12. Prohibiting Content

Contents

Summary

12.1 This chapter is about prohibitions on the distribution of Prohibited content. 'Prohibited' is the term that the ALRC recommends should replace the existing 'Refused Classification' (RC) category to describe content that is essentially 'banned' in Australia. The scope of this category is discussed in Chapter 11.

12.2 Although media regulation in Australia has seen a significant shift from censorship to classification, there remains content that is illegal to distribute. The new National Classification Scheme should continue to provide for the identification of this content, and allow for various means of prohibiting its distribution.

12.3 The ALRC recommends that the Classification of Media Content Act should provide that content providers must not sell, screen, provide online, or otherwise distribute Prohibited content. Content providers will therefore need to identify, or take reasonable steps to identify, Prohibited content.

12.4 This chapter also discusses when Prohibited content should be classified for the purpose of enforcing these prohibitions. The ALRC recommends that, generally, the content should be classified by the Classification Board before the Regulator or other law enforcement body takes enforcement action. However, the Classification of Media Content Act should enable the Regulator to notify Australian or international law enforcement agencies or bodies about Prohibited content without having the content first classified by the Classification Board.

12.5 Finally, the chapter outlines the main methods of restricting access to Prohibited content, namely: prohibitions on sale and distribution; prohibitions on import and export; prohibitions on publication online; and voluntary and mandatory internet filtering. The Classification of Media Content Act, or industry codes made under it, should provide for similar methods of prohibiting the distribution of Prohibited content.

The obligation

12.6 The ALRC recommends that the Classification of Media Content Act should provide that content providers must not sell, screen, provide online, or otherwise distribute Prohibited content. Prohibited content here refers to:

(a) content that has been classified Prohibited; or

(b) unclassified content that, if classified, would be likely to be classified Prohibited.

12.7 Under the *Broadcasting Services Act 1992* (Cth), 'prohibited content' has a much broader meaning, and captures X 18+ content, Category 1 and 2 Restricted content, and R 18+ and MA 15+ content that has not been properly restricted. The need for a single definition of Prohibited content that excludes content classified, or likely to be classified, MA 15+, R 18+ or X 18+, is discussed in Chapter 11.

12.8 Some elements of the obligation not to distribute Prohibited content are similar to the obligation to take reasonable steps to restrict access to adult content, discussed in Chapter 10. As with the latter obligation, the obligation not to distribute Prohibited content should apply to both commercial and non-commercial content. Also, although there are exemptions from classification requirements in other classification categories, there should not be similar exemptions from the obligation not to distribute Prohibited content.

12.9 The obligation not to distribute Prohibited content applies to unclassified content that is 'likely' to be Prohibited. While some stakeholders have expressed concern about provisions referring to the 'likely' classification of content,[1] similar language is used in the *Broadcasting Services Act*.[2] In the ALRC's view, the obligation not to distribute certain content should extend to unclassified content that is likely to be Prohibited, otherwise the obligation would only apply to the relatively small proportion of total media content that in practice is actually classified. As Prohibited content is to be illegal to distribute, there must be provision for enforcement of guidelines.

How to identify Prohibited content

12.10 Ideally, content providers should assess whether content is likely to be Prohibited before they distribute it. In light of the serious nature of this content, many

1 Eg, Foxtel, *Submission CI 2497*; Classification Board, *Submission CI 2485*.
2 *Broadcasting Services Act 1992* (Cth) sch 7 cl 21(1)(b).

content providers may even choose to have their content classified before distributing it, to determine whether it is Prohibited.[3]

12.11 However, this may be impractical or impossible for online content providers that deal with large quantities of content, much of which is dynamic and user-generated. Requiring 'pre-assessment' would be almost as onerous as requiring all content that 'may' be Prohibited to be classified, which the ALRC has concluded is impractical and prohibitively costly.

12.12 In the ALRC Discussion Paper, it was proposed that the Classification of Media Content Act should provide that all media content that may be RC must be classified by the Classification Board.[4] While some stakeholders supported this,[5] others were critical of the proposal. Some raised concerns about the huge quantity of media content that 'may' be RC.[6] One stakeholder submitted that it is

> impossible for anyone to know what would in fact be 'RC' under current broad and vague criteria; and the result is likely to be unnecessary self-censorship due to fear of being prosecuted for failure to have material classified.[7]

12.13 A number of stakeholders expressed the view that this sort of classification obligation would impose a considerable burden on content providers, many of whom will be unwilling or unable to comply.[8] Some expressed particular concern about the burden on non-commercial content providers, including individuals.[9] Google stated that, in light of the volume of online content,

> content platforms have no practical means of determining whether content is or is likely to be … RC in advance of the content being uploaded. … The only feasible approach to regulating this content is for content platforms to rely on users to notify them of content that may fall foul of the site's standards in order that this content can be reviewed and removed if considered appropriate.[10]

12.14 The Interactive Games and Entertainment Association submitted that it was critical that the new scheme clearly address the issue of intermediaries providing large quantities of content and the steps that must be taken to avoid liability for inadvertently providing Prohibited content:

---

3 In which case they could have the content classified by an accredited industry classifier, the Classification Board or using an authorised classification instrument. See Ch 7.

4 Australian Law Reform Commission, *National Classification Scheme Review*, ALRC Discussion Paper 77 (2011), Proposals 6–5 and 7–1(c).

5 Eg, FamilyVoice Australia, *Submission CI 2509*; Communications Law Centre, *Submission CI 2484*; N Goiran, *Submission CI 2482*; Collective Shout, *Submission CI 2477*; D Henselin, *Submission CI 2473*; Telstra, *Submission CI 2469*; R Harvey, *Submission CI 2467*; D Mitchell, *Submission CI 2461*; M Smith, *Submission CI 2456*; L D, *Submission CI 2454*.

6 I Graham, *Submission CI 2507*; J Denham, *Submission CI 2464*.

7 I Graham, *Submission CI 2507*.

8 Eg, Google, *Submission CI 2512*; J Trevaskis, *Submission CI 2493*; Australian Communications and Media Authority, *Submission CI 2489*; Interactive Games and Entertainment Association, *Submission CI 2470*.

9 A Hightower, *Submission CI 2511*; I Graham, *Submission CI 2507*; J Denham, *Submission CI 2464*.

10 Google, *Submission CI 2512*.

> While the actual steps might be set out in industry codes, the Classification of Media Content Act should not be silent on the issue.[11]

12.15 Others said it would be difficult or impractical to enforce such laws.[12] For example, the Australian Communications and Media Authority (the ACMA) stated it 'is likely to lead to a low regard for such a law and, as a consequence, a significantly diminished culture of compliance'.[13]

12.16 The ALRC agrees that it is unreasonable to expect content providers to have all of their content that 'may be' Prohibited classified before they distribute it. As discussed in Chapter 10 with respect to adult content, the effective regulation of media content online cannot rely on pre-screening or pre-classification. Such a model would not account for the sheer quantity of media content that is now available online, and in particular, the dynamic nature of online content and the volume of user-generated content.

12.17 Instead, the obligation not to distribute Prohibited content should require content providers to take reasonable steps to identify Prohibited content. Major content providers, for example, might have mechanisms that allow users to flag particular content to the owners of the site.

Who is the subject of the obligation?

12.18 The obligation not to distribute Prohibited content applies to a broader range of persons than the other statutory obligations discussed in this Report. In Chapter 5, the ALRC recommends that obligations in relation to Prohibited content should apply to content providers and internet intermediaries, including application service providers, host providers and internet access providers.[14] In the ALRC's view, obligations in relation to Prohibited content should—considering the serious nature of the content—be broad in application and apply to all content providers, commercial and non-commercial, and to internet intermediaries who do not otherwise have obligations to classify or restrict access to content.

12.19 As explained in Chapter 5, where Prohibited content is uploaded onto a website by an individual, that individual may commit an offence under the Classification of Media Content Act. The website owner would be under an obligation to take down the content when notified by the Regulator. Other internet intermediaries may have obligations to respond to notices from the Regulator with respect to the content. In the future, an internet service provider (ISP) may have an obligation to filter the content, particularly where the website owner is located overseas.

12.20 The obligation not to distribute Prohibited content would also apply to distributors in the 'offline' world, including broadcasters, retailers, and magazine and DVD distributors.

---

11 Interactive Games and Entertainment Association, *Submission CI 2470*.

12 Google, *Submission CI 2512*; Australian Communications and Media Authority, *Submission CI 2489*; J Denham, *Submission CI 2464*.

13 Australian Communications and Media Authority, *Submission CI 2489*.

14 Rec 5–7.

Recommendation 12–1 The Classification of Media Content Act should provide that content providers must not sell, screen, provide online, or otherwise distribute Prohibited content, that is:

(a) content that has been classified Prohibited; or

(b) unclassified content that, if classified, would be likely to be classified Prohibited.

Classifying before enforcement

12.21 The ALRC recommends that the Classification of Media Content Act should provide that content must be classified Prohibited by the Classification Board before a person is:

(a) charged with an offence under the Act that relates to Prohibited content; and

(b) issued a notice requiring the person to stop distributing the Prohibited content, for example by taking it down from the internet.

12.22 This provision would apply to Prohibited media content distributed on any platform or device, including offences for distributing hardcopy Prohibited content.

12.23 Similar requirements proposed in the Discussion Paper[15] were supported by a number of stakeholders.[16] Telstra said it favoured 'all measures that improve the transparency and accountability of this process'.[17] The New South Wales Council for Civil Liberties 'applauded' the proposal, because to 'provide otherwise is, in effect, to permit retrospective criminalisation'.[18] The Council also considered it important 'that law enforcement officers are not involved in decisions about what is to be censored'.[19]

12.24 The Victorian Government commented that, currently, 'enforcement bodies are required to request classification decisions (or proof of classification in the form of evidentiary certificates) for materials to establish breaches'.[20]

12.25 The main concern raised in submissions was that the proposal may unwittingly have a negative impact on the law enforcement response to child sexual abuse content.

---

15 Australian Law Reform Commission, *National Classification Scheme Review*, ALRC Discussion Paper 77 (2011), Proposal 6–6.

16 Eg, FamilyVoice Australia, *Submission CI 2509*; Collective Shout, *Submission CI 2477*; D Henselin, *Submission CI 2473*; National Association for the Visual Arts, *Submission CI 2471*; Interactive Games and Entertainment Association, *Submission CI 2470*; Telstra, *Submission CI 2469*.

17 Telstra, *Submission CI 2469*.

18 New South Wales Council for Civil Liberties, *Submission CI 2481*. See also R Harvey, *Submission CI 2467*.

19 New South Wales Council for Civil Liberties, *Submission CI 2481*.

20 Victorian Government, *Submission CI 2526*.

Some submissions raised a concern that the proposal could hamper enforcement, if the Classification Board could not classify the content promptly.[21]

12.26 The Justice and International Mission Unit of the Uniting Church in Australia also submitted that the 'dynamic nature' of online content had to be factored into the process.[22] This Unit of the Uniting Church was concerned that there may be 'a significant delay' in being able to deal with 'child sexual abuse material' if all RC content could only be classified by the Classification Board, as child sexual abuse images are now typically hosted for a matter of days.[23] It submitted that if the Classification Board was not resourced to classify child sexual abuse content in under a day, then 'other regulatory bodies and their officers, such as the ACMA, should be permitted to classify child sexual abuse material'.[24]

12.27 Civil Liberties Australia stated that, before content is added to any proposed list of content that must be filtered at the ISP-level,

> there needs to be an additional step requiring Australian law enforcement to exhaust all steps to have the content destroyed by at least contacting the hosting company or local law enforcement in the event Australia is not the country of origin.[25]

12.28 The Hon Nick Goiran MLC submitted that it is 'important that in the interim period of applying for a classification that the Regulator have power to prevent further distribution of material which is likely to be classified RC'.[26]

12.29 While the ACMA was of the view that classification by the Classification Board would be time-critical, it submitted that the proposal

> could work, provided that the dynamic nature of such content is taken into account (for example by capturing a copy of the content and identifying its source as soon as possible) and that such classifications could be done quickly (ideally within two business days) and not involve too much by way of double handling by the regulator and Classification Board.[27]

12.30 It was submitted that the Regulator or other law enforcement agency should be empowered to take certain action in the interim period.[28] The ACMA stated that it was appropriate to have provision for 'interim take-down notices' to be issued by qualified staff for 'potential prohibited content' to avoid problems if there is delay in the Classification Board's classification.[29]

---

21 Uniting Church in Australia, *Submission CI 2504*; Australian Communications and Media Authority, *Submission CI 2489*.
22 Uniting Church in Australia, *Submission CI 2504*. See also, Australian Communications and Media Authority, *Submission CI 2489*.
23 Uniting Church in Australia, *Submission CI 2504*.
24 Ibid.
25 Civil Liberties Australia, *Submission CI 2466*.
26 N Goiran, *Submission CI 2482*.
27 Australian Communications and Media Authority, *Submission CI 2489*.
28 Ibid; N Goiran, *Submission CI 2482*.
29 Australian Communications and Media Authority, *Submission CI 2489*.

12.31 If the Australian Government were to implement a mandatory ISP-level filtering scheme, as has been proposed, then content should also generally be classified Prohibited before ISPs are required to block or filter it. The ALRC made a similar proposal in the Discussion Paper.[30] Proposed accountability and transparency measures, outlined later in this chapter, also provide for the classification of some content before being added to the proposed list of content that must be filtered.

Recommendation 12–2 The Classification of Media Content Act should provide that content must be classified Prohibited by the Classification Board before a person is:

(a) charged with an offence under the Act that relates to Prohibited content; and

(b) issued a notice requiring the person to stop distributing the Prohibited content, for example by taking it down from the internet.

Recommendation 12–3 The Classification of Media Content Act should enable the Regulator to notify Australian or international law enforcement agencies or bodies about Prohibited content without having the content first classified by the Classification Board.

Prohibitions offline

12.32 The balance of this chapter outlines the existing mechanisms for preventing the distribution of RC content—first 'offline' and then 'online'. The Classification of Media Content Act should provide for similar methods for preventing the distribution of Prohibited content. The methods of preventing distribution offline are less contested than the methods used to control online Prohibited content.

Distributing and broadcasting

12.33 State and territory enforcement legislation proscribes certain dealings with RC content—such as selling, publicly exhibiting or possessing with an intention to sell. The ALRC recommends that the Classification of Media Content Act likewise prohibit the sale, distribution and exhibition of Prohibited content. The Classification of Media Content Act should, however, clarify that this also applies to online Prohibited content.

12.34 Similarly, the *Broadcasting Services Act* provides that the codes developed by television industry groups encompass such matters as 'preventing the broadcasting of programs that, in accordance with community standards, are not suitable to be broadcast'.[31] As stated above, the ALRC recommends that the Classification of Media Content Act should provide that content providers must not screen Prohibited content (whether so classified or likely to be so classified).

30 Australian Law Reform Commission, *National Classification Scheme Review*, ALRC Discussion Paper 77 (2011), Proposal 6–6.

31 *Broadcasting Services Act 1992* (Cth) s 123(2)(a).

12.35 In Western Australia and prescribed areas of the Northern Territory, it is illegal to possess RC content.[32] The ALRC makes no recommendation about the possession of Prohibited content.

Importing and exporting

12.36 Customs regulations currently prohibit the importation and exportation of 'objectionable goods'.[33] The Australian Customs and Border Protection Service (Customs) is empowered to identify and confiscate such objectionable goods at Australia's borders.

12.37 While the provisions relating to 'objectionable goods' do not explicitly refer to RC content, the Australian Government's intention was to align the scope of 'objectionable goods' with the RC category.[34] Customs has advised that if the scope of the RC category were changed, 'equivalent amendments are required to the [import regulations] to ensure that the controls at the border are consistent with the domestic controls'.[35]

12.38 The ALRC agrees that if the Australian Government narrows the scope of the new Prohibited classification category, as is recommended in Chapter 11, then it should also review the scope of 'objectionable goods' under the import and export regulations.

Prohibitions online

12.39 This section outlines the existing methods employed to address RC content online. The Classification of Media Content Act should provide for similar methods of stopping the distribution of Prohibited content.

12.40 The ACMA is required to investigate complaints made about online content defined as 'prohibited content' under the *Broadcasting Services Act*. As has been explained, the definition of 'prohibited content' in the *Broadcasting Services Act* captures a wider range of content than RC—although RC content is certainly captured.[36] The ACMA may also choose to investigate a matter on its own initiative.[37]

---

32 *Classification (Publications, Films and Computer Games) Act 1995* (Cth) ss 102, 103; *Classification (Publications, Films and Computer Games) Enforcement Act 1996* (WA) ss 62, 81, 89. State and territory offences under the classification cooperative scheme more generally are discussed in Ch 16.

33 *Customs (Prohibited Imports) Regulations 1956* (Cth) reg 4A; *Customs (Prohibited Exports) Regulations 1958* (Cth) reg 3.

34 Explanatory Statement, Customs (Prohibited Imports) Amendment Regulations 2007 (No 5) (Cth), 1; Explanatory Statement, Customs (Prohibited Exports) Amendment Regulations 2007 (No 4) (Cth), 1; Explanatory Statement, Customs (Prohibited Exports) Regulations (Amendment) 1997 (Cth), 1; Explanatory Statement, Customs (Prohibited Imports) Regulations (Amendment) 1995 (Cth), 1.

35 Australian Customs and Border Protection Service, *Submission to Senate Legal and Constitutional Affairs References Committee Inquiry into the Australian Film and Literature Classification Scheme*, 25 February 2011.

36 *Broadcasting Services Act 1992* (Cth) sch 7 cls 20, 21.

37 Ibid sch 5 cl 27; sch 7 cl 44.

12.41 The ACMA's trained content assessors then investigate the complaint. The action that the ACMA must then take depends, among other things, on whether the content is hosted in Australia.

Take-down notices

12.42 Currently, if the ACMA assesses that content is substantially likely to be 'potential prohibited content' and the content is hosted by a 'hosting service',[38] or provided by way of a 'live content service',[39] or by a 'links service'[40] with the appropriate Australian connection, then the ACMA must:

- issue an interim notice directing that certain steps be taken (broadly, that the content be taken down or removed); and
- apply to the Classification Board for classification of the content.[41]

12.43 The content must generally be taken down by 6 pm the next business day.[42] If the content is then classified RC, the ACMA issues a final take-down notice.[43] The requirement to comply with these interim and final take-down notices constitute 'designated content/hosting service provider rules',[44] so non-compliance may result in the commission of an offence[45] or the contravention of a civil penalty provision.[46]

12.44 The notice and take-down scheme has significantly reduced the amount of child sexual abuse online content hosted in Australia.[47] The ACMA reports that it has received '100% industry compliance' with its actions to remove such content.[48]

12.45 However, as the Internet Industry Association (IIA) has explained, for 'both technical and legal reasons, take-down notices can only apply in relation to content hosted in Australia'.[49]

Notifying law enforcement agencies

12.46 The ACMA has obligations in respect of 'sufficiently serious' online content, which has been the subject of complaint, regardless of whether the content is hosted in Australia or overseas. The ACMA considers the following online content 'sufficiently serious':

---

38 Defined in Ibid sch 7 cl 4.
39 Defined in Ibid sch 7 cl 2.
40 Defined in Ibid sch 7 cl 2.
41 Ibid sch 7 cl 47(2), 56(2), cl 62(2).
42 Ibid sch 7 cl 53(1), 60(1), 68(1).
43 Ibid sch 7 cl 47(1), 56(1), 62(1).
44 Ibid sch 7 cl 53(6), 60(4), 68(6).
45 Ibid sch 7 cl 106.
46 Ibid sch 7 cl 107.
47 W Wei, *Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System* (2011), 81.
48 Australian Communications and Media Authority, *The ACMA Hotline—Combating Online Child Sexual Abuse* <http://www.acma.gov.au/WEB/STANDARD/pc=PC_90103> at 23 August 2011.
49 Internet Industry Association, *Guide for Internet Users: Information about Online Content* (Updated 2011), 8.

- 'child abuse material';
- content that advocates the doing of a terrorist act; and
- content that promotes or incites crime or violence.[50]

12.47 This content 'mirrors' some of the content currently within the scope of the RC classification category. Some of this content comes within the ambit of some offences in the *Criminal Code* (Cth), so may be broadly understood as 'illegal content'.

12.48 The ACMA is obliged to refer online content that it considers to be 'sufficiently serious' to a member of an Australian police force or, where there is an arrangement in place with the chief of an Australian police force that the ACMA may notify the content to another person or body, to that other person or body.[51]

12.49 There is a Memorandum of Understanding in place between the ACMA and Commonwealth, state and territory police forces to ensure the swift reporting of such content[52] and associated information sharing.[53]

12.50 The ACMA has an arrangement with the Australian Federal Police (AFP) that online child abuse material that is hosted by a country which has membership with the International Association of Internet Hotlines (INHOPE) may be referred directly to INHOPE.[54] If the relevant jurisdiction is not an INHOPE member, then the ACMA refers the content to enforcement agencies such as the AFP[55] who in turn will liaise with international law enforcement agencies such as INTERPOL.

12.51 The ACMA refers online content that advocates the doing of a terrorist act to the AFP.[56]

Family friendly filters

12.52 If the ACMA is satisfied that content hosted outside Australia is prohibited content or potential prohibited content, as defined in the *Broadcasting Services Act*, the ACMA must, among other things,

> notify the content to internet service providers so that the internet service providers can deal with the content in accordance with procedures specified in an industry code or industry standard.[57]

---

50 Australian Communications and Media Authority, *Regulating Online Content: The ACMA's Role* (2011), 3.

51 *Broadcasting Services Act 1992* (Cth) sch 5 cl 40(1)(a) (content hosted offshore); sch 7 cl 69(1) (Australian-hosted content).

52 Australian Communications and Media Authority, *Regulating Online Content: The ACMA's Role* (2011), 3.

53 W Wei, *Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System* (2011), 47.

54 Australian Communications and Media Authority, *Working Together to Fight Online Child Abuse Material* <http://www.acma.gov.au/scripts/nc.dll?WEB/STANDARD/1001/pc=PC_90166> at 11 September 2011.

55 Australian Communications and Media Authority, *Regulating Online Content: The ACMA's Role* (2011), 3.

56 Ibid, 3.

57 *Broadcasting Services Act 1992* (Cth) sch 5 cl 2(b).

12.53 The ACMA notifies filter software makers or suppliers accredited by the IIA in accordance with the industry code in place under sch 5 of the *Broadcasting Services Act*.[58] To be designated an 'IIA Family Friendly Filter', the IIA must be satisfied that the internet filtering product or service meets certain requirements.[59]

12.54 The ACMA informs the filter software providers of the URLs that are to be excluded or 'blocked'. This list is known as the 'ACMA blacklist'.[60] The makers or suppliers of the 'Family Friendly' filtering products or services have agreed to give effect to the ACMA's notifications by updating their products or services. The ACMA regularly reviews the URLs on its blacklist, and provides filter providers with revised lists.

12.55 Australian-based ISPs then make these 'Family Friendly' filters available to their customers free of charge or on a cost recovery basis.[61] Australian internet users have a choice as to whether or not they opt to use these filters.[62] If an Australian internet user has opted to use one of these filters, the blocking then occurs at the user's end—namely on the user's computer—rather than at a network level.

12.56 Schedules 5 and 7 of the *Broadcasting Services Act* are silent about whether the ACMA may also notify 'Family Friendly' filter software makers and providers of URLs which have been determined to contain child sexual abuse content by overseas organisations such as the Internet Watch Foundation, INTERPOL, and the National Center for Missing and Exploited Children—that is, online content that may not have been the subject of complaint under the *Broadcasting Services Act* framework. These overseas organisations, and the criteria used to determine whether content should be included on their lists, are discussed in a later section of this chapter.

ISP-level filtering

12.57 The Australian Government has proposed a scheme for mandatory filtering of certain online content by ISPs. Voluntary filtering is also being undertaken by some Australian ISPs. A number of stakeholders commented on ISP-level filtering.

Mandatory filtering

12.58 In December 2009, the Australian Government announced that it planned to introduce legislative amendments to the *Broadcasting Services Act* to require all ISPs in Australia to filter or 'block' RC content hosted on overseas servers. The 'RC Content List' is to comprise:

---

58 Ibid, sch 5 cl 40.

59 Internet Industry Association, *Internet Industry Codes of Practice: Codes for Industry Co-regulation in Areas of Internet and Mobile Content* (2005), 23.

60 Department of Broadband, Communications and the Digital Economy, *Mandatory Internet Service Provider (ISP) Filtering: Measures to Increase Accountability and Transparency for Refused Classification Material–Consultation Paper* (2009), 3.

61 Internet Industry Association, *Internet Industry Codes of Practice: Codes for Industry Co-regulation in Areas of Internet and Mobile Content* (2005), 21.

62 Internet Industry Association, *Guide for Internet Users: Information about Online Content* (Updated 2011), 4.

- overseas-hosted online content which has been subject to complaint to the ACMA and which is being classified, or has been classified as RC, by the Classification Board using the classification scheme criteria; and
- international lists of overseas-hosted child sexual abuse material from 'highly-reputable' overseas agencies—following the ACMA's detailed 'assessment of the rigour and accountability of classification processes used by these agencies'.[63]

12.59 The scheme is intended to help reduce the risk of inadvertent exposure to RC content, particularly by children, and reduce the current inconsistency between the treatment of RC content that is hosted in Australia (which is subject to the notice and take-down scheme) and that hosted overseas.[64]

12.60 The Government announced nine measures to increase accountability and transparency in relation to the scheme.[65] These include measures to ensure some content must be classified by the Classification Board before the content is added to the 'RC Content List', and that aggrieved persons may seek review of these decisions.[66] It was also proposed that the ACMA would regularly publish an up-to-date, high-level breakdown of the list by category, and that an independent expert would undertake an annual review of the processes.[67]

12.61 An exemption is being considered for popular overseas sites with high traffic, such as YouTube, if the owners of the sites implement their own systems either to take down RC content or to block Australian access.[68]

12.62 A number of stakeholders expressed views on mandatory ISP-level filtering, with some supporting the policy,[69] and others expressing opposition.[70] Supporting mandatory filtering, the Communications Law Centre submitted that:

> A list of all material that has been refused classification should be published, with broad category descriptors explaining why the media content has been refused

---

63 S Conroy (Minister for Broadband, Communications and the Digital Economy), 'Measures to Improve Safety of the Internet for Families' (Press Release, 15 December 2009).

64 Department of Broadband, Communications and the Digital Economy, *ISP Filtering—Frequently Asked Questions* <www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering/isp_filtering_live_pilot/isp_filtering_-_frequently_asked_questions> at 16 February 2012.

65 Department of Broadband, Communications and the Digital Economy, *Outcome of Public Consultation on Measures to Increase Accountability and Transparency for Refused Classification Material* (2010).

66 Ibid, Measures 1 and 5.

67 Ibid, Measures 4 and 7.

68 Department of Broadband, Communications and the Digital Economy, *ISP Filtering—Frequently Asked Questions* <www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering/isp_filtering_live_pilot/isp_filtering_-_frequently_asked_questions> at 16 February 2012.

69 Eg, FamilyVoice Australia, *Submission CI 2509*; Australian Christian Lobby, *Submission CI 2500*; Communications Law Centre, *Submission CI 2484*; Bravehearts Inc, *Submission CI 1175*.

70 A Hightower, *Submission CI 2511*; I Graham, *Submission CI 2507*; Confidential, *Submission CI 2503*; Confidential, *Submission CI 2496*; Arts Law Centre of Australia, *Submission CI 2490*; National Association for the Visual Arts, *Submission CI 2471*; R Harvey, *Submission CI 2467*; D Mitchell, *Submission CI 2461*.

> classification (eg 'sexual violence'). Such media content should be compulsorily filtered at the ISP level.[71]

12.63 The Australian Christian Lobby likewise said that, 'despite the limitations and challenges of ISP filtering, there are a range of studies demonstrating that it would be an effective way of filtering Refused Classification material'.[72]

12.64 Among the reasons that were given for opposing mandatory ISP-level filtering were concerns about:

- there being very little child sexual abuse content on the web, because this content is more prevalent in peer-to-peer file sharing and virtual private networks, which will not be filtered;[73]
- the filter not being effective because it can be by-passed;[74]
- the potential cost of the scheme given these limitations;[75]
- the filter may be giving a false sense of protection to households;[76]
- the filter being counterproductive in terms of finding and prosecuting those distributing and/or accessing child sexual abuse content;[77]
- a government list of websites to be filtered being secret,[78] open to abuse[79] (including 'scope creep'—more categories of content being added over time), and infringing freedom of speech;[80] and
- the potential for over-blocking (that is, content being filtered that should not be filtered, such as creative/artistic works and information).[81]

Identifying content to be blocked

12.65 If ISPs were required mandatorily to filter all Prohibited or RC content, it is likely that certain content would have to be prioritised—and perhaps only a subcategory of Prohibited content would in fact be filtered. For example, the ACMA has recently reported that, of the 1,957 items of prohibited or potentially prohibited

---

71 Communications Law Centre, *Submission CI 2484*.
72 Australian Christian Lobby, *Submission CI 2500*.
73 Eg, L Mancell, *Submission CI 2492*; R Harvey, *Submission CI 2467*; Civil Liberties Australia, *Submission CI 2466*; D Mitchell, *Submission CI 2461*.
74 Eg, Confidential, *Submission CI 2503*; A Ameri, *Submission CI 2491*; Civil Liberties Australia, *Submission CI 2466*; J Denham, *Submission CI 2464*; Electronic Frontier Foundation, *Submission CI 1174*.
75 Eg, A Ameri, *Submission CI 2491*; D Mitchell, *Submission CI 2461*; Electronic Frontier Foundation, *Submission CI 1174*.
76 Eg, L Mancell, *Submission CI 2492*; K Weatherall, *Submission CI 2155*.
77 Eg, Confidential, *Submission CI 2503*.
78 Eg, A Hightower, *Submission CI 2511*; I Graham, *Submission CI 2507*.
79 Eg, Confidential, *Submission CI 2503*; Confidential, *Submission CI 2496*; R Harvey, *Submission CI 2467*; Civil Liberties Australia, *Submission CI 2466*; J Denham, *Submission CI 2464*.
80 Eg, Lin, *Submission CI 2476*; Electronic Frontier Foundation, *Submission CI 1174*.
81 Eg, Arts Law Centre of Australia, *Submission CI 2490*; National Association for the Visual Arts, *Submission CI 2471*; K Weatherall, *Submission CI 2155*.

content it identified in 2010–11, 1,054 items were determined to be offensive depictions of children, whereas only 68 items depicting a sexual fetish were determined to be RC content.[82]

12.66 In the Discussion Paper, the ALRC proposed that the Classification of Media Content Act should provide that, if content is classified RC, the classification decision should state whether the content comprises real depictions of actual child sexual abuse or actual sexual violence. This content, the ALRC stated, could then be added to any blacklist of content that must be filtered at the ISP level, should such a policy be implemented.[83]

12.67 Some submissions supported the proposal.[84] For example, Telstra stated that it would be a 'feasible and practical' approach to implement and could 'usefully form one element of a multi-faceted approach to this issue'.[85] However, others expressed concern that this would narrow the scope of what must be filtered. The Australian Council on Children and the Media, for example, said that 'any material that is judged to be RC should be on the blacklist', and particularly noted material 'that incites or instructs in matters of crime or violence (especially terrorism)'.[86] Similarly, Collective Shout submitted that the RC classification should be broadened to include 'any depiction of actual sex' and material that 'promotes, encourages or instructs in methods of suicide'.[87]

12.68 In contrast, Civil Liberties Australia, stated that:

> If the ALRC were prepared to suggest that the only content that could not be contained in the other classification categories is real depictions of actual child sexual abuse or actual sexual violence, then that would be a very strong step forward.[88]

12.69 Some submissions queried the distinction between 'actual' abuse and simulations of abuse. For example, Amy Hightower argued that, while the definition of 'child pornography material' in the *Criminal Code* (Cth)

> clearly captures abhorrent 'real' child sexual abuse material as intended, it also captures material which does not actually involve children at all, including cartoons, textual works or material where all involved parties are demonstrably over the age of eighteen. There is no legal distinction drawn between 'real' and 'fictional' abuse; to draw such a distinction would presumably require altering the *Criminal Code*.[89]

---

82 Australian Communications and Media Authority, *Annual Report 2010–11* (2011), 112–113.

83 Australian Law Reform Commission, *National Classification Scheme Review*, ALRC Discussion Paper 77 (2011), Proposal 10–1.

84 Eg, Uniting Church in Australia, *Submission CI 2504*; Arts Law Centre of Australia, *Submission CI 2490*; Telstra, *Submission CI 2469*.

85 Telstra, *Submission CI 2469*.

86 Australian Council on Children and the Media, *Submission CI 2495*.

87 Collective Shout, *Submission CI 2477*.

88 Civil Liberties Australia, *Submission CI 2466*.

89 A Hightower, *Submission CI 2511*.

12.70 The Justice and International Mission Unit of the Uniting Church submitted that it would like the proposal to be broadened to include simulated depictions of actual child sexual abuse.[90] Others also called for a clear definition of 'actual sexual violence'.[91]

12.71 Given the volume of Prohibited content on the internet, if ISPs were required mandatorily to filter Prohibited content, the Regulator may recommend that particular subcategories of Prohibited content will be prioritised. The selection of such subcategories should be carefully assessed. The ALRC notes in particular the community concerns about actual child sexual abuse and non-consensual sexual violence. In defining such a subcategory, the Regulator might also have regard to the types of content that are now the focus of international efforts to curb the distribution of child abuse material. The subcategory of 'sufficiently serious content', discussed above, might also be useful for this purpose.

Voluntary filtering

12.72 In early July 2010, the Australian Government announced that some Australian ISPs have agreed voluntarily to block, at the ISP level, a list of child abuse URLs.[92] The IIA then announced that it would develop a voluntary industry code for ISPs to block 'child pornography' websites.[93] On 27 June 2011, the IIA released the framework that would underpin its voluntary code.[94] A key feature of the voluntary scheme is that it uses INTERPOL's list rather than a list maintained by the ACMA, or any other organisation. The criteria for inclusion in the INTERPOL list are stricter than the definition of child pornography material under Australian criminal legislation.[95]

12.73 To join the IIA's voluntary code of practice, an ISP expresses interest in participation to the AFP and indicates that they have, or are preparing, their technical infrastructure to implement blocking of the list. The AFP then issues a 'request' to that ISP pursuant to s 313 of the *Telecommunications Act 1997* (Cth). This statutory provision outlines the obligations of 'carriers' and 'carriage service providers' to do their best to prevent relevant telecommunications networks and facilities from being used in, or in relation to, the commission of Commonwealth, state or territory offences and to give officers and authorities of the Commonwealth and of the states and territories such help as is reasonably necessary for the purpose of enforcing the criminal law, amongst other things. Section 313(5) of the *Telecommunications Act* provides complying ISPs with a 'safe harbour' or 'immunity' from civil litigation for

---

90 Uniting Church in Australia, *Submission CI 2504*.

91 A Hightower, *Submission CI 2511*; L Bennett Moses, *Submission CI 2468*.

92 S Conroy (Minister for Broadband Communications and the Digital Economy), 'Outcome of Consultations on Transparency and Accountability for ISP Filtering of RC Content' (Press Release, 9 July 2010).

93 Internet Industry Association, 'IIA to Develop New ISP Code to Tackle Child Pornography' (Press Release, 12 July 2010).

94 Internet Industry Association, 'Internet Industry Moves on Blocking Child Pornography' (Press Release, 27 June 2011).

95 *Debates*, Senate Standing Committee on Legal and Constitutional Affairs—Parliament of Australia, 2 November 2011, (Australian Federal Police answer to Question 25 on notice).

any 'act done or omitted in good faith' in performance of the duty that had been imposed on.

12.74 As of November 2011, the AFP had issued five s 313 requests to Australian ISPs,[96] which suggests that there are five Australian ISPs which are voluntarily filtering the INTERPOL blocklist at the ISP-level. There is no requirement for the ISPs to report their statistics, but for the period 1 July–15 October 2011, Telstra reported that there had been in excess of 84,000 redirections via its network.[97]

International cooperation

12.75 Alongside efforts to identify effective filtering strategies in Australia, there are international schemes which are working towards limiting the distribution of child sexual abuse content on the internet. There are four international schemes with this objective. International cooperation is vital to efforts to stop the distribution of child abuse material.

Internet Watch Foundation

12.76 The Internet Watch Foundation (IWF) is the national 'notice and take-down' body within the United Kingdom.[98] It operates an international blocklist of URLs which depict images of 'actual sexual abuse' or advertisements for and links to such content.[99] The URLs are assessed by the IWF Board in accordance with the UK Sentencing Guidelines Council criteria. Only those images assessed to be at a level 1 and above according to the criteria are considered for inclusion on the URL list, with level 1 being for images depicting persons below the age of 18 in erotic poses with no sexual activity.[100] The list contains approximately 500 URLs at any one time, is updated twice a day to ensure the entries are live, and is periodically audited by independent experts.[101] The list is designed to block specific URLs only, rather than whole domains.[102] The IWF also operates an appeals process by which any party with a legitimate association with the content, a victim, hosting company, publisher or internet consumer can appeal the placement of a particular URL on the list.[103]

INTERPOL

12.77 The international police organisation, INTERPOL, of which Australia is a member, also compiles a 'worst-of' list of domains distributing child sexual abuse

---

96 Ibid.

97 *Debates*, Senate Standing Committee on Legal and Constitutional Affairs Legislation Committee, 18 October 2011, 94 (N Gaughan).

98 Internet Watch Foundation, *IWF Facilitation of the Blocking Initiative* <www.iwf.org.uk/services/blocking> at 16 February 2012.

99 Ibid.

100 Internet Watch Foundation, *Assessment Levels* <www.iwf.org.uk/hotline/assessment-levels> at 16 February 2012.

101 Internet Watch Foundation, *IWF Facilitation of the Blocking Initiative* <www.iwf.org.uk/services/blocking> at 16 February 2012.

102 Ibid.

103 Internet Watch Foundation, *Content Assessment Appeal Process* <www.iwf.org.uk/accountability/complaints/content-assessment-appeal-process> at 16 February 2012.

material online.[104] The INTERPOL list contains domains found to be distributing 'child sexual abuse material'[105] which have been verified by INTERPOL and at least one other partner law enforcement agency.[106] Domains on the 'worst-of' list contain images of severe abuse of real children who are, or appear to be, younger than 13 years.[107] The list includes whole domains, if any part is found to contain child sexual abuse material.[108] This is because INTERPOL has determined that child sexual abuse material is not normally co-hosted with legal material but rather resides on specific domains created for the sole purpose of distributing the files.[109]

12.78 According to the AFP, the domains included in the INTERPOL list are updated approximately once per week, and although the total number of domains on the list varies with each update, by way of example the 25 October 2011 list contained 409 domains.[110] As stated earlier, the INTERPOL list is currently being used as the basis for the IIA's voluntary code in relation to ISP-level filtering.[111]

INHOPE

12.79 INHOPE is a worldwide network of internet hotlines which coordinates the investigation of internet content suspected to be illegal, including child sexual abuse content, and the reporting of illegal content to relevant law enforcement agencies and ISPs.[112] The INHOPE network includes 41 internet hotlines in 36 countries worldwide, including Australia.[113]

12.80 In 2010, INHOPE hotlines received 24,047 reports of potentially illegal child sexual abuse material, including 21,949 unique URLs.[114]

National Center for Missing and Exploited Children

12.81 The National Center for Missing and Exploited Children (NCMEC) is a private, not-for-profit organisation which was established by the US Congress in 1984 to reduce the incidence of missing children and child sexual exploitation.[115] Since 2007,

---

104 INTERPOL, *Access Blocking: Introduction* <http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking/Introduction> at 16 February 2012.

105 INTERPOL, like IWF, uses the term 'child sexual abuse material' rather than child pornography: for an outline of their definition of 'child sexual abuse material' see: INTERPOL, *Access Blocking: Criteria for Inclusion in the 'Worst of'-List* <http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking/Criteria-for-inclusion-in-the-Worst-of-list> at 16 February 2012.

106 Ibid.

107 Ibid.

108 Internet Industry Association, 'Internet Industry Moves on Blocking Child Pornography' (Press Release, 27 June 2011).

109 Ibid.

110 *Debates*, Senate Standing Committee on Legal and Constitutional Affairs—Parliament of Australia, 2 November 2011, (Australian Federal Police answer to Question 25 on notice).

111 Internet Industry Association, 'Internet Industry Moves on Blocking Child Pornography' (Press Release, 27 June 2011).

112 International Association of Internet Hotlines, *Annual Report 2010* (2010), 5.

113 International Association of Internet Hotlines, *About INHOPE* <www.inhope.org/gns/about-us/about-inhope.aspx> at 16 February 2012.

114 International Association of Internet Hotlines, *Annual Report 2010* (2010), 16.

115 National Center for Missing and Exploited Children, *Mission and History* <www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=4362> at 16 February 2012.

the NCMEC has coordinated an URL list of online 'child pornography' based on complaints made by the public to their 'CyberTipline'.[116] All reports to the CyberTipline are investigated by the NCMEC which then adds the 'worst of the worst' material—material containing images of real pre-pubescent children being sexually abused—onto a URL list.[117] The list is updated daily and made available to participating 'electronic service providers' and international law enforcement agencies, including the AFP.[118]

116 National Center for Missing and Exploited Children, *News and Events: Trend Micro Becomes the First Internet Security Company to Partner with the National Center for Missing and Exploited Children to Remove Child Pornography from the Internet* <www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=4253> at 16 February 2012.

117 Ibid.

118 Ibid.