

# **Harmful Digital Communications Bill**

Government Bill

As reported from the Justice and Electoral  
Committee

## **Commentary**

### **Recommendation**

The Justice and Electoral Committee has examined the Harmful Digital Communications Bill and recommends that it be passed with the amendments shown.

### **Introduction**

The Harmful Digital Communications Bill seeks to mitigate the harm caused to individuals by electronic communications and to provide victims of harmful digital communications with a quick and effective means of redress. We recognise that technology has made possible the rapid, anonymous distribution to a potentially huge audience, and the bill aims to strike a careful balance between preserving freedom of expression and preventing and reducing harm.

The bill would create a new civil enforcement regime and new criminal offences to deal with the most seriously harmful digital communications, and would make small amendments to legislation to clar-

ify its application to digital communications and to cover potential technological advances.

Complaints about harmful digital communications would be submitted to the Approved Agency, a body which would be appointed by the Governor-General by Order in Council as the first step in the civil enforcement regime. The agency would assess complaints, where appropriate investigating and using negotiation, mediation, or persuasion to resolve matters. The agency's primary functions would include education.

The bill sets out ten communication principles to guide the court and the Approved Agency in assessing whether a digital communication has caused or is likely to cause someone harm. "Harm" is defined as "serious emotional distress". We consider that the principles would provide a useful reference to help infer a common set of values when assessing whether behaviour was acceptable.

The bill would also include a safe harbour provision setting out a process for online content hosts to follow to limit their liability for content authored by others.

The bill would implement the Government's decisions on addressing harmful digital communications, which are based on the Law Commission's 2012 ministerial briefing paper *Harmful Digital Communications: The adequacy of the current sanctions and remedies*.

This commentary covers the main amendments we recommend to the bill; it does not cover minor or technical amendments.

## **Purpose**

We recommend amending the purpose of the bill (clause 3) to include the deterrence and prevention of harm. This would reflect the intent of the bill and the Approved Agency's role of providing education and advice for safe online conduct.

## **Internet Protocol Address Provider**

We recommend inserting into clause 4 (Interpretation) a definition of Internet Protocol Address Provider (IPAP) giving the term the same meaning it has in section 122A(1) of the Copyright Act 1993. An IPAP is an entity that provides users with internet access and allocates internet protocol (IP) addresses to users; for example Telecom and

Vodafone are IPAPs in their capacity as network providers. Adding the Copyright Act definition would mean IPAPs would be explicitly included in the bill.

We also recommend inserting subclause 17(2A) to allow the District Court, on application, to make an order against an IPAP to release the identity of an anonymous communicator to the court. This would mean the identity of an otherwise anonymous person's account could be revealed using IP address matching by the IPAP.

### **Professional leader**

We recommend including in clause 4 (interpretation) of the bill a definition of "professional leader" consistent with section 120 of the Education Act 1989. Professional leaders would include principals, and supervising teachers of registered schools. Under subclause 10(1)(c) a professional leader could apply to a District Court for an order mitigating harm, by means including the taking-down or disabling of material, concerning a student at their institution. This would give schools and other educational institutions another tool, in addition to their own policies and procedures, to protect their students from cyberbullying.

### **Approved Agency**

We recommend inserting new subclause 7(5) to make the Approved Agency subject to the Ombudsmen Act 1975, the Official Information Act 1982, and the Public Records Act 2005, in respect of the functions it would perform under the bill.

We recommend inserting new subclause 8(4) to require the Approved Agency if it took no further action on a complaint to notify the complainant of their right to apply to the District Court for an order under this legislation. This would be consistent with the approach taken by the Human Rights Commission under the Human Rights Act 1993.

We recommend inserting new clause 8A allowing the Approved Agency, subject to the Minister's approval, to delegate any of its functions or powers to any person or organisation with the appropriate knowledge, skills, and experience. Subclause 8A(6) would provide for any action or decision of a delegate to be treated as an action or decision of the Approved Agency. Subclause 8A(7) would require a delegate to comply with all reasonable requests or require-

ments of the agency regarding its compliance with the Ombudsmen Act, the Official Information Act, or the Public Records Act. Documents held by a delegate would therefore have to be accessible to the Approved Agency for the purposes of requests made under the Acts listed. It is common practice for statutory bodies to use external agencies to assist them, and the amendments would ensure that the Approved Agency could access the expertise necessary to perform its statutory functions.

### **Threshold for proceedings**

We consider that threats to cause harm should be included as grounds for making an order, reflecting the likelihood of harm occurring if the threat were to be carried out. Therefore, we recommend amending clause 11(2)(a) to reflect this.

### **Varying or discharging an order**

We recommend inserting new clause 17A to allow the District Court, upon application by one or more parties, to vary the duration or any conditions of an order, or discharge an order.

### **Penalty levels**

We recommend adjusting the maximum penalties for the new offences of non-compliance with a court order (clause 18), and causing harm by posting a digital communication (clause 19) to make them consistent with the penalties for similar offences in the Harassment Act 1997. We consider it important that harassment in the physical world and online be dealt with consistently. Therefore, we recommend amending subclause 18(2) to provide for a maximum penalty for an individual of six months' imprisonment or a \$5,000 fine, and \$20,000 for a body corporate; and amending subclause 19(3) to increase the maximum penalty for an individual to two years' imprisonment.

In respect of the clause 19 penalty, we are aware that under section 39(1) of the Sentencing Act 2002, where an enactment only allows a sentence of imprisonment the court may sentence an offender to pay a fine instead. We would like to emphasise that the penalties we

propose are maximum penalties; a Judge would impose a sentence proportionate to the nature of the offending in each case.

### **Safe harbour**

We have considered carefully the submissions on the safe harbour provisions of the bill, and recommend amending clause 20 to provide for a timely “notice-notice-takedown” approach (a regime of notices followed by enforced takedown) suitable for the wide range of online content hosts. In particular, we consider hours to be the best measure of time in an online environment.

We recommend inserting subclause 20(3) to require an online content host who had received a notice of complaint about specific content to notify the author of the content as soon as practicable but no later than 48 hours.

New subclause 20(3)(a)(ii) would allow the author to respond to the online content host within 48 hours with a counter-notice. If the author agreed with the complaint or did not respond, the content would have to be removed or public access to it disabled. If the author responded within 48 hours and did not agree with the complaint, the online content host would have to leave the content in place. New subclause 20(3)(d)(i) would require an online content host to notify the complainant of the action that had been taken as soon as reasonably practicable and bring to their attention other remedies. New provisions would require the complainant and the author to indicate in their notices whether they consented to their identity details being passed to the other person.

While we have struggled to find a perfect solution, we consider this proposal strikes a balance between ensuring the quick removal of harmful or illegal content; ensuring unpopular content which was nevertheless not illegal or harmful was not unilaterally removed; preventing frivolous, groundless or trivial complaints; clarifying the liability and obligations of online content hosts; and providing a practical and affordable procedure for everyone involved.

### **Regulations**

In accordance with advice from the Regulations Review Committee we recommend reversing the order of subclauses 21(1) and (2) so that the standard form of regulation-making power used in legis-

lation since 1962 is followed. New subclause 21(a) would provide for the making of regulations concerning the practice and procedure for the conduct of matters before the Approved Agency, and subclause 21(b) would provide for the making of regulations regarding any other matters. Listing the general power after the more specific would have the effect of reducing the scope of the catch-all provision.

### **Labour Party minority view**

Labour supports the intent of this bill which is to mitigate the harm caused to individuals by electronic communications and to provide victims of harmful digital communications with a quick and effective means of redress.

This bill creates a precedent, not only in New Zealand, but internationally, for establishing criminal offences which only apply to the digital environment. For that reason alone it is important to take time and to consider carefully the impact of a stand-alone law which applies to the online environment.

We support the communication principles to guide the court and the Approved Agency in assessing whether a digital communication has caused or is likely to cause someone harm.

We support the inclusion of a safe harbour provision setting out a process for online content hosts to follow to limit their liability for content authored by others. We believe however that more consultation is required to get this provision right.

We remain concerned at the unnecessarily fast passage of this bill through the select committee; the lack of wider views sought when faced with issues of fundamental importance such as the definition of harm; the impact of the new criminal sanctions on young people; the lack of detail about the role of the Approved Agency and how those functions might be delegated to another authority; and the lack of awareness of and representation by younger people on the impact of a new online cyber-abuse law.

## **Appendix**

### **Committee process**

The Harmful Digital Communications Bill was referred to the committee on 3 December 2013. The closing date for submissions was 21 February 2014. We received 39 submissions from interested groups and individuals, and heard 13 submissions. We received advice from the Ministry of Justice. We also considered a report from the Regulations Review Committee on the regulation-making powers in the bill.

### **Committee membership**

Scott Simpson (Chairperson)

Paul Foster-Bell

Joanne Hayes

Raymond Huo

Andrew Little

Alfred Ngaro

Holly Walker

Hon Kate Wilkinson

Clare Curran was a substitute for this item of business.

David Clendon replaced Holly Walker for this item of business.

---





**Harmful Digital Communications Bill**

---

**Key to symbols used in reprinted bill**

**As reported from a select committee**

text inserted unanimously

text deleted unanimously

---



*Hon Judith Collins*

# **Harmful Digital Communications Bill**

Government Bill

## **Contents**

		Page
1	Title	3
2	Commencement	3
<b>Part 1</b>		
<b>Approved Agency and enforcement</b>		
Subpart 1—Purpose, interpretation, the Crown, and communication principles		
3	Purpose	3
4	Interpretation	4
5	Act binds the Crown	6
<i>Communication principles</i>		
6	Communication principles	6
Subpart 2—Enforcement provisions		
<i>Approved Agency</i>		
7	Approved Agency	7
8	Functions and powers of Approved Agency	8
8A	Power of Approved Agency to delegate	9
9	Protection for employees of Agency	10
<i>Proceedings may be brought in District Court</i>		
10	Who may bring proceedings	11
11	Threshold for proceedings	11
12	District Court may refer matter back to Approved Agency	12

## Harmful Digital Communications Bill

---

<i>Procedure</i>		
13	Applications	12
14	Mode of hearing and evidence	13
15	Technical advisers	13
16	Interim orders	14
17	Orders that may be made by court	14
17A	Court may vary or discharge order	16
<i>Offences</i>		
18	Offence of non-compliance with order	16
19	Causing harm by posting digital communication	16
<i>Liability of online content host</i>		
20	Liability of online content host for content posted by user	19
20A	Further provisions relating to liability of online content host	21
<i>Regulations and rules</i>		
21	Regulations	22
22	Rules	23
22A	Consequential amendments to other Acts	23
<b>Part 2</b>		
<b>Amendments to other Acts concerning use of digital communications</b>		
Subpart 1—Crimes Act 1961		
23	Principal Act	23
24	Section 179 amended (Aiding and abetting suicide)	23
Subpart 2—Harassment Act 1997		
25	Principal Act	23
26	Section 3 amended (Meaning of harassment)	24
27	Section 4 amended (Meaning of specified act)	24
28	Section 19 amended (Standard conditions of restraining orders)	24
Subpart 3—Human Rights Act 1993		
29	Principal Act	24
30	Section 61 amended (Racial disharmony)	25
31	Section 62 amended (Sexual harassment)	25
32	Section 63 amended (Racial harassment)	25
Subpart 4—Privacy Act 1993		
33	Principal Act	25
34	Section 6 amended (Information privacy principles)	25

35	Section 56 amended (Personal information relating to domestic affairs)	25
	<b>Schedule</b>	26
	<b>Consequential amendments to other Acts</b>	

**The Parliament of New Zealand enacts as follows:**

**1 Title**

This Act is the Harmful Digital Communications Act **2013**.

**2 Commencement**

- (1) **Sections 19 and 20 to 20A, and Part 2** come into force on the day after the date on which this Act receives the Royal assent. 5
- (2) The rest of this Act comes into force on the earlier of—
  - (a) a date appointed by the Governor-General by Order in Council; and 10
  - (b) 2 years after the date on which this Act receives the Royal assent.
- (3) One or more Orders in Council may be made under **subsection (2)** appointing different dates for different provisions.

**Part 1** 15

**Approved Agency and enforcement**

Subpart 1—Purpose, interpretation, the Crown, and communication principles

**3 Purpose**

The purpose of this Act is to mitigate harm caused to individuals by digital communications and to provide victims of harmful digital communications with a quick and efficient means of redress. 20

**3 Purpose**

The purpose of this Act is to— 25

- (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.

#### 4 Interpretation 5

In this Act, unless the context otherwise requires,—

**applicant** means anyone who makes an application under **section 10**

**application** means an application to a District Court under **section 13** 10

**Approved Agency** or **Agency** means a person ~~or an organisation,~~ organisation, department, or entity appointed as an Approved Agency under **section 7**

**chief executive** means the chief executive of the department that is for the time being responsible for the administration of this Act 15

**defendant**, in relation to an application made to, or an order made by, a court under this Act, means a person against whom an order is sought or made

**digital communication**— 20

- (a) means any form of electronic communication; and
- (b) includes any text message, writing, photograph, picture, recording, or other matter that is communicated electronically

**harm** means serious emotional distress 25

**individual** means a natural person

**intimate visual recording**—

- (a) means a visual recording (for example, a photograph, videotape, or digital image) that is made in any medium using any device with or without the knowledge or consent of the individual who is the subject of the recording, and that is of— 30

- (i) an individual who is in a place which, in the circumstances, would reasonably be expected to provide privacy, and the individual is— 35

- (A) naked or has his or her genitals, pubic area, buttocks, or female breasts exposed, par-

- tially exposed, or clad solely in undergarments; or
- (B) engaged in an intimate sexual activity; or
- (C) engaged in showering, toileting, or other personal bodily activity that involves dressing or undressing; or 5
- (ii) an individual's naked or undergarment-clad genitals, pubic area, buttocks, or female breasts which is made—
- (A) from beneath or under an individual's clothing; or 10
- (B) through an individual's outer clothing in circumstances where it is unreasonable to do so.
- (b) includes an intimate visual recording that is made and transmitted in real time without retention or storage in— 15
- (i) a physical form; or
- (ii) an electronic form from which the recording is capable of being reproduced with or without the aid of any device or thing 20

IPAP has the same meaning as in section 122A(1) of the Copyright Act 1994

**Minister** means the Minister of the Crown who, under the authority of any warrant or with the authority of the Prime Minister, is for the time being responsible for the administration of this Act 25

**online content host**, in relation to a digital communication, means the person who has control over the part of the electronic retrieval system, such as a website, on which the communication is posted and accessible by the user 30

online content host, in relation to a digital communication, means 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 35

**posts a digital communication—**

(a) means transfers, sends, posts, publishes, disseminates, or otherwise communicates by means of a digital communication—

(i) any information, whether truthful or untruthful, about the victim; or 5

(ii) an intimate visual recording of another individual; and

(b) includes an attempt to do anything referred to in **paragraph (a)** 10

**professional leader** has the same meaning as in section 120 of the Education Act 1989

**registered school** has the same meaning as in section 2(1) of the Education Act 1989.

**5 Act binds the Crown** 15  
This Act binds the Crown.

*Communication principles***6 Communication principles**

(1) The communication principles are—

*Principle 1* 20

A digital communication should not disclose sensitive personal facts about ~~an~~another individual.

*Principle 2*

A digital communication should not be threatening, intimidating, or menacing. 25

*Principle 3*

A digital communication should not be grossly offensive to a reasonable person in the ~~complainant's position~~position of the affected individual.

*Principle 4* 30

A digital communication should not be indecent or obscene.

*Principle 5*

A digital communication should not be ~~part of a pattern of conduct that constitutes harassment~~tused 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.

5

*Principle 8*

A digital communication should not incite or encourage anyone to send a message to a ~~person with the intention of causing harm to that person~~ individual for the purpose of causing harm to the individual.

10

*Principle 9*

A digital communication should not incite or encourage another ~~person~~ individual to commit suicide.

*Principle 10*

A digital communication should not denigrate a ~~person~~ individual by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation, or disability.

15

(2) In performing functions or exercising powers under this Act, the Approved Agency and courts must—

- (a) take account of the communication principles; and
- (b) act consistently with the rights and freedoms contained in the New Zealand Bill of Rights Act 1990.

20

Subpart 2—Enforcement provisions

*Approved Agency*

**7 Approved Agency**

25

(1) The Governor-General may, by Order in Council made on the recommendation of the Minister,—

(a) appoint as the Approved Agency for the purpose of this Act—

(i) any person or organisation:

30

(ii) any department:

(iii) any Crown entity:

(b) prescribe the functions of the Approved Agency that are in addition to the functions specified in **section 8(1)** and are related to the purpose of this Act:

35

- (c) prescribe any reporting requirements and accountability measures that the Approved Agency must comply with.
- (2) Before recommending the making of an Order in Council under **subsection (1)**, the Minister must be satisfied that the appointee has the appropriate knowledge, skills, and experience to carry out some or all of the functions of the Approved Agency under this Act. 5
- (3) The Approved Agency holds office for the term specified in the order made under **subsection (1)**.
- (4) A person is not to be regarded as being employed in the service of the Crown for the purposes of the State Sector Act 1988 or the Government Superannuation Fund Act 1956 solely because of his or her appointment as the Approved Agency. 10
- (5) The Approved Agency is subject to the Ombudsmen Act 1975, the Official Information Act 1982, and the Public Records Act 2005 in respect of functions it performs under this Act. 15

## 8 Functions and powers of Approved Agency

- (1) The functions of the Approved Agency are—
- (a) to receive and assess complaints about harm caused to persons~~individuals~~ by digital communications: 20
- (b) to use negotiation, mediation, and persuasion (as appropriate) to resolve complaints:
- (c) to investigate complaints, unless the Agency considers that—
- (i) the complaint is trivial, frivolous, or vexatious; 25
- or
- (ii) the subject matter or nature of the complaint is unlikely to cause harm to any individual; or
- (iii) investigating the subject matter or nature of the complaint is unlikely to uphold or enhance the communication principles: 30
- (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: 35

- (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**. 5
- (2) The Agency may, subject to any other enactment, seek and receive any information that the Agency considers will assist it in the performance of its functions.
- (2A) The Agency may refuse to investigate, or cease investigating, any complaint if the Agency considers that— 10
- (a) the complaint is trivial, frivolous, or vexatious; or
- (b) the subject matter or nature of the complaint is unlikely to cause harm to any individual; or
- (c) the subject matter or nature of the complaint does not contravene the communication principles. 15
- (3) The Agency may decide not to take any further action on a complaint if, in the course of assessing or investigating the complaint, it appears to the Agency that, having regard to all the circumstances of the case, any further action is unnecessary or inappropriate. 20
- (4) If the Agency decides not to take any further action on a complaint, it must notify the complainant of the right to apply to the District Court for an order under this Act.
- 8A Power of Approved Agency to delegate** 25
- (1) Subject to the approval of the Minister, the Approved Agency may delegate to any person or organisation any of its functions and powers except this power of delegation.
- (2) Before delegating any functions or powers, the Approved Agency must be satisfied that the delegate has the appropriate knowledge, skills, and experience to carry out those functions or powers. 30
- (3) A delegation—
- (a) must be in writing; and
- (b) is subject to any restrictions and conditions specified by the Approved Agency that it thinks fit, including conditions that relate to the Approved Agency's obligations under **section 7(5)**; and 35

- (c) is revocable at any time, in writing; and  
(d) does not prevent the performance or exercise of a function or power by the Approved Agency.
- (4) A person or organisation performing or exercising any delegated functions or powers may perform and exercise them in the same manner and with the same effect as if they had been conferred directly by this Act and not by delegation. 5
- (5) A person or organisation who acts under a delegation given under this section is presumed to be acting in accordance with its terms in the absence of evidence to the contrary. 10
- (6) Any action or decision of a delegate under the delegation is treated as an action or decision of the Approved Agency under this Act.
- (7) A delegate must comply with all reasonable requests or requirements of the Approved Agency for the purpose of enabling the Agency to comply with the Ombudsmen Act 1975, the Official Information Act 1982, and the Public Records Act 2005 in respect of functions to which the delegation applies. 15
- 9 Protection for employees of Agency**
- (1) This section applies if the Approved Agency is not a department or Crown entity. 20
- (2) If this section applies, no civil action lies against any employee of the Agency, or against any employee of a delegate of the Agency, for any act done or omitted by the Agency, or by the delegate, or by him or her, in good faith in the performance or intended performance of the functions, duties, or powers of the Agency. 25
- (3) However, **subsection (2)** does not prevent a person from filing an application for review under section 4 of the Judicature Amendment Act 1972 in relation to the exercise, refusal to exercise, or proposed or purported exercise by the Approved Agency of a statutory power within the meaning of that Act or otherwise affect the operation of that Act. 30

*Proceedings may be brought in District Court***10 Who may bring proceedings**

- (1) Any of the following may apply to a District Court for an order under **section 16 or 17**:
- (a) an individual (the affected individual) who alleges that he or she has suffered harm as a result of a harmful-digital communication: 5
  - (b) a parent or guardian on behalf of a person described in **paragraph (a)** the affected individual: 5
  - (c) the principal of an educational establishment, if a student of that establishment is a person described in **paragraph (a)** and the student consents to the principal bringing the proceedings: 10
  - (c) the professional leader of a registered school or his or her delegate, if the affected individual is a student of that school and consents to the professional leader or delegate bringing the proceedings: 15
  - (d) the Police, if the digital communication constitutes a threat to the safety of any person an individual.
- (2) The chief coroner may apply for an order under **section 16 or 17(1)(a) or (b) or (2)(a)** in respect of a digital communication that contravenes a provision of the Coroners Act 2006. 20

**11 Threshold for proceedings**

- (1) ~~A person to whom~~ An applicant referred to in section 10(1)(a), (b), or (c) applies may not apply for an order under **section 16 or 17** in respect of a digital communication unless the Approved Agency has first considered a complaint about the communication and had a reasonable opportunity to consider and decide what action (if any) to take. 25
- (2) In any case, a District Court must not grant an application from a person an applicant referred to in **section 10(1)(a) to (c), (b), or (c)** for an order under **section 16 or 17** unless it is satisfied that— 30
- (a) there has been a ~~serious or repeated~~ serious, repeated, or threatened breach of 1 or more communication principles; and 35
  - (b) the breach has caused or is likely to cause harm to a person an individual.

- (3) The court may, on its own initiative, dismiss an application from a ~~person to whom~~ man applicant referred to in **section 10(1)(a), (b), or (c)** ~~applies~~ without a hearing if it considers that the application is frivolous or vexatious, or for any other reason does not meet the threshold in **subsection (2)**. 5
- (4) The court may, on its own initiative, dismiss an application under **section 10** from the Police if satisfied that, having regard to all the circumstances of the case, the application should be dismissed.
- 12 District Court may refer matter back to Approved Agency** 10
- (1) This section applies when a District Court considers an application under **section 10** that arises from the subject matter of a complaint that has been considered by the Approved Agency (as required by **section 11(1)**).
- (2) The court— 15
- (a) must consider whether an attempt has been made to resolve the complaint (whether through mediation or otherwise); and
- (b) may adjourn the proceeding and refer the matter back to the Approved Agency unless satisfied that attempts 20  
at resolution, or further attempts at resolution, of the matter by the parties and the Agency—
- (i) will not contribute constructively to resolving the matter; or
- (ii) will not, in the circumstances, be in the public 25  
interest; or
- (iii) will undermine the proceedings before the court.

### *Procedure*

- 13 Applications**
- (1) Applications for any orders under **section 16 or 17** must— 30
- (a) be filed in a District Court; and
- (b) be in the prescribed form (if any).
- (2) The court may give directions as to service and, if the court considers it appropriate to do so in the circumstances, having regard to the principles of natural justice, the court may con- 35  
sider an application made on a without notice basis.

- (3) No filing fee is payable for an application.

#### 14 Mode of hearing and evidence

- (1) The court must, having regard to the circumstances of the particular case, direct that an application be determined—
- (a) just on the basis of written material provided to it; or 5
- (b) by way of a hearing involving oral submissions.
- (2) The court may deal with an application in any manner that it thinks will preserve the anonymity of the applicant, victim, or respondent.
- (3) The court must give reasons for any decision it makes in the proceedings and publish its decision. 10
- (3A) The decision, including the reasons, must be published.
- (4) **Subsection (3) is**Subsections (3) and (3A) are subject to **subsection (2)**.
- (5) The court may receive any evidence or information that may 15  
in its opinion assist it to deal effectively with any proceedings under this Act, whether or not the evidence or information would be otherwise admissible in a court of law.

#### 15 Technical advisers

- (1) A District Court or the High Court, as the case may be, may 20  
appoint a technical adviser to assist it in considering and determining an application for an order under **section 17** or any appeal under section 72 of the District Courts Act 1947.
- (2) The duties of a technical adviser are—
- (a) to sit with the court; and 25
- (b) subject to **subsection (3)(4)**, to act in all respects as an extra member of the court.
- (3) The court must appoint a technical adviser if the court is considering an application for an order under **section 17(2)(a) or (b) or (2A) or (3)(a)**. 30
- (4) The Judge may give any weight to the technical adviser's advice that the Judge thinks fit, and the Judge alone must determine the application or appeal.
- (5) The Minister must maintain a panel of persons who may be appointed under this section as technical advisers, and only per- 35

sons named on the panel may be appointed under this section as technical advisers.

- (6) The chief executive must pay technical advisers the remuneration and allowances determined from time to time by the Minister. 5

## 16 Interim orders

- (1) This section applies if a party applies for any orders under **section 17**:

- (2) A District Court may, if the court considers it is desirable to do so, grant any interim orders pending the determination of the application for orders under **section 17**. 10
- (3) An interim order under this section may do anything that may be done by order under **section 17** and expires when the application under that section is determined.

## 17 Orders that may be made by court

15

- (1) The District Court may, on an application, make 1 or more of the following orders against a defendant:

- (a) an order to ~~takedown~~ take down or disable material:
- (b) an order that the defendant cease the conduct concerned:
- (c) an order that the defendant not encourage any other persons to engage in similar communications towards the person specified in **section 10(1)(a)** affected individual: 20
- (d) an order that a correction be published:
- (e) an order that a right of reply be given to the person specified in **section 10(1)(a)** affected individual: 25
- (f) an order that an apology be published.

- (2) The District Court may, on an application, make 1 or more of the following orders against an online content host:

- (a) an order to take down or disable public access to material: 30
- (b) an order that the identity of the author of an anonymous or pseudonymous communication be released to the court:
- (c) an order that a correction be published: 35



- (d) an order that a right of reply be given to the ~~person specified in section 10(1)(a)~~ affected individual.
- (2A) The District Court may, on application, make an order against an IPAP that the identity of an anonymous communicator be released to the court. 5
- (3) The court may also do 1 or more of the following:
- (a) make a direction applying an order provided for in **subsection (1) or (2)** to other persons specified in the direction, if there is evidence that those others have been encouraged to engage in harmful digital communications towards the ~~person specified in section 10(1)(a)~~ affected individual: 10
- (b) make a declaration that a communication breaches a communication principle:
- (c) order that the names of any specified parties be suppressed. 15
- (4) In deciding whether or not to make an order, and the form of an order, the court must take into account the following:
- (a) the content of the communication and the level of harm caused by it: 20
- (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: 25
- (e) the age and vulnerability of the ~~victim~~ affected individual:
- (f) the truth or falsity of the statement:
- (g) whether the communication is in the public interest: 30
- (h) the conduct of the defendant, including any attempt by the defendant to minimise the harm caused:
- (i) the conduct of the ~~victim~~ affected individual or complainant:
- (j) the technical and operational practicalities, and the costs, of an order: 35
- (k) the appropriate individual or other person who should be subject to the order.

- (5) In doing anything under this section, the court must act consistently with the rights and freedoms contained in the New Zealand Bill of Rights Act 1990.

#### **17A Court may vary or discharge order**

- (1) Any applicant who obtains an order under **section 16 or 17** or any other party to that order may apply for an order under **subsection (2)**. 5
- (2) The District Court may, by order, do any of the following things to an order made under **section 16 or 17**:
- (a) vary the duration of the order: 10
- (b) vary any conditions of the order:
- (c) discharge the order.

#### *Offences*

#### **18 Offence of non-compliance with order**

- (1) A person who, without reasonable excuse, fails to comply with an order made under **section 16 or 17** commits an offence. 15
- (2) A person who commits an offence against this section is liable on conviction to a fine not exceeding—
- (a) in the case of a natural person, imprisonment for a term not exceeding 6 months or a fine not exceeding \$5,000: 20
- (b) in the case of a body corporate, a fine not exceeding \$20,000.

#### **19 Causing harm by posting digital communication**

- (1) A person commits an offence if—
- (a) the person posts a digital communication with the intention that it cause harm to a victim; and 25
- (b) posting the communication would cause harm to an ordinary reasonable person in the position of the victim; and
- (c) posting the communication causes harm to the victim. 30
- (2) In determining whether a post would cause harm, the court may take into account any factors it considers relevant, including—
- (a) the extremity of the language used;
- (b) the age and characteristics of the victim: 35

- (c) whether the digital communication was anonymous:
  - (d) whether the digital communication was repeated:
  - (e) the extent of circulation of the digital communication:
  - (f) whether the digital communication is true or false:
  - (g) the context in which the digital communication appeared. 5
- (3) A person who commits an offence against this section is liable on conviction to imprisonment for a term not exceeding 3 months 2 years or a fine not exceeding \$2,000.
- (4) In this section,— 10
- intimate visual recording—**
- (a) means a visual recording (for example, a photograph, videotape, or digital image) that is made in any medium using any device with or without the knowledge or consent of the person who is the subject of the recording, and that is of— 15
    - (i) a person who is in a place which, in the circumstances, would reasonably be expected to provide privacy, and that person is—
      - (A) naked or has his or her genitals, pubic area, buttocks, or female breasts exposed, partially exposed, or clad solely in undergarments; or 20
      - (B) engaged in an intimate sexual activity; or
      - (C) engaged in showering, toileting, or other personal bodily activity that involves dressing or undressing; or 25
    - (ii) a person’s naked or undergarment-clad genitals, pubic area, buttocks, or female breasts which is made— 30
      - (A) from beneath or under a person’s clothing; or
      - (B) through a person’s outer clothing in circumstances where it is unreasonable to do so. 35
  - (b) includes an intimate visual recording that is made and transmitted in real time without retention or storage in—
    - (i) a physical form; or

- (ii) an electronic form from which the recording is capable of being reproduced with or without the aid of any device or thing

**posts a digital communication—**

- (a) means transfers, sends, posts, publishes, disseminates, or otherwise communicates by means of a digital communication any information, whether truthful or untruthful, about the victim; and 5
- (b) includes publishing an intimate visual recording of another person; and 10
- (c) includes an attempt to do anything referred to in **paragraph (a) or (b)**

**victim** means the person who is the target of the conduct elicited by the posted digital communication.

- (4) In this section, **victim** means the individual who is the target of a posted digital communication. 15

Compare: 1961 No 43 s 216G; Michigan Penal Code 1931 S750.411s

**20 Liability of online content host for content posted by user**

- (1) This section applies to the liability of an online content host for the content of a digital communication posted by a person and hosted by the online content host. 20
- (2) No civil or criminal proceedings may be brought against the online content host in respect of the content complained of (the **specific content**) unless—
  - (a) the person who provides the specific content does so on behalf, or at the direction, of the online content host; or 25
  - (b) the online content host—
    - (i) receives a notice of complaint about the specific content; and
    - (ii) does not take reasonable steps as soon as is reasonably practicable to remove or disable access to the specific content. 30
- (3) A notice of complaint must—
  - (a) specify the complainant's name; and
  - (b) set out the specific content, and explain why the complainant considers that—
    - (i) the specific content is unlawful; or 35

- (ii) the specific content ought to be taken down or access to it disabled because it is harmful or otherwise objectionable; and
- (c) sufficiently enable the specific content to be readily located; and 5
- (d) contain any other information that the complainant considers relevant.
- (4) The Approved Agency may lodge a notice of complaint on behalf of a complainant and provide advice and assistance to the complainant in relation to the complaint. 10
- (5) The protection conferred on an online content host by **subsection (2)** does not apply if the host does not provide an easily accessible mechanism that enables a user to contact the host about specific content as provided in **subsection (3)**.
- (6) Nothing in **subsection (2)** affects— 15
  - (a) section 211 of the Criminal Procedure Act 2011; or
  - (b) section 19 of the Bail Act 2000; or
  - (c) copyright liability, or any proceedings, under the Copyright Act 1994; or
  - (d) any enactment that expressly overrides **subsection (2)**. 20

*Liability of online content host*

**20 Liability of online content host for content posted by user**

- (1) This section and **section 20A** apply to the liability of an online content host for the content of a digital communication posted by a person and hosted by the online content host. 25
- (2) No civil or criminal proceedings may be brought against the online content host in respect of the content complained of (the **specific content**) unless—
  - (a) the person who provides the specific content does so on behalf, or at the direction, of the online content host; 30
  - (b) the online content host—
    - (i) receives a notice of complaint about the specific content; and
    - (ii) does not comply with **subsections (3) and (4)**.
- (3) The requirements of this subsection are that— 35

- Host to notify author of complaint*
- (a) the online content host must, as soon as practicable but no later than 48 hours after receiving a notice of complaint,—
- (i) provide the author of the specific content with a copy of the notice of complaint; and 5
- (ii) notify the author that the author may submit a counter-notice to the host within 48 hours after receiving that notification:
- (b) if the host is unable to contact the author (for example, because the identity of the author is unknown) after taking reasonable steps to do so, the host must take down or disable the specific content as soon as practicable after taking those steps: 10
- Author's counter-notice consenting to removal of content* 15
- (c) if the author submits a valid counter-notice no later than 48 hours after receiving the host's notification under **paragraph (a)**, in which the author consents to the removal of the specific content, the host must take down or disable the specific content as soon as practicable after receiving that counter-notice: 20
- Author's counter-notice refusing consent to removal of content*
- (d) if the author submits a valid counter-notice no later than 48 hours after receiving the host's notification under **paragraph (a)**, in which the author refuses to consent to the removal of the specific content, the host must leave the specific content in place and, as soon as practicable after receiving that counter-notice,— 25
- (i) notify the complainant of the author's decision; and 30
- (ii) if the author consents, provide the complainant with personal information that identifies the author: 35
- Author failing to submit valid counter-notice*
- (e) if the author does not submit a valid counter-notice in accordance with this subsection (whether by failing

to submit a counter-notice or by submitting an invalid counter-notice), the host must take down or disable the specific content as soon as practicable but no later than 48 hours after notifying the author under **paragraph (a)**.

5

(4) A notice of complaint must—

(a) state the name and address for service of the complainant; and

(b) state the specific content, and explain why the complainant considers that the specific content—

10

(i) is unlawful; or

(ii) breaches 1 or more communication principles and has caused harm; and

(c) sufficiently enable the specific content to be readily located; and

15

(d) state whether the complainant consents to personal information that identifies the complainant being released to the author; and

(e) contain any other information that the complainant considers relevant.

20

(5) A counter-notice must state—

(a) the name and address for service of the author; and

(b) whether the author consents to personal information that identifies the author being released to the complainant; and

25

(c) whether the author consents to the removal of the specific content.

(6) The protection conferred on an online content host by this section does not apply if the host does not provide an easily accessible mechanism that enables a user to contact the host about specific content as provided in this section.

30

**20A Further provisions relating to liability of online content host**

(1) If consent to the release of personal information that identifies the party giving the notice is withheld under **section 20**, the online content host must hold that personal information as confidential information that is not to be released except by

35

- order of a District Court Judge or High Court Judge made on an application under this subsection.
- (2) The Approved Agency may lodge a notice of complaint under **section 20** on behalf of a complainant and provide advice and assistance to the complainant in relation to the complaint. 5
- (3) The fact that an online content host does not take advantage of **section 20(2)** does not of itself create any civil or criminal liability for hosting the specific content.
- (4) Nothing in **section 20** or this section affects—  
 (a) section 211 of the Criminal Procedure Act 2011; or 10  
 (b) section 19 of the Bail Act 2000; or  
 (c) copyright liability, or any proceedings, under the Copyright Act 1994; or  
 (d) any enactment that expressly overrides **subsection (2)**.
- (5) Nothing in **section 20** or this section limits the right of an individual to injunctive relief in relation to the content of a digital communication posted by another person and hosted by the online content host. 15

### *Regulations and rules*

- 21 Regulations** 20
- (1) The Governor-General may, by Order in Council, make regulations providing for any matters contemplated by this Act, necessary for its administration, or necessary for giving it full effect.
- (2) Without limiting the generality of **subsection (1)**, regulations made under that subsection may prescribe the practice and procedure for the conduct of matters under this Act before the Approved Agency. 25
- 21 Regulations** 30
- The Governor-General may, by Order in Council, make regulations for all or any of the following purposes:
- (a) prescribing the practice and procedure for the conduct of matters under this Act before the Approved Agency;
- (b) providing for any other matters contemplated by this Act, necessary for its administration, or necessary for giving it full effect. 35



**22 Rules**

- (1) The power to make rules of court under section 51C of the Judicature Act 1908 and section 122(1) of the District Courts Act 1947 includes the power to make rules regulating the practice and procedure of courts in the exercise of jurisdiction conferred by this Act. 5
- (2) Without limiting the generality of **subsection (1)**, rules made in accordance with that subsection may—
- (a) prescribe forms for applications and orders under this Act: 10
- (b) prescribe the practice and procedure for the conduct of matters under this Act before the District Court.

**22A Consequential amendments to other Acts**

Amend the Acts specified in the Schedule as set out in that schedule. 15

**Part 2****Amendments to other Acts concerning use of digital communications****Subpart 1—Crimes Act 1961**

- 23 Principal Act** 20  
**This subpart** amends the Crimes Act 1961.
- 24 Section 179 amended (Aiding and abetting suicide)**  
In section 179, insert as subsections (2) and (3):
- “(2) A person commits an offence who incites, counsels, or procures another person to commit suicide, if that other person does not commit or attempt to commit suicide in consequence of that conduct. 25
- “(3) A person who commits an offence against **subsection (2)** is liable on conviction to imprisonment for a term not exceeding 3 years.” 30

**Subpart 2—Harassment Act 1997**

- 25 Principal Act**  
**This subpart** amends the Harassment Act 1997.

**26 Section 3 amended (Meaning of harassment)**

After section 3(2), insert:

“(3) For the purposes of this Act, a person also harasses another person if—

“(a) he or she engages in a pattern of behaviour that is directed against that other person; and

“(b) that pattern of behaviour includes doing any specified act to the other person that is one continuing act carried out over any period.

“(4) For the purposes of **subsection (3), continuing act** includes a specified act done on any one occasion that continues to have effect over a protracted period (for example, where offensive material about a person is placed in any electronic media and remains there for a protracted period).”

**27 Section 4 amended (Meaning of specified act)**

(1) In section 4(1)(d), after “correspondence,” insert “electronic communication,”.

(2) After section 4(1)(e), insert:

“(ea) giving offensive material to a person by placing the material in any electronic media where it is likely that it will be seen by, or brought to the attention of, that person.”.

**28 Section 19 amended (Standard conditions of restraining orders)**

After section 19(1), insert:

“(1A) It is a condition of every restraining order that applies to a continuing act within the meaning of section 3 that the respondent must take reasonable steps to prevent the specified act from continuing.”

## Subpart 3—Human Rights Act 1993

**29 Principal Act**

**This subpart** amends the Human Rights Act 1993.

- 30 Section 61 amended (Racial disharmony)**
- (1) In section 61(1)(a), after “radio or television” insert “or other electronic communication”.
- (2) In section 61(2), after “radio or television” insert “or other electronic communication”. 5
- 31 Section 62 amended (Sexual harassment)**  
After section 62(3)(j), insert:  
“(k) participation in fora for the exchange of ideas and information.”
- 32 Section 63 amended (Racial harassment)** 10  
After section 63(2)(j), insert:  
“(k) participation in fora for the exchange of ideas and information.”
- Subpart 4—Privacy Act 1993
- 33 Principal Act** 15  
**This subpart** amends the Privacy Act 1993.
- 34 Section 6 amended (Information privacy principles)**
- (1) In section 6, Principle 10(a), after “publicly available publication”, insert “and that, in the circumstances of the case, it would not be unfair or unreasonable to use the information”. 20
- (2) In section 6, Principle 11(b), after “publicly available publication”, insert “and that, in the circumstances of the case, it would not be unfair or unreasonable to disclose the information”.
- 35 Section 56 amended (Personal information relating to domestic affairs)** 25  
In section 56, insert as subsection (2):  
“(2) The exemption in subsection (1) ceases to apply once the personal information concerned is collected, disclosed, or used, if that collection, disclosure, or use would be highly offensive to an ordinary reasonable person.” 30

**Schedule****s 22A****Consequential amendments to other Acts****Ombudsmen Act 1975 (1975 No 9)**

In Schedule 1, Part 2, insert in its appropriate alphabetical order: “Approved Agency under the Harmful Digital Communications Act 2013, in its role under that Act”.

5

**Public Records Act 2005 (2005 No 40)**

In section 4, definition of **public office**, after paragraph (c)(x), insert:

“(xa) the Approved Agency under the Harmful Digital Communications Act 2013, in its role under that Act; and”.

10

**Legislative history**

5 November 2013

Introduction (Bill 168–1)

3 December 2013

First reading and referral to Justice and Electoral Committee