Chapter 1

Introduction

1.1 On 7 September 2017 the Senate referred the following matter to the Legal and Constitutional Affairs References Committee (the committee) for inquiry and report by 29 November 2017:

> The adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying, including:
>
> (a) the broadcasting of assaults and other crimes via social media platforms;
>
> (b) the application of section 474.17 of the Commonwealth Criminal Code 'Using a carriage service to menace, harass or cause offence', and the adequacy of the penalty, particularly where the victim of cyberbullying has self-harmed or taken their own life;
>
> (c) the adequacy of the policies, procedures and practices of social media platforms in preventing and addressing cyberbullying;
>
> (d) other measures used to combat cyberbullying predominantly between school children and young people; and
>
> (e) any other related matter.[1]

1.2 On 19 October 2017 the Senate extended the committee's reporting date to the last sitting day in March 2018.[2]

Conduct of this inquiry

1.3 Details of this inquiry were advertised on the committee's website, including a call for submissions to be received by 13 October 2017.[3] The committee continued to accept submissions after this deadline. The committee wrote directly to some organisations inviting them to make submissions. The committee received 34 submissions, of which three were received *in camera*. An attachment to one of the 34 submissions was also received *in camera*. The submissions are listed at appendix 1 of this report.

1.4 The committee held two public hearings. The first hearing was in Canberra on 9 February 2018 and the second in Melbourne on 7 March 2018. A list of witnesses who appeared at the hearings is available at appendix 2.

1.5 The committee thanks all those who made submissions or gave evidence at its public hearings. The committee gives particular thanks to those who gave evidence regarding the extreme effects of cyberbullying and online abuse on their lives.

---

1 *Proof Journals of the Senate*, No. 59, 7 September 2017, p. 1896.

2 *Proof Journals of the Senate*, No. 67, 19 October 2017, p. 2140.

3 The committee's website can be found at www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs.

Structure of this report

1.6 There are 5 chapters in this report:

- This chapter provides information about the conduct of the inquiry as well as relevant background.
- Chapter 2 examines the nature and prevalence of cyberbullying.
- Chapter 3 considers the adequacy of existing criminal offences.
- Chapter 4 examines the policies, procedures and practices of social media platforms, as well as education and prevention initiatives.
- Chapter 5 provides the committee's view.

Background

1.7 The motion referring this matter to the committee was moved by former Senator Kakoschke-Moore.[4] The former senator stated that she moved the motion in response to the death of Libby Bell, a 13 year old girl who resided in South Australia.[5] Ms Bell committed suicide in August 2017 and her family has said that she suffered cyberbullying and physical bullying.

1.8 The problem of cyberbullying has received significant public attention.[6] In particular, the committee is aware of a number of youth suicides in recent years that were linked in the media, to at least some extent, with cyberbullying. One recent, high profile example is the suicide of 14 year old Amy "Dolly" Everett in January 2018.

1.9 The Council of Australian Governments (COAG) discussed cyberbullying at its meeting on 9 February 2018. The communique from that meeting stated:

> Bullying has no place in Australia, and can be especially harmful on children and young people. The growth of social media and mobile devices means that Australians can be subject to bullying 24 hours a day and from any location. Leaders heard from the eSafety Commissioner, Ms Julie Inman Grant, on initiatives to combat cyberbullying and acknowledged the ongoing importance of this work. First Ministers agreed that if we are to successfully reduce the incidence of bullying, we must better understand its underlying drivers and adopt a whole-of-community approach. COAG agreed that a working group of senior officials from First Ministers', Education, Justice and Health departments consider existing and potential initiatives to help combat bullying and cyberbullying and establish a work program to be led by the Education Council. The

4 *Proof Journals of the Senate*, No. 59, 7 September 2017, p. 1896.

5 Skye Kakoschke-Moore, 'Skye Kakoschke-Moore: Cyberbullying won't be solved quickly', *The Advertiser*, 2 October 2017, http://www.adelaidenow.com.au/news/opinion/skye-kakoschkemoore-cyberbullying-wont-be-solved-quickly/news-story/2234ab1b5af0257dfb2ea39750513c3f (accessed 13 December 2017).

6 See, for a recent example, Genevieve Gannon, 'Sticks and stones and mobile phones' *The Australian Women's Weekly*, March 2018, pp. 40–44.

> Education Council will report to COAG at its next meeting on tangible measures where there is an identified need.[7]

1.10 On 19 February 2018, the Queensland Government announced the formation of an anti-cyberbullying task force to make recommendations by 31 August 2018. The task force is chaired by Ms Madonna King, journalist and author.[8]

1.11 On 25 February 2018, it was reported that Minister for Education and Training, Senator the Hon. Simon Birmingham, stated:

> Following the discussion of bullying at COAG I have asked all state education ministers to bring examples of effective anti-bullying programs and the evidence that supports them to our next education council meeting.[9]

1.12 On 28 February 2018, the Prime Minister, the Hon. Malcolm Turnbull MP, and the Minister for Education and Training, Senator the Hon. Simon Birmingham, wrote to all school principals in Australia. Their letter stated: '[w]e encourage you and your school community to get involved in the National Day of Action against Bullying and Violence 2018', then upcoming on 16 March 2018.[10]

The eSafety Commissioner

1.13 The Children's eSafety Commissioner was established under the *Enhancing Online Safety Act 2015* (Online Safety Act) as an independent statutory office '…to take a national leadership role in online safety for children.'[11]

1.14 In June 2017 the Children's eSafety Commissioner's functions were expanded to include all Australians, not only Australian children.[12] Accordingly, the name was changed to the eSafety Commissioner. The broadened role of the eSafety Commissioner includes:

---

7 Council of Australian Governments, COAG meeting Communiqué, 9 February 2018, http://www.coag.gov.au/meeting-outcomes/coag-meeting-communiqu%C3%A9-9-february-2018 (accessed 26 February 2018).

8 The Hon. Annastacia Palaszczuk, Premier and Minister for Trade, 'Membership and terms of reference for Queensland Anti-Cyberbullying Task Force', *Media Statements*, 19 February 2018, http://statements.qld.gov.au/Statement/2018/2/19/membership-and-terms-of-reference-for-queensland-anticyberbullying-task-force (accessed 21 March 2018).

9 Senator the Hon. Simon Birmingham, Minister for Education and Training, in Lanai Scarr, 'Cyber-bullying epidemic: Australia falls behind in efforts to protect vulnerable kids', *Sunday Tasmanian*, 25 February 2018, p. 19.

10 Australian Government Department of Education and Training, answers to questions on notice, 7 March 2018 (received 16 March 2018), Attachment A.

11 Explanatory Memorandum, Enhancing Online Safety for Children Bill 2014 and Enhancing Online Safety for Children (Consequential Amendments) Bill 2014, pp. 1–2.

12 Enhancing Online Safety for Children Amendment Bill 2017.

> …functions in relation to persons at risk of family or domestic violence, in relation to victims of the non-consensual sharing of intimate images, and in relation to the safe use of the internet by older Australians.[13]

1.15 A key function of the eSafety Commissioner is to administer a complaints system for cyberbullying material targeting an Australian child.[14] The eSafety Commissioner stated that '[t]he scheme empowers the office to remove cyberbullying material that is posted online quickly. It is the only one of its kind in the world…'.[15]

1.16 However, the 2017 expansion did not extend the cyberbullying complaints scheme to adults; the scheme remains limited to cyberbullying material targeting an Australian child. The Explanatory Memorandum for the relevant bill explained:

> This is because while the Government recognises that online dangers such as cyber-bullying apply to both adults and children, there are existing avenues, including existing criminal laws, which apply to using the internet to menace and harass people of all ages.
>
> In our society, there are a range of areas where extra protections are put in place for children consistent with Australia's obligations under the [Convention on the Rights of the Child]. The Government considers child victims of cyber-bullying a priority.
>
> The Government does not consider there is any need to create any new powers to investigate cyberbullying complaints between adults at this time.[16]

1.17 Since the Office of the eSafety Commissioner (eSafety Office) was established in July 2015, '…the Commissioner has resolved approximately 550 complaints in relation to cyberbullying material.'[17] Between 1 October 2017 and 31 January 2018, cyberbullying complaints to the eSafety Office increased by 30% compared to the same period 12 months prior.[18] In addition, the eSafety Office has referred approximately 6,000 young Australians to the Kids Helpline.[19] The committee notes that it is plausible that there are many more cases of cyberbullying than indicated by these figures, as many cases would not be reported to the eSafety Commissioner.

---

13 Explanatory Memorandum, Enhancing Online Safety for Children Amendment Bill 2017, p. 2.

14 Explanatory Memorandum, Enhancing Online Safety for Children Bill 2014 and Enhancing Online Safety for Children (Consequential Amendments) Bill 2014, p. 2; Office of the eSafety Commissioner (eSafety Office), *Submission 13*, p.4.

15 Ms Julie Inman Grant, eSafety Commissioner, eSafety Office, *Committee Hansard*, 9 February 2018, p. 61.

16 Explanatory Memorandum, Enhancing Online Safety for Children Amendment Bill 2017, p. 9.

17 eSafety Office, *Submission 13*, p. 2.

18 eSafety Office, answers to questions on notice, 9 February 2018 (received 7 March 2018), p. 2.

19 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 64.

1.18 The eSafety Office manages these cyberbullying cases, and its other work, with a staff of approximately 78 and a budget of about $17 million per annum. The team that deals with cyberbullying complaints is comprised of four staff.[20]

The tier scheme for cyberbullying complaints

1.19 The Online Safety Act '…establishes a two-tiered scheme for the rapid removal from social media services of cyberbullying material targeted at an Australian child.'[21] The eSafety Office explained that:

> [a] social media service can apply to the Commissioner to be declared a Tier 1 social media service. To be declared a Tier 1 service, the Commissioner must be satisfied that the social media service meets certain basic online safety requirements.[22]

1.20 These safety requirements include that the platform have terms of use that prohibit cyberbullying, that it provide a clear complaints process for users, and that it designate a contact person to liaise with the eSafety Office for the purposes of the Online Safety Act.[23]

1.21 The eSafety Commissioner can issue a notice requesting that a Tier 1 service remove cyberbullying material within 48 hours:

> Non-compliance with a notice by a Tier 1 service does not attract a legal penalty. However, if a Tier 1 service repeatedly fails to comply with a request to remove material, or if it no longer complies with the Act's basic online safety requirements under section 21 of the Act, the Commissioner can revoke its tier 1 status.
>
> The Commissioner may also publish a statement on the Commissioner's website to the effect that a Tier 1 social media service has failed to remove material when requested.[24]

1.22 A social media service may be declared as Tier 2 by the minister on recommendation from the eSafety Commissioner. To make such a recommendation, the eSafety Commissioner '…must be satisfied that the service is a "large social media service", or that the service has *requested* to be a Tier 2 service.'[25]

1.23 Tier 2 services are '… subject to somewhat more interventionist measures.'[26] The eSafety Commissioner may issue a Tier 2 service with a notice requiring the

---

20 Ms Inman Grant, eSafety Commissioner, and Mr Toby Dagg, Acting Manager, Compliance Tools and Citizen Services, eSafety Office, Committee Hansard, 9 February 2018, p. 73.

21 eSafety Office, *Submission 13*, p. 4.

22 eSafety Office, *Submission 13*, p. 5.

23 eSafety Office, *Submission 13*, p. 4; Mr Dagg, eSafety Office, *Committee Hansard*, 9 February 2018, p. 63.

24 eSafety Office, *Submission 13*, p. 5.

25 eSafety Office, *Submission 13*, p. 5.

26 Mr Dagg, eSafety Office, *Committee Hansard*, 9 February 2018, p. 63.

service to remove cyberbullying material within 48 hours. However, the material must have first been reported to the service by a user, and 48 hours must have elapsed since that time. If a Tier 2 service does not comply with a notice then enforcement action may be taken.[27]

1.24 This tier scheme was summarised by the eSafety Office follows:

> Basically, the tier 1 scheme is an opt-in scheme, so a company can volunteer. However, in the instances where we've identified that a lot of cyberbullying is occurring on a particular site and we've invited them to become tier 1 but they didn't elect to take up that offer or invitation, we can declare them or recommend that they be declared tier 2, which, in turn, gives us more enforcement power.[28]

1.25 Currently, the social media services declared as Tier 1 are: airG, Ask.fm, Snapchat, Twitter, Yahoo!7 Answers, and Yahoo!7 Groups. The services declared as Tier 2 are: Facebook, Google+, Instagram, and Youtube.[29]

The eSafety Commissioner's discretionary powers

1.26 The eSafety Commissioner has '…a broad range of discretionary powers and civil penalties…'.[30] The eSafety Commissioner stated that:

> [t]his includes fines of up to $18,000 a day for tier 2 social media sites that do not comply with our take-down notices. While this might be pocket change for some of the behemoths, using our position to name and shame, and to make a reputational impact, cannot be underestimated.[31]

1.27 The eSafety Commissioner has not yet used its formal powers or issued any civil penalties as it has not yet considered this to be appropriate.'[32]

1.28 The eSafety Commissioner may also issue an end-user notice to an individual person who posted cyberbullying material, requiring them to:

- take all reasonable steps to ensure the removal of the material;
- refrain from posting any cyberbullying material targeting a child, or
- apologise for posting the material.[33]

---

27 eSafety Office, *Submission 13*, p. 5; Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 62.

28 Ms Maria Vassiliadis, Executive Manager, eSafety Office, *Committee Hansard*, 9 February 2018, p. 63.

29 eSafety Office, *Submission 13*, p. 6.

30 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 61.

31 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 61.

32 Ms Inman Grant, eSafety Commissioner, and Mr Dagg, eSafety Office, *Committee Hansard*, 9 February 2018, p. 64.

33 eSafety Office, *Submission 13*, p.6.

1.29 The eSafety Office submitted that it '…recognise[s] the need to be proportionate and balanced in how discretionary powers might be used to deal with cyberbullying', particularly where the cyberbullying material was posted by a child.[34]

1.30 The eSafety Office stated that it has not yet issued any end-user notices:

> To date, the cases handled by the Office have not warranted such an intervention. Each has been resolved through the 'hybrid' approach of taking the material down quickly whilst also working with schools, parents and victims.[35]

Australian Cybercrime Online Reporting Network

1.31 The Australian Cybercrime Online Reporting Network (ACORN) is:

> …a national policing initiative of the Commonwealth, State and Territory governments. It is a national online system that allows the public to securely report instances of cybercrime. It will also provide advice to help people recognise and avoid common types of cybercrime.[36]

1.32 The ACORN was '…a key initiative under the 2013 *National Plan to Combat Cybercrime*.'[37] The ACORN's website lists cyberbullying as a type of cybercrime.[38]

Existing policies and legislation

1.33 The committee heard evidence about polices and legislation that relate to cyberbullying both in Australia and overseas.[39]

Australia

1.34 In general, Commonwealth offences that could apply to cyberbullying relate to the misuse of carriage services. These offences are examined in greater detail in Chapter 3.

1.35 State and territory criminal offences that could apply to cyberbullying vary between jurisdictions. Generally speaking, there are a variety of offences in each jurisdiction that could apply to cyberbullying behaviours. These offences tend to relate

---

34 eSafety Office, *Submission 13*, p.6.

35 eSafety Office, *Submission 13*, p.7.

36 Australian Cybercrime Online Reporting Network (ACORN), 'About the ACORN', https://www.acorn.gov.au/about-acorn (accessed 19 March 2018).

37 Attorney-General's Department, 'Cybercrime', https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx (accessed 19 March 2018).

38 ACORN, 'Learn about cybercrime', https://www.acorn.gov.au/learn-about-cybercrime (accessed 19 March 2018).

39 See, for example, eSafety Commissioner, answers to questions on notice, 9 February 2018 (received 7 March 2018).

to stalking, harassment, assault, threats, and defamation.[40] Some examples of specific offences are as follows:

- Section 60E of the *Crimes Act 1900* (New South Wales) contains '…a criminal provision for bullying which makes it an offence to assault, stalk, harass or intimidate any school student or member of staff of a school while the student or member of staff is attending a school.'[41] The maximum penalty ranges from five to 12 years' imprisonment depending on the severity of the offence. While this provision could apply to cyberbullying, '…the necessary act must take place at a school', thereby limiting the application of the offence.[42]
- Part 5A of the *Summary Offences Act 1953* (South Australia) includes a range of offences relating to cyberbullying and the non-consensual sharing of intimate images. This includes offences against humiliating or degrading filming, distribution of an invasive image, indecent filming, and threatening to distribute invasive images.[43]
- "Brodie's Law" in Victoria makes serious bullying a criminal offence by extending '…the definition of stalking in section 21A of the *Crimes Act 1958* (Vic) to specifically include behaviour that could lead a person to self-harm.'[44] The offence is punishable by up to 10 years' imprisonment, and could apply to serious cyberbullying.[45] The offence was introduced following the passage of the Crimes Amendment (Bullying) Bill 2011 in June 2011. It is known as "Brodie's Law", named after Ms Brodie Panlock who committed suicide in 2006 at age 19 after suffering bullying in her workplace.

Non-consensual sharing of intimate images

1.36 The committee heard evidence relating to the non-consensual sharing of intimate images as a further type of cyberbullying.[46] In May 2017 all Australian jurisdictions agreed, through the Law, Crime and Community Safety Council, to the

40 For listings of specific legislative provisions, see Australian Universities' Anti-bullying Research Alliance, *Submission 1*, pp. 5–6; Law Council of Australia, *Submission 15*, p. 11.

41 Mental Health Commissions of Australia, *Submission 9*, pp. 4–5.

42 Mental Health Commissions of Australia, *Submission 9*, p. 5.

43 South Australian Government, *Submission 21*, pp. 2–5.

44 Mental Health Commissions of Australia, *Submission 9*, p. 3.

45 Victoria State Government Justice and Regulation, *Bullying – Brodie's Law*, http://www.justice.vic.gov.au/home/safer+communities/crime+prevention/bullying+-+brodies+law (accessed 20 December 2017).

46 See, for example, Instagram, *Submission 3*, p. 3; Facebook, *Submission 4*, p. 4; Western Australia Police Force, *Submission 11*, p. 2; Australian Women Against Violence Alliance, *Submission 14*, p. 2; South Australian Government, *Submission 21*, p. 8;

National Statement of principles relating to the criminalisation of the non-consensual sharing of intimate images.[47] These principles are non-binding and state:

> This document identifies best practice principles to be considered as each jurisdiction continues to develop and review its criminal law, policy and practices to suit local needs, and for each jurisdiction to adopt and implement as that jurisdiction sees fit.[48]

1.37 Most Australian states and territories have introduced offences that specifically relate to the non-consensual sharing of intimate images.[49]

1.38 On 6 December 2017 the Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Bill 2017 was introduced into the Senate by the Assistant Minister to the Prime Minister, Senator the Hon. James McGrath. The bill would introduce a civil penalty regime for the non-consensual sharing of intimate images, with penalties of up to $105,000 for an individual and $525,000 for a body corporate. The regime would be administered by the eSafety Commissioner.

1.39 The bill passed the Senate with amendments on 14 February 2018.[50] The bill was amended to:

- require the minister to cause an independent review of the operation of the bill to be conducted within three years, and to table a copy of the review's report in parliament; and
- introduce criminal offences relating to the non-consensual sharing of intimate images.

1.40 At the time of writing, the bill is before the House of Representatives.

Harmful Digital Communications Act 2015 (New Zealand)

1.41 Some submitters referred to New Zealand's *Harmful Digital Communications Act 2015* (Harmful Communications Act) as potentially useful for considering reform in Australia.[51]

---

47 Communique, Law, Crime and Community Safety Council, 19 May 2017, https://www.ag.gov.au/About/CommitteesandCouncils/Law-Crime-and-Community-Safety-Council/Documents/19-May-LCCSC-Communique.pdf (accessed 5 February 2018).

48 National statement of principles relating to the criminalisation of the non-consensual sharing of intimate images, Law, Crime and Community Safety Council, https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National-statement-of-principles-criminalisation-non-consensual-sharing-intimate-images.PDF (accessed 5 February 2018).

49 Terry Goldsworthy, 'Revenge porn laws may not be capturing the right people', *The Conversation*, 29 September 2017, https://theconversation.com/revenge-porn-laws-may-not-be-capturing-the-right-people-84061 (accessed 13 March 2018).

50 *Proof Journals of the Senate*, No. 86, 14 February 2018, p. 2714.

51 See, for example, National Council of Single Mothers & their Children, *Submission 7*, p. 2; Alannah & Madeline Foundation, *Submission 10*, p. 6; Media, Entertainment & Arts Alliance, *Submission 28*, p. 7; Maurice Blackburn Lawyers, *Submission 29*, p. 5

1.42 Key features of the Harmful Communications Act include the following:[52]

- Making it a criminal offence to '…post a digital communication with the intention that it cause harm to a victim…', where posting the communication harmed the victim and would have caused harm '…to an ordinary reasonable person in the position of the victim…'.[53] The offence is punishable by up to two years' imprisonment or a maximum fine of $50,000 for individuals or $200,000 for companies.
- Establishing an approved agency to resolve complaints about harmful digital communications. NetSafe has been appointed as the approved agency.
- Enabling a court to hear civil proceedings about serious or repeated harmful digital communications. The court does not issue fines or prison terms, but can order certain remedies. Failure to comply with these orders is punishable by up to six months' imprisonment or a fine of $5,000 for individuals or $20,000 for companies. The court is able '…to order a broad range of remedies…', which include:
  - orders to take down material;
  - cease-and-desist orders;
  - orders to publish a correction or an apology, or to give the complainant a right of reply;
  - orders to release the identity of the source of an anonymous communication, and
  - ordering name suppression for any parties.[54]
- Limiting the liability of telecommunications companies and social media platforms for harmful content posted by others, as long as those companies follow a certain procedure for users' complaints.
- Making it a criminal offence to incite someone to commit suicide, regardless of whether or not the person attempts suicide (previously, it was only an offence if the person attempted or committed suicide). The offence is punishable by up to three years' imprisonment.

1.43 During his second reading speech on the bills that established the Australian eSafety Commissioner, the then Parliamentary Secretary to the Minister for

52 New Zealand Ministry of Justice, 'Key parts of the Act', 2 October 2017, https://www.justice.govt.nz/justice-sector-policy/key-initiatives/harmful-digital-communications/key-parts-of-the-act/ (accessed 19 March 2018).

53 *Harmful Digital Communications Act 2015* (New Zealand), subsection 22(1).

54 New Zealand Ministry of Justice, 'Key parts of the Act', 2 October 2017, https://www.justice.govt.nz/justice-sector-policy/key-initiatives/harmful-digital-communications/key-parts-of-the-act/ (accessed 19 March 2018).

Communications, the Hon. Paul Fletcher MP, referred to various elements of the Harmful Communications Act that had been considered.[55]

Network Enforcement Law in Germany

1.44 The Netzwerkdurchsetzungsgesetz (also known as NetzDG or Network Enforcement Law) places various obligations on social media platforms in Germany. It was passed in June 2017 and came into force in early October 2017, although there was a transition period until 1 January 2018.[56]

1.45 The Network Enforcement Law applies to social media platforms that have over two million registered users in Germany.[57] It requires the platforms to block or remove access to:

- 'manifestly unlawful content' within 24 hours of receiving a complaint, and
- 'unlawful content' within seven days of receiving a complaint.[58]

1.46 The meaning of 'unlawful content' is limited to content that contravenes certain enumerated criminal offences. These offences include those relating to hate speech, inciting others to violence or crime, terrorist offences, glorifying violence, defamation, insult, and child pornography.[59]

1.47 The Network Enforcement Law also requires social media platforms to:

- maintain an effective procedure for users to make complaints about content;[60]
- publish half-yearly reports providing certain specified data relating to the implementation of the law,[61] and
- name and authorise a person to receive service in Germany.[62]

---

55 The Hon. Paul Fletcher MP, Parliamentary Secretary to the Minister for Communications, *House of Representatives Hansard*, 3 December 2014, p. 14039.

56 'Germany starts enforcing hate speech law', *BBC News*, 1 January 2018, http://www.bbc.com/news/technology-42510868 (accessed 19 March 2018).

57 Network Enforcement Act (English translation), subsection 1(1), https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2 (accessed 19 March 2018).

58 Network Enforcement Act (English translation), subsection 3(2), https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2 (accessed 19 March 2018).

59 Network Enforcement Act (English translation), subsection 1(3), https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2 (accessed 19 March 2018).

60 Network Enforcement Act (English translation), subsections 2(1) and (2), https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2 (accessed 19 March 2018).

61 Network Enforcement Act (English translation), subsection 1(1), https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2 (accessed 19 March 2018).

1.48 Failing to meet the requirements of the Network Enforcement Law can result in fines of up to 50 million euros.[63]

USA Communications Decency Act 1996

1.49 The eSafety Commissioner explained that legislation in the United States of America '…has given the social media sites what is called intermediary liability—what I believe some of them now call intermediary immunity—which says that they're not responsible for anything that users do on their platform.'[64] This is under the *Communications Decency Act 1996*, of which subsection 230(c)(1) states that:

> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.[65]

Note on references

1.50 In this report, references to *Committee Hansard* are to proof transcripts. Page numbers may vary between proof and official transcripts.

62 Network Enforcement Act (English translation), section 5, https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__blob=publicationFile&v=2 (accessed 19 March 2018).

63 Ben Knight, 'Germany implements new internet hate speech crackdown', *Deutsche Welle*, 1 January 2018, http://www.dw.com/en/germany-implements-new-internet-hate-speech-crackdown/a-41991590 (accessed 19 March 2018); Philip Oltermann, 'Tough new German law puts tech firms and free speech in spotlight', *The Guardian*, 5 January 2018, https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight (accessed 19 March 2018).

64 Ms Inman Grant, eSafety Commissioner, *Committee Hansard*, 9 February 2018, p. 71.

65 *Communications Decency Act 1996* (USA), Subsection 230(c)(1), in eSafety Office, answers to questions on notice, 9 February 2018 (received 7 March 2018), p. 3.