that, where a teenager posts his or her own sensitive personal facts online, the teenager's parents could apply for an order if they suffer serious emotional distress as a result. An example of this could be if their teenage daughter was announcing her pregnancy.[162]

The Justice and Electoral Committee initially amended the principle to avoid this situation.[163] However, the Act returns to the original wording.

The principle also does not preclude a situation where the applicant consented to the disclosure. This means that, if someone is willingly interviewed and voluntarily discloses sensitive personal facts but later regrets it, he or she could seek redress under the Act. This is unsatisfactory considering the time, energy and money that interviewers often spend to solicit and conduct an interview.

---

156 Such as when it involves defacing Internet tribute sites: see Tony Keim "Facebook troll Bradley Paul Hampson jailed for posting child porn on tribute pages for dead children" *The Courier Mail* (online ed, Brisbane, 25 March 2011).

157 Khan, above n 155, at 12–13, argues that current legislative changes in the United Kingdom are unlikely to be effective and that a more libertarian approach may be better at combatting internet trolls.

158 In *Brown*, above n 1, at [237]–[240], this meant that the causation element of the harassment claim was not satisfied.

159 This intention is absent in trolling. See Hardaker, above n 154, at 237.

160 This is because the purpose of the communicator is to be considered under s 19(5)(b).

161 Jacob Rowbottom "To Rant, Vent and Converse: Protecting Low Level Digital Speech" (2012) 71 CLJ 355 at 356.

162 Google, above n 64, at 20.

163 The prohibition on disclosing "sensitive personal facts about an individual" was narrowed so as to apply only to "sensitive personal facts about another individual": Harmful Digital Communications Bill, cl 6(1).

Whistleblowing

Under existing law, whistleblowing can be covered by breach of confidence,[164] although it is protected by a defence of public interest.[165] The new regime omits this defence, leaving public interest as a matter to be considered by the District Court in deciding whether or not to make an order.[166] The Protected Disclosures Act 2000 will prevent civil or criminal proceedings under the Act where the whistleblower is an employee disclosing "serious wrongdoing" about his or her organisation. However, no such protection exists in relation to individuals who fall outside this definition. The Protected Disclosures Act shows that, in many cases, whistleblowing is valued in society. The Act should reflect this sentiment by further protecting such individuals.

Hyperlinks

In its submission, Google argued that the definition of "digital communication" should expressly exclude hyperlinks.[167] The Ministry of Justice disagreed, noting:[168]

> If hyperlinks were explicitly excluded from the definition, a person could provide a link from their own blog (blog A) to harmful content on blog B and the provision of that link would not constitute a breach of a communication principle. This would be the case no matter how egregious the content relating to the link on blog A, or the content linked to on blog B.

I do not see how this supports the Ministry of Justice's case. If the content of blog B is harmful, a complaint should be made about blog B. If the content on blog A is egregious, a complaint could also be made about blog A. Courts should be encouraged to resolve the source of the problem, not beat around the bush.

The application of the Act to hyperlinks would be less of a problem if it remained at that. But there is a risk that this sort of reasoning could extend the scope of the Act even further. The essence of a hyperlink is that it refers to content in another location. A non-hyperlinked reference to a website or even a mention of harmful content online would have the same

---

164 Whistleblowing can be defined narrowly to only include disclosure of information obtained in an employment relationship: William De Maria *Deadly Disclosures: Whistle Blowing and the Ethical Meltdown of Australia* (Wakefield Press, Adelaide, 1999) at 27. However, other definitions do not restrict the term to employees. For example, *The New Zealand Oxford Dictionary* definition is "a person who exposes or brings to public attention an irregularity or a crime, esp. from within an organisation": Deverson and Kennedy, above n 120, at 1288.

165 See Stephen Todd "Interference with Intellectual Property" in Stephen Todd (ed) *The Law of Torts in New Zealand* (6th ed, Thomson Reuters, Wellington, 2013) 717 at 760.

166 Harmful Digital Communications Act, s 19(5)(g).

167 Google, above n 64, at 15. Indeed, Tim Berners-Lee, the inventor of the World Wide Web and hypertext (text with hyperlinks) has stated that "[t]he intention in the design of the web was that normal links should simply be references, with no implied meaning": Tim Berners-Lee "Links and Law" (April 1997) World Wide Web Consortium <www.w3.org>.

168 Ministry of Justice, above n 64, at [73].

effect, as the content could easily be located with a search engine. The application of the Act to this sort of communication is a step too far.

Social and Political Campaigns

Campaigns against war, poverty, or other social issues often use very offensive images in order to shock the public into action. Such images could be considered a serious breach of principle 3 (communication that is grossly offensive to a reasonable person in the position of the affected individual) and to cause serious emotional distress to a child or a particularly sensitive person. Even news articles with graphic images could be considered to pass this threshold. Courts could have their work cut out for them if these forms of expression are not explicitly protected.

V CONCLUSION

The fact that Parliament has tried to improve the safety of New Zealanders online is commendable. However, the Act is a "quick fix" that will be only minimally effective. Worse, it creates an unnecessarily onerous environment for free speech on the Internet and an unjustifiable workload for the judiciary. It is clear that people are encountering trouble with harmful communication in the digital world. While some forms of legislation may be able to help the situation, this Act will not. If Parliament wishes to create "a First World regime to complement other efforts already taking place",[169] and that "has the potential to be quite world leading", it needs to rectify the many deficiencies and unintended consequences identified in this article.[170]

169 (14 November 2013) 694 NZPD 14748.
170 (14 November 2013) 694 NZPD 14751.