Australian Government

Department of Communications, Information Technology and the Arts

REVIEW OF THE OPERATION OF SCHEDULE 5 TO THE BROADCASTING SERVICES ACT 1992

Report

ISBN 0 642 752117

Produced by the Commonwealth Department of Communications, Information Technology and the Arts, May 2004

TABLE OF CONTENTS

EXECUTIVE SUMMARY AND KEY FINDINGS

This is the report of the Review of Schedule 5 to the *Broadcasting Services Act 1992* (the Act), conducted by the Department of Communications, Information Technology and the Arts (the Department). Schedule 5 of the Act establishes the Online Content Co-regulatory Scheme (the Scheme), which commenced on 1 January 2000.

The purpose of this Review is to evaluate the operation of Schedule 5. The Review is required under Schedule 5 to take into account developments in filtering technologies and whether these technologies have developed to a point where it would be feasible to filter R-rated information hosted overseas that is not subject to a restricted access system. In addition, the then Minister for Communications, Information Technology and the Arts requested the Review to examine Australian Government community education initiatives under the Scheme.

The Department's Review issues paper of September 2002 (at Attachment C) set out background to the Scheme, provided detailed information about a number of issues related to the operation of Schedule 5 including outlining relevant activities of the Australian Broadcasting Authority (ABA) and NetAlert Limited, and called for comment on a range of issues. Twenty-six submissions were received from a range of public and industry groups (see Attachment B).

In order to undertake the technical analysis required as part of the Review, the Department contracted Ovum Pty Ltd to report on Internet content filtering technologies and live-streamed content (Attachments D and E respectively).

Background to the Online Content Co-regulatory Scheme

The Online Content Co-regulatory Scheme was introduced in response to community concern about the accessibility of illegal and offensive Internet content, particularly by children. Clause 1 of Schedule 5 makes clear that the key elements of the Scheme are:

1. The regulation of Internet service providers (ISPs) and Internet content hosts (ICHs) through the industry codes of practice and a complaints mechanism provided for by Schedule 5.
2. State and territory laws that impose obligations on producers of content and persons who upload or access content, and the Commonwealth *Crimes Act 1914* which makes it an offence to intentionally use an Internet carriage service with the result that another person is menaced or harassed, or in such a way as would be regarded by reasonable persons as offensive.
3. Non-legislative measures including community education.

This Review did not examine the operation of the *Crimes Act 1914* or state and territory laws as these are matters outside the scope of the *Broadcasting Services Act 1992* and are the responsibility of the Attorney-General and state and territory Ministers.

The structure and development of the Internet industry

Internet services are more ubiquitous and accessible than they were at the introduction of the Scheme. While the number of ISPs has declined since the introduction of the Scheme, following some rationalisation of the Australian Internet industry and the international economic downturn in the telecommunications sector, there has been a marked increase in Internet subscribers, from 3.85 million in September 2000 to 4.56 million in September 2002 (an 18 per cent increase).

In addition, the numbers of subscribers serviced by 'Large' (10 000 – 100 000) and 'Very large' ISPs (>100 000) grew by six per cent and 11 per cent respectively over the two years to September 2002. Subscribers in these two size categories of ISPs represent almost 87 per cent of all Internet subscribers.

Internet industry revenues have also grown significantly since the introduction of the Scheme, from $850 million in 1999 to an estimated $2.4 billion in 2003.

Ongoing role for the Online Scheme

The majority of submissions to the Review expressed clear support for the Scheme. The elements receiving greatest support included:

- the complaints mechanism administered by the ABA
- the referral of 'sufficiently serious' material by the ABA to the relevant police authorities or counterpart overseas hotlines
- the co-regulatory framework, which includes industry codes of practice
- community education as a key element of the Scheme
- international liaison, particularly with the European hotline forum INHOPE (Internet Hotline Providers in Europe Association) and the Internet Content Rating Association.

However, some submitters called for the Scheme to be either wound back or repealed.

Key findings

There has been a range of technological and market developments in online services, both domestically and overseas, since the introduction of the Scheme in 2000. Technologically, developments have resulted in more powerful servers at the ISP-level and some improvements in filtering technologies. New types of convergent communications devices have been introduced since 2000, capable of transmitting voice, data and multimedia services using the radio spectrum.

The Internet market in Australia has matured and become more mainstream than it was at the introduction of the Scheme, with subscriber numbers increasing and a higher percentage of subscribers using the larger ISPs. International cooperation has expanded, with INHOPE membership increasing by eight hotlines since the Scheme commenced. Developments in online services should be closely monitored as the technologies and market structures further mature and change in order to facilitate the appropriate regulatory response.

During the Review, a number of specific issues emerged that are relevant to the continued effectiveness of the Scheme. The key findings in relation to these issues are as follows.

Filtering technologies

- Filtering technologies have not developed to the point where they can feasibly filter R-rated content hosted overseas that is not subject to a restricted access system.
- Complex analysis filtering technologies are not practical in a national proxy filtering system. However, due to developments in search algorithms and server power, Uniform Resource Locator (URL) or Internet Protocol (IP) addressed-based filtering does appear technically feasible at the ISP or server level.
- There are a number of practical difficulties in mandating URL/IP based filtering at the ISP level, including accuracy rates and, according to the Internet industry, impact on broadband. Ovum has estimated that URL/IP based filtering would involve implementation costs of approximately $45 million and ongoing costs of more than $33 million per annum. Such costs could significantly impact on the financial viability of smaller ISPs, in particular. Given the limited benefits of an ISP-level filtering system, the costs of a mandated requirement to filter do not appear justified.
- Take-up of the Internet Industry Association's (IIA) family-friendly ISP program is low among ISPs, and many of the ISPs that provide information on filtering technologies do not give this information prominence on their homepages. Community safeguards in relation to filters could be strengthened by requiring more active promotion and research of filtering technologies by the Internet industry. The review of the industry codes, which commenced in November 2003, should address these issues.
- Requiring ISPs to offer filtering services on an 'opt-out' basis could also strengthen community safeguards. However, any increased costs for the ISPs would inevitably be passed on to consumers. These costs may be greater for customers of smaller ISPs, which do not have a large subscriber base over which to distribute costs. Further investigation is needed to establish the additional costs involved and to consider appropriate arrangements for charging for the filtering products. In the first instance, this investigation should take place via the review of industry codes.
- Developments in filtering technologies should continue to be monitored.

Community education

- There is clear support for community education as a key element of the Scheme.
- The Australian Government has addressed the need, identified by a number of submitters, for greater focus in NetAlert's community education activities by consolidating its objects and powers to focus on child safety online and researching access management technologies.

- The ABA and NetAlert should cooperatively develop an understanding of the appropriate constituencies for their different roles and functions. Such constituencies should include local councils, libraries, state and territory education departments, academic institutions and other Australian Government portfolios. NetAlert should take these factors into account in commissioning an independent evaluation of its community education activities.

Spam and transitory content (including chat rooms and live-streaming)

- Spam and transitory content such as live-streamed material or online chat room conversations are not specifically covered under the Scheme, largely because these activities are not suited to regulation by a content scheme. Nevertheless, complaints may be made about Internet content associated with such material, and greater publicity should be given to how the Scheme may be used in such cases.
- The Australian Government has created new offences for the possession and distribution of Internet child pornography. These will update and broaden the existing offences under section 85ZE of the *Crimes Act 1914*, which make it illegal to use a carriage service in a menacing, harassing or offensive manner, and will strengthen child protection regulation of the Internet.
- Increased use of filters could significantly reduce the problems associated with spam and transitory content, by blocking spam or certain streamed material, or prohibiting the sending of specified personal information.
- The Australian Government has introduced a range of anti-spam measures, including legislation, prohibiting spam from being sent from Australia, minimising spam for Australian end-users and extending Australia's involvement in worldwide anti-spam initiatives. This approach is likely to be more effective than making amendments to the Scheme.
- Under the Scheme, the ABA and NetAlert play a valuable role in educating children and carers about the dangers of predatory behaviour within Internet chat rooms. The state and federal police, however, are the organisations with the necessary investigative and arrest powers to actively intervene to prevent such behaviour. ISPs should also be encouraged to cooperate with law enforcement agencies in relation to chatroom safety and this issue should be considered in the context of the current review of the IIA Codes.

Usenet newsgroups

- The ABA should continue to use its powers to issue take-down notices in relation to complaints about Usenet newsgroup content found to be prohibited under the Scheme.
- During the review of the Internet industry codes, the industry should amend the codes to require ISPs not to host newsgroups that are notified by the ABA to regularly contain paedophile material.

Racist content

- The Scheme relies on classification decisions of the Classification Board, which is supported by the Office of Film and Literature Classification. The Classification Board makes its decisions in accordance with the National Classification Code and classification guidelines, which are agreed to by the Commonwealth, states and territories. Changes to the Code or the classification guidelines require the agreement of all participating jurisdictions. As such, the Human Rights and Equal Opportunity Commission may wish to consult Censorship Ministers about the treatment of racist material in the national classification scheme. Such an approach would ensure that online content continues to be treated in the same manner as content in other media.

Development of convergent devices

- While the Department, the ABA and NetAlert have an ongoing role in monitoring technological and market developments in convergent devices, there is a need to ensure that appropriate protections are in place for end-users, especially children, who may access audiovisual content as it becomes available on convergent devices.
- In the short-term, these protections may be achieved in relation to content delivered on short message services (SMS) and multimedia message services (MMS) through service provider rules imposed under the *Telecommunications Act 1997*. In the longer term, a review should consider whether future regulatory arrangements are required and take into account the nature and availability of these and other new and emerging services. The review would be most appropriately conducted by the Department in consultation with the ABA, the Australian Communications Authority (ACA), industry and other stakeholders.
- The current review of the IIA Codes should also consider the means for ensuring appropriate access management controls for Internet content delivered on convergent devices, especially Internet enabled 3G mobile phones.
- There is also a need to ensure that effective coordination mechanisms are in place between the ABA, appropriate law enforcement agencies and other relevant agencies in the event that the ABA receives complaints about convergent devices being used illegally for menacing purposes, including to address child safety issues.

Research into filters and associated technologies

- NetAlert should commission regular assessments of filtering and associated technologies, and widely promote this information in user-friendly brochures and reports as part of its community education and advisory role.
- The ABA should conduct regular reviews of filters listed in the schedule to the industry codes of practice, and actively enforce filters' compliance with the designated notification Scheme.
- Clause 65 of Schedule 5 could be amended to provide for the ABA to regularly update the filtering schedule separately to replacing the codes.

Monitoring of industry codes

- Internet industry codes should be reviewed at least every three years to ensure the Scheme appropriately deals with technological and market developments.

International liaison

- ABA participation in INHOPE and similar forums assists in the achievement of international best practice for administration of the ABA's complaints mechanism and should continue.
- The ABA's participation in the exchange of information between hotlines within INHOPE is an important means of responding to some forms of illegal content not sourced from Australia.
- The ABA and the Internet industry should promote the take-up of the labelling system developed by the Internet Content Rating Association, and the modification of the system for the Australian context.

1 INTRODUCTION—REQUIRED REVIEW AND PROCESS

1.1 The Review

The Online Content Co-regulatory Scheme, which commenced operation on 1 January 2000, is established by Schedule 5 to the *Broadcasting Services Act 1992* (the Act). As set out in section 3 of the Act, the objects of the Scheme are to:

- provide a means for addressing complaints about certain Internet content
- restrict access to certain Internet content that is likely to cause offence to a reasonable adult
- protect children from exposure to Internet content that is unsuitable for children.

Clause 95 of Schedule 5 to the Act requires that, before 1 January 2003, the Minister for Communications, Information Technology and the Arts must cause to be conducted a review of the operation of Schedule 5. Subclause 95(2) requires the following matters to be taken into account when conducting the review:

- the general development of Internet content filtering technologies
- whether Internet content filtering technologies have developed to a point where it would be feasible to filter R-rated information hosted overseas not subject to a restricted access system
- any other matters relevant to Internet content regulation.

The then Minister for Communications, Information Technology and the Arts requested the Department of Communications, Information Technology and the Arts (the Department) to undertake the required review of Schedule 5. In addition, the then Minister requested the Review to examine Commonwealth community education initiatives under the Scheme.

1.2 Review process

On 27 September 2002, the Department released an issues paper (Attachment C) that contained background to the Scheme and invited comments on a number of issues related to the Scheme's operation, including community education. It is recommended that the issues paper be consulted to put the matters raised in this report into context.

At the same time, the then Minister issued a media release announcing the release of the Review issues paper and calling for comment from the public and industry. The Department posted a call for submissions on its website following this media release. Submissions were sought by 8 November 2002.

The Department received 26 submissions in response to the issues paper, from a range of organisations including industry players, government bodies, community organisations and concerned citizens. Copies of submissions were posted on the Department's webpage. A list of the submitters is at Attachment B.

Following a competitive tender process, the Department contracted Ovum Pty Ltd to undertake the technological analysis required as part of the Review. Among other things, Ovum undertook detailed consultations with filter vendors and ISPs, and collected primary data on Internet content technologies and their costs. Ovum presented final reports on streaming technologies and filtering technologies on 4 April 2003. The filtering report is discussed in section 5.1 of this report and is at Attachment D. The streaming report is discussed in section 5.3 of this report and provided at Attachment E.

2 BACKGROUND TO THE ONLINE CONTENT CO-REGULATORY SCHEME

Section 2 of the Review issues paper provided a detailed outline of the Online Content Co-regulatory Scheme. In summary, the main elements are as follows.

2.1 Objects of the Act

Three objects of the Act at Section 3 are relevant to the regulation of online services:

(k) to provide a means for addressing complaints about certain Internet content

(l) to restrict access to certain Internet content that is likely to cause offence to a reasonable adult

(m) to protect children from exposure to Internet content that is unsuitable for children.

2.2 Regulatory policy

Section 4 of the Act sets out Parliament's intention that different levels of regulatory control be applied across the range of broadcasting, datacasting and Internet services according to the degree of influence the services are able to exert in shaping community views in Australia.

With specific regard to Internet services, section 4 also sets out Parliament's intention that Internet content hosted in Australia, and Internet carriage services supplied to end-users in Australia, be regulated in a manner that:

- enables public interest considerations (particularly those relating to offensive Internet content) to be addressed in a way that does not impose unnecessary financial and administrative burdens on ICHs and ISPs
- readily accommodates technological change
- encourages the development of Internet technologies and their application and the provision of services made practicable by those technologies to the Australian community
- encourages the supply of Internet carriage services at performance standards that reasonably meet the social, industrial and commercial needs of the Australian community.

2.3 Outline of the Scheme

The Scheme has three main components, as is set out in clause 1 of Schedule 5 to the Act:

1. The regulation of ISPs and ICHs through the industry codes of practice and complaints mechanism provided for by Schedule 5.
2. State and territory laws that impose obligations on producers of content and persons who upload or access content, and the Commonwealth *Crimes Act 1914* which makes it an offence to intentionally use a carriage service with the result that another person is menaced or harassed, or in such a way as would be regarded by reasonable persons as offensive.
3. Non-legislative measures including community education.

2.3.1 Prohibited content

Under Part 3 of Schedule 5, prohibited Internet content is material that is, or would be, classified RC or X by the Classification Board or, if it is Australian-hosted, classified R and access to the content is not subject to a restricted access system.

Potentially prohibited content is material that has not been classified by the Classification Board, but if it were to be classified there is a substantial likelihood that it would be prohibited content.

2.3.2 Industry codes of practice

Part 5 of Schedule 5 provides for the development and operation of three Internet industry codes of practice that are registered by the ABA. The codes require ISPs and ICHs to take appropriate steps to protect the public from 'prohibited and potentially prohibited' Internet content.

Clause 60 of Schedule 5 sets out a range of matters that Internet industry codes must deal with, including to:

- restrict access accounts to persons over 18 years old
- provide information about Internet content management and regulation
- assist customers in dealing with spam that promotes or advertises offensive Internet content
- provide information about, and access to, filtering technologies.

The codes also set out the current opt-in filtering arrangements, whereby ISPs are required to provide for subscribers—on a cost recovery basis—one of the filter products listed in the schedule to the codes. The ABA notifies prohibited or potentially prohibited overseas-hosted content to the makers of these filters. The filter makers have agreed to update their filters to subsequently block ABA notified content.

While compliance with the Internet industry codes is not compulsory in the first instance, Schedule 5 states that once the ABA directs an ISP or ICH to comply with a registered code, they must then do so. If codes are found to be deficient, the ABA may develop a compulsory industry standard.

2.3.3 Complaints mechanism

Part 4 of Schedule 5 establishes a complaints mechanism, administered by the ABA, to investigate complaints about Internet content. If the ABA finds content to be prohibited, as defined above, the ABA may order it to be taken down if it is hosted in Australia or, if hosted overseas, referred to filter makers. The ABA's Online Complaints Hotline is accessible at: *www.aba.gov.au*.

In the case of 'sufficiently serious' content, such as child pornography, the ABA refers such material to the relevant police authorities or counterpart Internet hotlines overseas.

2.3.4 Community education

Subclauses 94(b) and (c) of Schedule 5 provide for the ABA to undertake community education and advisory activities. This includes providing advice and assistance to families about the supervision and control of children's access to Internet content and conducting community education programs about Internet content and related issues.

NetAlert was established by the Australian Government in 1999 as an independent body to promote Internet safety, particularly for young people and their families. NetAlert works to achieve this through its advisory services, a tollfree national Help Line (1800 880 176), information kits, a website (*www.netalert.net.au)* and research into Internet content filters.

2.3.5 Research

Subclauses 94(d) and (f) of Schedule 5 empower the ABA to conduct research into issues relating to Internet content and Internet carriage services that will provide information to inform itself and the Minister on technological developments and service trends in the Internet industry. In addition, NetAlert was established to, among other things, undertake research into Internet access management technologies.

2.3.6 International liaison

Subclause 94(e) of Schedule 5 empowers the ABA to liaise with regulatory and other relevant bodies overseas about cooperative arrangements for the regulation of the Internet industry. Such arrangements may include, but are not limited to, collaborative arrangements to develop multilateral codes of practice and Internet labelling technologies.

2.4 State and territory laws and the Commonwealth Crimes Act

Clause 1 of Schedule 5 makes clear that state and territory laws and the *Crimes Act 1914* (section 85ZE) are integral components of the Online Content Co-regulatory Scheme.

The Explanatory Memorandum to the Broadcasting Services Amendment (Online Services) Bill 1999 indicates states and territories would be responsible for enacting legislation to regulate the activities of persons who create, upload or access content.

In relation to the Crimes Act, section 85ZE makes it an offence to intentionally use a carriage service supplied by a carrier in an offensive way or to menace or harass another person.

On 4 April 2003, the Minister for Justice and Customs announced that the Australian Government intended to introduce specific new offences for the possession and distribution of Internet child pornography. Accordingly, an exposure draft of the Crimes Legislation Amendment (Telecommunications and Other Offences) Bill 2004 was released on 14 March 2004.

As was indicated in the issues paper of September 2002, this Review is not examining the operation of the *Crimes Act 1914* or state and territory laws. These are matters outside the scope of the *Broadcasting Services Act 1992* and are the responsibility of the Attorney-General and state and territory Ministers.

3 STRUCTURE AND DEVELOPMENT OF THE INTERNET INDUSTRY

As noted in section 2.2 above, section 4 of the Act sets out Parliament's intention that broadcasting, datacasting and Internet services be regulated according to the degree of influence they are able to exert in shaping community views in Australia. Australian Bureau of Statistics (ABS) data indicates that Internet services are more ubiquitous and accessible than they were at the introduction of the Online Content Co-regulatory Scheme in January 2000.

The online industry consists of a number of participants. ISPs are a type of carriage service provider under the *Telecommunications Act 1997*, and essentially offer access to the Internet. ICHs are defined in clause 3 of Schedule 5 to be persons who host, or propose to host, Internet content in Australia. A person may be only an ISP, or only an ICH or both. ISPs and ICHs are not routinely aware of the content of material that is either accessed through, or hosted on, their services unless it is brought to their attention.

The Internet industry also includes other online service providers, which may offer a range of additional services to clients such as email, file transfer services, network 'news' groups and telephony. They may offer clients World Wide Web services in which clients' websites are hosted on the service provider's computer systems and are accessible to other users through the Internet. They may also offer caching services in which sites overseas are mirrored on their service to facilitate speed of access in Australia.

According to the ABS' *Internet Activity Survey* (ABS, Cat. no. 8153.0), there were 718 ISPs in September 2000. Following some rationalisation of the Australian Internet industry and the international economic downturn in the telecommunications sector, the number of Australian ISPs decreased to 563 in September 2002 (a 22 per cent decline).

As shown in Table 3.1, the decline in ISP numbers has been uneven across ISP categories. The numbers of Very small ISPs (<100 subscribers) and Small ISPs (101–1000 subscribers) declined significantly. However Medium ISPs (1001–10 000 subscribers) and Large ISPs (10 001–100 000 subscribers) experienced little change. Very large ISPs declined from eight to six.

Table 3.1: Number of ISPs

	Sept 2000	Sept 2002	Change %
Very small	132	102	-22.7
Small	377	254	-32.6
Medium	173	172	-0.6
Large	28	29	-3.6
Very large	8	6	-25.0
Total	718	563	-21.6

There has been a shift in subscribers to the Very large ISPs in the two-year period. At September 2002, of a total of 563 ISPs, the 356 Small and Very small ISPs account for just over two per cent of subscribers. Details are set out in Table 3.2.

While the overall number of ISPs declined, total Internet subscribers increased from 3.85 million in September 2000 to 4.56 million in September 2002, (an 18 per cent increase). During this time, household subscribers increased by 14 per cent, from 3.4 million to 3.9 million, and business and government subscribers increased by 51 per cent, from 432 000 to 650 000.

The numbers of subscribers serviced by Large and Very large ISPs grew by six per cent and 11 per cent respectively over the two years. Subscribers in these two size categories of ISPs represented almost 87 per cent of all Internet subscribers.

Revenue statistics also indicate that the Australian Internet market has grown considerably since the introduction of the Scheme. Buddecomm's report *Internet and Online Services Market: Australia 2002/2003*, states that Internet market revenues have grown from $850 million prior to the introduction to the Scheme in 1999, to $1.8 billion in 2001, to an estimated $2.4 billion in 2003 (estimated 282 per cent increase over five years).[1] Telstra's Internet operation, Bigpond, has generated similar growth in its revenue, from $197 million in 2001–02 to $505 million in 2002–03 (a 256 per cent increase over three years).[2]

Table 3.2: ISP market share (per cent)

	Sept 2000	Sept 2002	Change %
Very small	0.1	0.1	0.0
Small	4	2	-50.0
Medium	13	11	-15.4
Large	23	19	-17.4
Very large	60	68	13.3

1 Buddecomm, 2002, *Internet and Online Services Market: Australia 2002/2003*, Paul Budde Communication PTY LTD, Bucketty NSW Australia, p. 101.
2 See *www.telstra.com.au/investor/frep03fy.htm*.

In addition to the increase in subscriber numbers and industry revenue, the ABS' *Internet Activity Survey* noted that data downloads also increased overall in the two years to September 2002. Data download increased by 157 per cent in the household sector and 79 per cent in the business and government sector. On a per-user basis, the average household subscriber downloaded 390MB in the three months to September 2002, a 125 per cent increase over two years, while the average business/government subscriber downloaded 1260MB in the same three-month period (a 19 per cent increase over two years).

4 ONGOING ROLE FOR THE ONLINE SCHEME

The issues paper called for comment on specific matters in relation to the operation of the Online Content Co-regulatory Scheme, and on the Scheme in general. The majority of submissions to the Review expressed clear support for the continued operation of the Scheme. The elements of the Scheme that received greatest support included:

- the ABA complaints mechanism[3]
- the referral of 'sufficiently serious' material to the relevant police authorities or counterpart overseas hotlines[4]
- the co-regulatory framework, including industry codes of practice[5]
- community education as a key element of the Scheme[6]
- international liaison, particularly with the European hotline forum (INHOPE) and the Internet Content Rating Association[7].

However, several submissions called for the Scheme to be wound-back or repealed, based on claims about limits to information technology employment or freedom of speech, or the costs of maintaining the Scheme. For example, Adultshop.com Limited stated that the Scheme has a negative impact on information technology related employment:

> ASC [AdultShop.com Limited] would be in a position to employ more Australians in website development and hosting services were it not for the ban on X-rated material. The censorship of X-rated Internet content hosted in Australia is responsible for exporting jobs and represents a national disadvantage in the Internet economy. Not only does 'sex sell'—it also provides work in cutting edge technologies and associated financial services. In our submission, legislation that merely drives 'adult' sites offshore has only delivered adverse outcomes. (Adultshop submission, p. 1)[8]

Dr Ben Caradoc-Davies claimed that the Scheme restricts freedom of expression:

> The Schedule deprives adults of their human right to freedom of expression, discouraging them from expressing themselves through fear of prosecution or arbitrary disconnection by ISPs fearful of the legality of content. It also discriminates against poorer members of society, who may not be able to afford to establish foreign-hosted web sites or subscribe as content providers to restricted access systems. (Dr Caradoc-Davies submission, p. 5)[9]

3 See submissions made by ABA, Austar, Australian Children's Television Foundation, Childnet, Convergent Communications Research Group, Communications Law Centre, Internet Content Rating Association, Internet Industry Association, Optus and Vodafone which submitted its support for the submissions of the Internet Industry Association and Optus.

4 See submissions made by Australian Children's Television Foundation, Childnet and Communications Law Centre.

5 See submissions made by ABA, Australian Consumer's Association, Childnet, Internet Content Rating Association, Internet Industry Association and Vodafone.

6 See submissions made by ABA, Internet Content Rating Association, NetAlert and Young Media Australia.

7 See submissions by ABA, Australian Children's Television Foundation, Childnet and Internet Content Rating Association.

8 See also submission by Dr Ben Car relocated overseas (p. 2), and submission by Electronic Frontiers Australia.

9 See also submissions by Dimens that is doesn't infringe on freedom of expression' (p. 1).

Electronic Frontiers Australia stated the cost of maintaining the Scheme is difficult to justify given the limited outcomes achieved:

> There is no evidence or indication in government reports to support the [then] Minister's claim that the Internet has been made safer as a result of the Federal Government's Internet censorship law. (Electronic Frontiers Australia submission, p. 24)[10]

The Review does not consider that these submissions have made a substantive case for the wind-back or repeal of the Scheme. As noted above, on the basis of submissions to the Review there is strong community support for the Scheme, particularly the complaints mechanism, liaison with police authorities and community education.

While the Scheme does impose some compliance costs on ISPs and ICHs, these do not appear to have hampered the growth of e-commerce or the growth of the Internet in Australia. Optus, for example, expressed support for the current level of regulation:

> As both an ICH and an ISP, Optus has experienced the operation of the regime first hand and believes that the current regulatory regime for Internet Content works extremely well… The regime provides an effective and efficient structure to balance the needs of the Australian community and in particular families, with the need not to impose unnecessary financial and administrative burdens on Internet content hosts and Internet service providers.
>
> Optus urges the Government to maintain the current regime as it provides a sensible and practical approach to Internet issues and provides a sound basis for Australia to develop its information economy as we move into the twenty-first century. (Optus submission, pp. 2–4)[11]

By helping to ensure that the online environment is as safe as possible, it can be argued that the Scheme promotes confident and safe use of the Internet and, therefore, e-commerce in Australia. Similarly, by encouraging non-users who might otherwise have been deterred from accessing the Internet—because of fears that they or their children will come across harmful material—the Scheme assists Australians to realise the benefits of going online.

In relation to freedom of expression, Schedule 5 is premised on the principle that what is illegal offline should also be illegal online. It does not provide for more onerous restrictions than those that apply to conventional media regulated under the Act. Definitions of prohibited material are based on specific and detailed criteria of the widely accepted national classification scheme administered by the Office of Film and Literature Classification. This scheme is designed to balance the public interest in allowing adults to read, hear and see material of their own choosing, with the public interest in protecting minors from material likely to harm or disturb them, and in protecting the community generally from offensive material.

The views expressed in the majority of submissions suggest that the Online Content Co-regulatory Scheme has been effective in meeting its objectives and is in line with community views on this issue. The complaints-based regulatory framework responds to community concerns in relation to Internet content by enabling persons to complain about Internet content. More than 300 Australian-hosted items have been issued with take-down notices to date, and more than 1500 items have

10 Dr Peter Chen similarly submitted that the Scheme has not been effective in achieving its objectives (Chen, 2002).

11 See also submissions by Internet Industry Association, Telstra and Vodafone.

been referred to Scheduled filter makers so that the filters block access to the content. The ABA has also referred more than 600 items of sufficiently serious material (typically child pornography) to the relevant police authorities or counterpart hotlines overseas.

5 ISSUES

During the Review a number of issues emerged that are relevant to the continued effectiveness of the Online Content Co-regulatory Scheme. The Review has proposed refinements to the Scheme in areas where changing technology or market structures have highlighted the need for additional community safeguards, including in relation to filtering technologies, Usenet groups and monitoring of the codes of practice.

The Review has also suggested the need for a regulatory response where technological convergence is likely to bring about significant change, such as convergent devices. In this context, it is noted that there have been some recent initiatives to strengthen community safeguards in relation to the use of carriage services. In particular, the Minister for Justice and Customs and the Minister for Communications, Information Technology and the Arts have jointly announced new offences in relation to the possession and distribution of Internet child pornography.

It is also argued that the Scheme is not the most appropriate framework for addressing certain matters.

The following sections provide more information on the issues that have emerged:

- filtering technologies
- community education
- spam and transitory content (including chat rooms and live streaming)
- usenet newsgroups
- racist content
- convergent devices (e.g. 3G)
- research into filters and associated technologies
- monitoring of industry codes
- international liaison.

5.1 Filtering technologies

The Internet provides access to a wide range of material. Some of this material may not be suitable for children or may be generally offensive or illegal. Filtering technologies can limit the Internet content end-users can access by preventing or blocking access to specified pieces of types of content.

The Review has examined technological developments in filtering technologies since the introduction of the Scheme and the arrangements under the Scheme for the provision of filters to end-users.

Section 1.1 above notes that clause 95 of Schedule 5 requires the Review to take into account the general development of Internet content filtering technologies and whether these technologies have developed to feasibly filter R-rated information hosted overseas that is not subject to a restricted access system. The Department contracted Ovum Pty Ltd to undertake the required technical analysis. Ovum is a consulting group, based in the United Kingdom, well known for its work in the field of telecommunications, software and information technology services. On 4 April 2003, Ovum presented the Department with its *Internet Content Filtering Report* (Attachment D).

Clause 95 of Schedule 5 also requires the Review to assess its operation. Therefore a key issue for the Review is the operation and effectiveness of the current filtering arrangements. Subclause 60(2) of Schedule 5 requires the industry codes to deal with procedures for ISPs to follow to deal with prohibited overseas-hosted content; for example, to provide filtering.

To this end, the IIA codes set out a requirement for ISPs to provide their subscribers—on a cost recovery basis—with a filter listed in the Schedule to the codes.

The ABA issues prohibited content hosted in Australia with a take-down notice and refers prohibited overseas-hosted content to the makers of the Scheduled filters so that the filters are updated to subsequently block access to the content.

5.1.1 Developments in filtering technologies

The Ovum report notes that filtering can be performed at four locations, namely:

- the end-user's personal computer (PC)
- server at the ISP-level[12]
- firewall[13]
- network device (ie. router).[14]

Of the non-PC locations, Ovum states that server and firewall are the most effective locations:

> …it is possible to route all Internet traffic through a firewall or server (or a set of them). With network devices, e.g. router, it is not possible to guarantee that all Internet traffic will pass through the filtering enabled ones…
>
> It is also possible to implement granular filtering (i.e. different levels of filtering for different users) on servers and firewalls, but not on network devices. Granular filtering is something that is important to enterprises, and would be essential for any system that needed to distinguish between children, teenagers and adults. (Ovum, 2003, p. 19)

Ovum was directed to report on the technical and financial matters associated with ISP-level filtering. To this end, Ovum states that the most effective method to ensure the filtering of all web content is to use a pass-through, or proxy server.[15] This ensures that every access request from every user is subject to the same rules and that nothing can pass without inspection and filtering (Ovum, 2003, p. 19).

12 An ISP web server is a computer which provides a 'service' on the Internet (e.g. hosting web pages and web applications).

13 Firewalls are commonly used by enterprises to prevent unauthorised access to or from the enterprise's private network.

14 A router is the backbone of the numbers) and, using this information, directs the data towards its destination. Router filtering would block information even before it reaches the Australian ISP. It is reported that this approach is used in China.

15 A proxy server is a server which sits between an end-user and a real server. Proxy servers were designed to improve ISPs' security and performance by caching (i.e. saving) commonly accessed pages. Proxy servers intercept requests to assess whether they can fulfil the request themselves and, therefore, provide the content to the user more quickly and minimise the ISP's downloads.

In this context, in relation to the developments in filtering technologies, the Ovum report states that it is no more practical than it was at the introduction of the Scheme to use complex 'analysis' filtering techniques via a proxy system. It is, however, more technically feasible to use 'index' filtering than it was previously.

In a proxy system, the analysis filtering techniques assess the content of a webpage prior to providing access to the page. There are five main types of such analysis filtering techniques:

- file type to block all files of one format (e.g. all jpeg image files or all mpeg audiovisual files)
- text type to 'read' the content of a page for occurrences of specified words or phrases
- link type to assess the pages that are linked or referenced on the requested webpage
- image type to 'read' pictures for sexual content (e.g. occurrence of skin tones)
- profile type to compare a page against the common characteristics of pages which typically would be blocked.

In relation to the analysis filtering techniques, such as file type and link type, analysis may result in a high degree of false positives as they do not assess the content of a particular page. Textual, image and profile type analyses can have a significant impact on network performance, as greater accuracy typically requires increased system resources resulting in slower response times.

Ovum states that none of the five analysis methods are of practical use in a national proxy system (Ovum, 2003, pp. 19–21). However, analysis-filtering techniques are more practical in PC-based products, where the filter is required to deal with the requests of only one computer, or in off-line mode where content is not assessed for blocking in real time but for blocking in response to subsequent requests for the content.

As noted above, Ovum states that index filtering is now more feasible in a proxy system than it was at the commencement of the Scheme. Index filtering technologies are based on blocking access to pre-determined lists of URLs (uniform resource locators—alpha-numeric web addresses) and/or IP addresses (Internet protocol addresses—32-bit numbers identifying points on the Internet).

Ovum states that improvements in index filtering, including more sophisticated search algorithms and greater processing power at the server level, have reduced the delay of such filtering at the ISP-level to approximately ten milliseconds per request. This delay generally is not noticeable to the end-user. Filter vendors and ISPs noted that while larger lists of URL and IP addresses previously increased response times, this is no longer the case.

Nevertheless, filtering that utilises only index technologies is limited by the list employed, as it does not block unlisted content. Maintaining an effective list is complicated by the dynamic nature of the Internet where new pages are constantly posted online. Moreover, while filter vendors commonly update their indices at least daily, some pages

will be miscategorised during automated analysis and many vendors manually check each new URL identified for blocking. This requires significant resources and may create additional delays in listing pages for blocking.

With particular regard to indices of IP addresses, filtering based on such lists blocks access to all traffic from web sites on the same IP address. Many modern hosting services host thousands of domains on a single published IP address. Accordingly, IP address-based filtering may result in significant overblocking of content that is not prohibited but is located on the same IP as listed prohibited content.

There are a number of practical difficulties that could impact on the implementation of ISP-level index filtering. While the Ovum report states that index filtering at the ISP-level would not make broadband unfeasible (p. 24), this conclusion is not supported by the Internet industry or its representative body which has argued that mandating the use of filters at the ISP-level could significantly reduce the access speed of broadband connections. Speed is the leading value proposition for broadband customers, and any reduction in performance may impact on this key advantage. One Australian ISP consulted during the Review stated that it offers ISP-level filtering on its narrowband connection but not on its broadband connection, due in part to the time lag of the filtering. It stated that the delays associated with the filtering it employs are not noticeable on the slower narrowband connections, but would be noticeable to end-users on its broadband connections. In this context, the ISP recommends that broadband subscribers use a PC-based filtering tool.

In addition, there would be significant cost imposts involved in requiring ISPs to implement filtering at the server-side. The costs estimated by Ovum are at Table 5.1.1. The figures comprise initial set-up costs including extra servers to run the filtering software and personnel to establish the system, and ongoing annual costs of software licences and personnel. More information can be found at section 3.6 of the Ovum report.

As Ovum notes in relation to these costs:

> [T]he cost of implementing such a system remains high. In addition to the initial set-up costs, ISPs also have an ongoing annual cost for licence fees, any lease costs of additional infrastructure and ongoing administrative costs. The costs in the first year of implementation are sizeable and are unlikely to be regained even if charges are passed on to users.
>
> The effects of these costs on small ISPs will have more significant impact than on the larger ISPs. Larger ISPs may potentially use this as a competitive advantage by not passing on costs to users. Although larger ISPs will also see reduced margins, there will be less of an impact than on the smaller ISPs. (Ovum, 2003, pp. 5–6)

Table 5.1.1: Ovum's estimated establishment costs for ISP-level filtering

	Initial set up costs				Ongoing annual costs			
Definition	Server/s (AUD$)	Setup costs (employee-months)	Setup costs (AUD$)	Total (AUD$)	Software licenses (AUD$)	Admin costs (employee-months)	Admin costs (AUD$)	Total (AUD$)
Very small	8000	3	18 750	**26 750**	500	1	6250	**6750**
Small	8000	4	25 000	**33 000**	5000	3	18 750	**23 750**
Medium	50 000	6	37 500	**87 500**	35 000	9	56 250	**91 250**
Large	500 000	12	75 000	**575 000**	200 000	18	112 500	**312 500**
Very large	500 000+	18	112 500	**612 500+**	200 000+	24	150 000	**350 000+**

The figures given are based on the maximum number of subscribers in each category, except for the 'Very large' category where the minimum has been used.

On the basis of Ovum's estimates, the estimated cost per subscriber of implementing ISP-level filtering is significantly higher for small-to-medium enterprises. For example, initial setup costs for such filtering would be eight times greater for very small ISPs than for small ISPs, and almost four times greater for small ISPs than for medium ISPs. Ongoing costs would similarly have a greater impact on the smaller ISPs. Details are at Table 5.1.2.

Table 5.1.2: Estimated costs per subscriber for ISP-level filtering

	Initial setup $	Ongoing annual $
Very small	267.50	67.50
Small	33.00	23.75
Medium	8.75	9.12
Large	5.75	3.12
Very large	6.12	3.50

The figures given are based on the maximum number of subscribers in each category, except for the 'Very large' category where the minimum has been used.

On the basis of Ovum's estimates and factoring in the most recent ABS data of ISP numbers in Australia, the total cost of implementing ISP-level filtering would be over $45 million for initial setup and over $33 million per annum. Details are at Table 5.1.3.

Table 5.1.3: Estimated total costs to the Internet industry

	No of ISPs	Initial setup $	Ongoing annual $
Very small	102	2 728 500	688 500
Small	254	8 382 000	6 032 500
Medium	172	15 050 000	15 695 000
Large	29	16 675 000	9 062 500
Very large	6	>3 675 000	>2 100 000
Total	563	>$46 510 500	>$33 578 500

Industry estimates provided during consultations of the cost of ISP-level filtering are significantly higher than those provided by Ovum. However, even the Ovum estimates suggest that the costs associated with implementing ISP-level filtering would create an onerous burden on the Internet industry. If the costs are borne by providers, the imposition could result in a number of small firms, in particular, becoming commercially unviable. If, as is to be expected, costs are largely passed on to consumers, the resulting increase in subscription fees and associated decrease in demand, particularly for smaller ISPs, would similarly result in reduced commercial viability.

Generally, PC-based filter technologies can apply more sophisticated filtering technologies than are practical at the ISP-level. This is primarily due to the reduced system resources required to filter only one end-user's Internet requests. In this context, a number of PC-based filters apply a combination of filtering technologies. For example, such filters which use a URL/IP list may also use keyword searching in titles and sometimes in text. The currently available filters that use the complex analysis filtering technologies are generally PC-based filters, and there have been significant developments in PC-based filters to combine two or more filtering techniques in an integrated package.[16] These developments in PC-based filtering technologies are leading to substantial improvements in the blocking accuracy of these filters.

5.1.2 Operation of filtering arrangements

As noted in section 2.3.2 above, subscribers currently have the option to opt-in to a filtering product or service under the registered industry codes of practice. ISPs make available at cost price one of the 19 filters listed in the industry codes. The ABA notifies prohibited overseas-hosted content to the makers of these filters so they are updated to block access to the prohibited content. The filters may be configured to suit the needs of different user profiles, which can include 'whitelists'[17] of selected sites for younger children, general filtering for older children, and more limited blocking for adults and businesses.

With regard to industry promotion of filtering services, subclause 60(1) of Schedule 5 requires the industry codes to deal with giving users information about supervising and controlling children's access to Internet content, including

16 Community funded filter projects at *www.saferinternet.org/projects/index.asp#filtering*. For example, the prototype NetProtect (see *www.net-protect.org*) combine list-based filtering with real time linguistic and image analysis.

17 Whitelist filters allow access to a selected younger children.

giving information about the availability and use of filtering software ((d) and (k) of subclause 60(1)). However, for the purposes of this obligation, clause 5.4 of the IIA Content Code 1 allows ISPs merely to provide a link from their homepage to such resources made available by the IIA, ABA, NetAlert or other approved organisations.

It seems reasonable to conclude that the majority of ISPs could improve their community education activities. This is acknowledged by the IIA which states in its submission that it 'would like to see better compliance' (p. 5). Twenty-four months after launching its Family-Friendly ISP seal program—ISPs that are fully compliant with the Internet industry codes may display the IIA-endorsed 'ladybird logo' on their website—the IIA has advised that only eleven ISPs have registered under the program and are entitled to display the seal. While the introduction of the program is welcome, as it provides families with clear guidance in choosing code compliant ISPs, take-up of this program is low among Australia's 563 ISPs— particularly among the smaller ones.

In addition, it appears that community awareness of the role of filtering tools under the Scheme is not high. The ABA's 2001 report *The Internet at home: A report on Internet use in the home* stated that only 32 per cent of parents surveyed who had the Internet at home recalled being told about filter software by their ISP.

In this context, there would appear to be value in strengthening the filtering requirements under the Scheme. Two practical options would be to strengthen the current opt-in filtering approach by increasing industry community education requirements and/or to require ISPs to offer filtering on an opt-out basis. Both options, however, would maintain the current focus on end-user filtering.

Option 1

Strengthen current 'opt-in' approach

Current community safeguards could be promoted by strengthening the current opt-in approach for choosing a filtering product by requiring more active industry promotion of filtering technologies. To this end, ISPs could actively promote filter services during subscription sign-on. This would draw filtering technologies to the attention of people who are new to the Internet, and remind existing Internet users who are changing ISPs of the available tools for managing Internet access.

In addition, ISPs could regularly advertise filtering services to their subscribers to encourage uptake. This could be in the form of quarterly subscriber email bulletins as well as more obvious links to filtering services and filtering information on the ISP's homepage. Currently, a number of ISPs that do link to the IIA's resources on filtering technologies often do so at the bottom of their homepage or from a subsidiary page. One IIA member provides information on filtering options under the heading 'Net Censorship'.

The Internet industry could also promote and undertake community education and research activities in relation to filtering technologies. The ABA and NetAlert undertake the bulk of this work under the Scheme. In line with the co-regulatory framework for online content

regulation, it would be appropriate for the industry to actively support the education and advisory functions of NetAlert in this regard.

Option 2

Require ISPs to offer end-user filtering on an opt-out basis

Making ISPs offer end-user filtering products with Internet subscriptions, on an opt-out basis, could also be a further step in strengthening the filtering requirements under the Scheme.

ISPs could be required to offer Internet subscriptions that automatically include an end-user filtering product or service. Accepting the filter could be set as a subscription default option. Therefore users would have to actively select not to accept the filter. The approved filtering products would be limited to the most effective products listed in the Schedule to the industry codes. This would require ongoing technical assessment of the listed filters, which could be undertaken or commissioned by the ABA and/or NetAlert.

Such filtering arrangements would promote the use of filtering technologies to all Internet users, while enabling users who do not wish to use a filter to opt-out. For existing users, ISPs could be required to email subscribers on a quarterly basis providing information about access management technologies and linking to the download of an approved filter.

The costs of requiring ISPs to implement an automatic filter inclusion are unclear and would need to be assessed in consultation with industry. The relative impacts on smaller ISPs would require detailed consideration, as these ISPs have a smaller subscription base to distribute the costs of establishing and maintaining the opt-out arrangements. Nevertheless, the overall costs to industry would be significantly lower than requiring mandatory implementation of server-side filtering. Consideration should also be given to arrangements for charging for filtering products and services and the additional costs involved. However, it is reasonable to assume that the additional costs for industry would inevitably be passed on to consumers in the price of the service.

Implementation of proposed options

There are a number of regulatory instruments that could be considered for strengthening the filtering requirements under the Scheme.

First, the industry could be encouraged to adopt the proposed filtering requirements in the industry codes. Clause 60 of Schedule 5 requires that the industry codes deal with the provision of information about Internet content management and regulation, and sets out procedures for ISPs to follow that deal with prohibited overseas-hosted content. Clause 66 provides that ISPs and ICHs must comply with any ABA direction to comply with the registered Internet industry codes. Such a direction could apply to strengthened filtering requirements if they are incorporated into codes registered by the ABA.

Second, clause 80 of Schedule 5 allows the ABA to make written determinations setting out rules that apply to ISPs in relation to the supply of Internet carriage services. These 'online provider determinations' could apply

to strengthened filtering requirements. Compliance with online provider determinations is an 'online provider rule' under Schedule 5, contravention of which is an offence with a maximum penalty of $5500 per day for an individual or $27 500 per day for a company.

5.1.3 Detection of access restriction mechanisms

In addition to the general prohibition on RC and X material, prohibited Australian-hosted content also includes R material that is not protected by a restricted access system.

Restricted access systems are adult verification devices that allow only people who are 18 years or older to access adult material on the Internet. Used in conjunction with filters and adult supervision, restricted access systems help protect children from exposure to material that may be unsuitable for them.

For the purposes of Schedule 5, an ABA declaration setting out minimum system requirements for restricted access systems was tabled in Parliament on 7 December 1999. The declaration sets out the process by which a person can gain access to Internet content that is likely to be rated R by the Classification Board. It relies on credit card validation as a means to check that a person is 18 years or older.

Subclause 95(5) of Schedule 5 states Parliament's intention that, in the event that filtering technologies are developed that can in practice prevent end-users from accessing overseas-hosted content not subject to a restricted access system, legislative amendments should be introduced to include such R category overseas-hosted content.

Ovum was tasked with undertaking this assessment. As explained in its report on filtering technologies, Ovum concluded that no commercially available filtering system can detect a user as having passed through a restricted access system (p. 22). Filtering technologies have not developed to the point where they can detect whether a user has been authorised to access restricted content, and cannot practically prevent end-users from accessing content not subject to such a system.

Key findings—filtering technologies

Filtering technologies have not developed to the point where they can feasibly filter R-rated content hosted overseas that is not subject to a restricted access system. Complex analysis filtering technologies are not practical in a national proxy filtering system. However, due to developments in search algorithms and server power, URL or IP addressed-based filtering does appear technically feasible at the ISP or server level.

There are a number of practical difficulties in mandating URL/IP based filtering at the ISP-level, including accuracy rates and, according to the Internet industry, impact on broadband. Ovum has estimated that URL/IP based filtering would involve implementation costs of approximately $45 million and ongoing costs of more than $33 million per annum. Such costs could significantly impact on the financial viability of smaller ISPs, in particular. Given the limited benefits of an ISP-level filtering system, the costs of a mandated requirement to filter do not appear justified.

cont...

Take-up of the IIA's family-friendly ISP program is low among ISPs, and many of the ISPs that provide information on filtering technologies do not give this information prominence on their homepages. Community safeguards in relation to filters could be strengthened by requiring more active promotion and research of filtering technologies by the Internet industry. The current review of the industry codes should address these issues.

Requiring ISPs to offer filtering services on an opt-out basis could also strengthen community safeguards. However, any increased costs for the ISPs would inevitably be passed on to consumers. These costs may be greater for customers of smaller ISPs, which do not have a large subscriber base over which to distribute costs. Further investigation is needed to establish the additional costs involved and to consider appropriate arrangements for charging for the filtering products. In the first instance, this investigation should take place via the review of industry codes.

Developments in filtering technologies should continue to be monitored.

5.2 Community education

Section 1.1 above noted that the then Minister requested the Review to examine Commonwealth community education initiatives under the Scheme. Clause 94 of Schedule 5 empowers the ABA to undertake community education initiatives including providing advice about Internet content and access management. As part of the Online Scheme, NetAlert particularly was established to:

- monitor online content
- provide advice about options for addressing concerns about content
- provide a community-based hotline to receive and pass information about illegal Internet content to the ABA and police authorities.

5.2.1 Australian Broadcasting Authority

The issues paper provided information about the ABA's activities in regard to community education (section 3.3). The ABA's submission stated that its activities in this regard are underpinned by research into community views about Internet content, the ways the Internet is used by Australian households and the information needs of Internet users, particularly families with children.

> Prior to commencement of the Scheme, the ABA undertook and commissioned research on community attitudes toward Internet content and alternative regulatory responses. Following commencement of the Scheme, the ABA commissioned the Internet @ home research project… The findings of this research have been a key input to development and implementation of the ABA's community education strategy for Internet content. The focus of the strategy has been the redesign of online and offline materials, including replacement of the Australian Families Guide to the Internet with the Cybersmartkids web site, www.cybersmartkids.com.au… To complement the site, a range of information brochures has been developed. They include general Internet safety tips, information about selection of filter software, and advice on dealing with spam. A brochure about safety in chat rooms will be released in December 2002. (ABA submission, p. 29)

Submitters to the online review were generally supportive of the ABA's community education activities. Particular reference was paid to the ABA's cybersmartkids website, which provides Internet safety tips for children and their guardians and information brochures about online safety.

Electronic Frontiers Australia, however, submitted that the ABA should not be involved in community education:

> EFA submits that this is an inappropriate role for a regulator. The Reserve Bank does not presume to take a role in education of the public as to home budgeting. (Electronic Frontiers Australia submission, p. 18).

Overall, it does not seem that this argument is generally accepted. Clause 94 of Schedule 5 makes clear that Parliament intended that the ABA would undertake community education as part of the Scheme. The ABA is empowered to advise and assist adults in relation to the supervision and control of children's access to Internet content, and to conduct and/or coordinate community education programs about Internet content and Internet carriage services (subclauses (b) and (c)). The ABA uses the expertise it has developed in relation to the broad range of Internet content to inform users of safe surfing practices, in addition to advising the Internet industry of its obligations under the Scheme.

5.2.2 NetAlert

In the 2003–04 Federal Budget, the Australian Government extended its funding commitment to NetAlert by a further $2 million for the three years to 2005–06. The Government had previously allocated NetAlert $4.5 million in the four years to 2002–03.

Information about NetAlert's activities under the Scheme is also provided in the issues paper (section 3.3). NetAlert submitted that it has promoted the use of the Internet while educating users about the risks of Internet access:

> In a country as large and diverse as Australia, the Internet is proving the ideal tool to erode distances and bring together consumers across rural, regional and urban areas of Australia. The Internet can be used to make connections, increase social capital, create or reveal new business opportunities, break down misunderstandings and barriers based on ignorance and educate Australians of any age.
>
> However, we would also be failing in our duty of care if we did not raise awareness of the dangers to be found on the Internet and address these dangers with appropriate measures to minimise the impact such dangers can have on young people, Australian businesses and communities and Australians in general (NetAlert submission, pp. 7–8).

Submitters generally expressed support for the continued operation of NetAlert. For example, the IIA stated:

> For its part, NetAlert has risen to the challenge of becoming the primary resource for community advice across a range of content related issues. The NetAlert site has been very well received and is experiencing marked and sustained increases in its usage. In addition, NetAlert's outreach programs are bringing the empowerment story to an ever-increasing number of Australians. Its media profile has grown substantially in the past 12 months and we believe that it will soon, if it hasn't already, establish itself as the unequivocal community information point for internet related issues. (IIA submission, p. 10)

However, a number of submitters expressed concern about the role and effectiveness of NetAlert, particularly its proposed 'Growing Australia Online' re-branding effort and consequently an apparent lack of focus on its core role of promoting Internet safety. Consultations undertaken as part of the Review highlighted the following areas of concern:

- there could be greater public awareness of NetAlert[18]
- NetAlert could develop greater links with local councils, libraries, state and territory education departments, academic institutions and other Commonwealth portfolios in developing its community education programs[19]
- NetAlert should further extend its community education activities to the 'offline' environment, including computer retailers, libraries and schools[20]
- NetAlert should commission independent evaluation of its community education activities.[21]

It is notable that on 2 July 2003, the then Minister announced that the Australian Government had consolidated NetAlert's objects and powers, as set out in its Constitution, to delete redundant provisions and further focus the organisation on child safety online. The Government stated that it envisages that NetAlert will maintain its website and advisory hotline, undertake research into publicly available filtering technologies and liaise with relevant domestic bodies. In addition, NetAlert will continue to provide community feedback on draft industry codes prior to registration by the ABA.

The revised objects and powers are set out on the following page.

18 For nding that less than one-third of libraries were aware of NetAlert and few actively used it (ALIA supplementary submission, p. 1).

19 See submissions by ALIA, Australian Children's Television Foundation, Childnet and Young Media Australia.

20 See submissions by Australian Consumer's Association and Australian Children's Television Foundation.

21 See submissions by Childnet, Electronic Frontiers Australia and Young Media Australia.

NetAlert's Objects and Powers

OBJECTS

NetAlert's objects are to promote a safer Internet experience, particularly for young people and their families, and in particular to:

(a) provide users with sensible, helpful and reliable advice and information about potential problems, dangers and threats present on the Internet and ways in which users can act to minimise or avoid these problems

(b) develop and promote information on existing technological solutions that assist users and the Internet industry to better manage Internet content

(c) work closely with Commonwealth and state agencies—particularly the ABA—the Internet industry and community organisations in order to promote Internet safety

(d) maintain an active awareness of Internet content and take appropriate action on prohibited and potentially prohibited content, including operating an email and telephone advisory services to receive concerns about offensive material and pass any appropriate information to the ABA and relevant law enforcement agencies

(e) consult with industry bodies on the development of effective draft industry codes that promote and support the Company's objects and promote industry compliance with the online Scheme.

POWERS

NetAlert has the powers set out in the Law but only to do all things that are necessary, convenient or incidental to carry out the above objects including:

(a) initiating research into filtering and adult verification technologies for ISPs, ICHs and their clients

(b) ensuring that parents and other concerned Australians are easily able to make contact with the Company in order to report or complain about prohibited content, potentially prohibited content or other inappropriate Internet content

(c) embarking on public awareness and education campaigns to raise public awareness of ways in which parents and other concerned Australians can improve the management of the Internet to create a safer web experience

(d) becoming a designated body under clause 58 of Schedule 5 of the Broadcasting Services Act and provide quality feedback on any industry codes or industry standards.

Given that the ABA has a legislated education function and community awareness raising role, and the Government established NetAlert to promote Internet safety, it is important that the ABA and NetAlert ensure that their activities are complementary and coordinated. NetAlert, as a community-based organisation, and the ABA, as a government agency, can be expected to have different strengths and capabilities, and different relevant constituencies in awareness raising.

Key findings—community education

There is clear support for community education as a key element of the Online Content Co-regulatory Scheme. The need identified by a number of submitters for greater focus in NetAlert's community education activities has been addressed by the Australian Government by consolidating NetAlert's objects and powers to focus the organisation on child safety online and researching access management technologies.

The ABA and NetAlert should work cooperatively to ensure their activities complement each other. The ABA and NetAlert should also cooperatively develop an understanding of the appropriate constituencies for their different roles and functions. Such constituencies should include local councils, libraries, state and territory education departments, academic institutions and other Australian Government portfolios. NetAlert should take these factors into account in commissioning an independent evaluation of its community education activities.

5.3 Spam and transitory content (including chat rooms and live streaming)

Clause 3 of Schedule 5 specifically excludes ordinary email from the definition of Internet content and therefore from the Scheme. The Second Reading Speech to the Broadcasting Services Amendment (Online Services) Bill 1999,[22] which provided for Schedule 5, noted that transitory content, such as chat rooms and real time streaming, is also excluded from the Scheme given that it would not be possible to classify 'live' material.

5.3.1 Spam

Spam is the commonly used term for unsolicited (commercial) electronic messages. The National Office for the Information Economy's (NOIE) final report of April 2003 into spam[23] stated that it is a significant and growing problem. Spam represents at least 50 per cent of all global email traffic and this proportion appears to be growing rapidly. The NOIE report stated that there are community and regulatory agency concerns with the illicit content of spam, particularly in relation to fraudulent activities, health advice and pornography.

22 Senate Hansard, Wednesday 21 April 1999, pp. 3957–3963.

23 NOIE, 2003, *Spam: Final report of the NOIE review of the spam problem and how it can be countered*, available at: *www.noie.gov.au/projects/confidence/Improving/spam.htm.*

Among other things, the NOIE report recommended that national legislation be introduced to require commercial electronic messaging to require the prior consent of the end user and to contain accurate details of the sender's name and physical and electronic addresses. The report also recommended that ISPs be required to provide spam filtering at a reasonable cost, and to evaluate and publicise spam filtering options and products.

Of particular relevance to this Review, the NOIE report recommended that consideration should be given to whether additional steps should be implemented to minimise exposure of Internet users, particularly minors, to pornographic and other offensive spam (p. 19).

The issues paper called for comment on the application of the Scheme to spam (see section 3.6 of the issues paper). The issues paper stated:

> Typically, spam is not hosted nor is it generally accessible on the Internet. The question arises, therefore, of the method by which the complaints Scheme and system of take-down notices could apply to offensive spam email or how the existing Scheme could be amended to apply specifically to offensive spam. (Review issues paper, p. 19)

The ABA's submission to the Review noted that its powers in relation to issuing take-down notices are limited to Internet content hosts, which does not necessarily cover senders of spam. The ABA stated that it will continue to undertake investigation of content linked in spam, and community education of users to minimise spam.

While the ABA agrees with the recommendation by NOIE that there is merit in exploring how complaints about spam could be dealt with under the co-regulatory Scheme for Internet content, the ABA considers that mechanisms contained in Schedule 5 of the Act would have limited capacity to effectively address the issue on their own. In particular, constraints on the application of the complaint handling mechanism to spam arise from the separation between the senders of unsolicited email on the one hand and the hosts of the Internet content to which the email relates on the other. The ABA's powers are limited to issuing take-down notices for Internet content hosted in Australia and notifying overseas Internet content to the makers of filter products and services, and the ABA cannot take action in relation to the senders of email itself.

In the ABA's view, an effective anti-spam strategy will need to include measures directed at combating the sources of spam, together with activities to raise community awareness about avoiding and managing spam. It sees merit in considering whether further guidance could be given to ISPs through the codes by way of specific examples of procedures that ISPs could adopt, for example, a standard information page with options for the provision of spam filtering products and services that could be included on an ISP's website. (ABA submission, p. 13)

The submitters that commented on the spam issue recommended that the Scheme not be extended to cover spam. For example, the Australian Consumers' Association noted that incorporating spam into the Scheme would complicate the definition of Internet content in clause 3 of Schedule 5, which excludes ordinary email from the definition of Internet content.

> A lot of the offensive UBE [unsolicited bulk e-messages] is offensive because it touts for or points to online sites (for which the consumer is often asked to pay). These sites would fall within the content regime as defined and could be complained about and dealt with accordingly. It is difficult to see how including actual emails themselves in the regime would assist, since there is not an effective methodology in place to discourage the sending of UBE. However, such a step would blur the line between personal email and Internet content, a line that should be maintained. (Australian Consumers' Association submission, p. 4)[24]

5.3.2 *Live-streamed content*

On 29 April 2002, the ABA released a report on media streaming and broadband services in Australia.[25] Media streaming is a technique for making video and audio available in digital form, over narrowband platforms. While the report predicted that streaming would be overtaken by successor technologies within approximately five years, it argued that live-streamed content is not covered by Schedule 5.

The ABA report noted that clause 3 of Schedule 5 defines Internet content to mean information that is kept on a data storage device and is accessed, or available for access, using an Internet carriage service (excluding ordinary electronic mail or information transmitted in the form of a broadcasting service). In this context, the report argued that content that is live-streamed is not kept on a data storage device and, therefore, does not fall under the definition of Internet content.

It was in this context that the Review issues paper of September 2002 called for comment on application of the Scheme to live-streamed material (section 3.6).

The ABA's submission to the Review recommended that the regulatory status of live-streamed content be clarified and that such content be regarded as Internet content for the purposes of the Scheme (ABA submission, p. 3). Similarly, the Australian Consumers' Association recommended that live-streamed content be dealt with under the Scheme:

> It would in our view be incongruous for live-streamed Internet content to somehow be an exception to the general regime of content control. We agree with the determination that streamed media should not be treated as broadcast, and hence such material would be best dealt with as a form of Internet content and regulated accordingly. (Australian Consumer's Association submission, p. 4)

However, the IIA and the Internet Society of Australia argued that live-streamed content should not be covered under the Scheme. Specifically, the IIA stated that live-streamed content is not compatible with the take-down arrangements under the Scheme:

> In the case of live-streamed content, it is our firm view that its regulation is incompatible with a complaints based Scheme relying on due process and evaluation against the National Classification Guidelines by the relevant

24 See also submissions by the Communicati

25 Centre for Telecommunications Information Networking, 2002, *Media Streaming and Broadband in Australia: Report to the Australian Broadcasting Authority*, available at: *www.aba.gov.au/abanews/conf/2002/papers/ctin.pdf*

> authority. We are aware of no evidence to suggest that children's access to inappropriate live-streamed content is yet so pressing an issue as to warrant any regulatory measures operating in real time, even if they were capable of being developed. (IIA submission, p. 12)

The Review commissioned Ovum to provide advice as to the technical aspects of live-streamed content, as a basis for legal advice on its regulatory status under Schedule 5. The *Live Media Streaming Report* on live-streamed content is provided at Attachment E. In summary, the subsequent legal advice confirms the view put in the 29 April 2002 report to the ABA that live-streamed content is not Internet content for the purposes of Schedule 5. If streamed content were accessed from a library or archive of past live-streamed content, however, it would be considered to be kept on a data storage device and therefore would classify as Internet content under Schedule 5.

The Review is not aware of live-streamed content providing offensive or illegal content. Submissions to the Review did not indicate that such services are widely available, and the ABA has advised that it has received only one complaint in relation to live-streamed material. The level of complaints about such content may indicate that offensive or illegal services are not common in this format, or that such content is not easily accessible.

Further, the practical implications of establishing a live-streamed service would suggest it would be at a significant commercial disadvantage to one involving the distribution of stored content. This might suggest that commercial factors will tend to limit the prospect of wide-spread development of such services.

5.3.3 Chat rooms

Clause 3 of Schedule 5 defines Internet content to mean, among other things, information that is kept on a data storage device and is accessed, or available for access, using an Internet carriage service. Chat rooms generally allow real time (or at least near real time) interaction between users and, as such, the content is not typically kept on a data storage device. In this context, chat rooms do not fall under the definition of Internet content under Schedule 5.

Users take part in Internet chat by registering a nickname or screen name for a particular chat room. In the chat room, the messages users type are shown instantly to every other member of the room. As well as chatting in a specific room, individuals can request and initiate private conversations with other members of a chat room. There are often facilities to break out into a private chat room and invite particular individuals to that chat room.

There is a large number of chat rooms, provided by major ISPs, companies running large websites or individuals. Chat rooms may be dedicated to particular interests, hobbies, news events or making contact with other users.

Many chat rooms use a technology called Internet Relay Chat (IRC), where, by downloading and using specific software, users are linked to the same computer (i.e. server) allowing them to have conversations with other users both locally and overseas. Chat is also available on individual web pages, which is a popular chat technology as specific software is not required to participate in Internet chat, however the speed at which chat 'postings' appear may not be as fast as IRC-based chat.

Chat services are particularly popular with young people, providing an opportunity for discussion of a range of issues and with a potentially large number of other users. However, there is concern that chat rooms can be used by adults with a sexual interest in children to make contact with them.

5.3.4 Regulatory measures to deal with spam and transitory content

As noted in the issues paper, the Scheme does not—and because it focuses on take-down notices, cannot—specifically apply to spam or transitory services. However, there are a number of measures to address such content, including some recent initiatives. These measures may be broadly applicable to spam and transitory content, or are specifically relevant to the particular types of such content.

Measures to deal with spam and transitory content

In relation to spam and transitory material in general, complaints may be made to the ABA about any Internet content linked or referenced in such material. If the content were found to be prohibited under the Scheme, it would be subject to the ABA take-down notices or referrals to filter makers as appropriate. The ABA's website promotes the ability for users to make complaints about linked or referenced content.[26]

Second, the telecommunications offences under the *Crimes Act 1914* have application to offensive spam or transitory services. Section 85ZE of the Crimes Act makes it an offence to intentionally use a carriage service in a manner that is menacing, harassing or offensive. This could include the distribution of pornography or paedophile activity. On 14 March 2004, the Minister for Justice and Customs and the Minister for Communications, Information Technology and the Arts also announced new offences for the possession and distribution of Internet child pornography. These offences complement state and territory offences related to production and possession of child pornography, and attract penalties of up to ten years imprisonment.

Third, greater use of filters could significantly reduce problems associated with spam and transitory content. ISPs already make available Internet content filtering software on a cost-recovery basis under the registered Internet industry codes. A number of commercially available filters can be configured to block specified personal information from being posted in chat rooms (e.g. full name, school and address), and filters may block access to portals which provide access to streamed content that is offensive. In relation to spam filtering, on 23 July 2003 the then Minister for Communications, Information Technology and the Arts announced that the Australian Government would work with the Internet industry to develop relevant codes of practice building on initiatives such as the IIA's 'No Spam' campaign. Since April 2003, this campaign has enabled users to access anti-spamming filters for a free month's trial.

Measures to specifically deal with spam

As part of their community education activities, the ABA and NetAlert have produced materials on dealing with spam which can be accessed from these organisations' websites. Specifically, the

26 See for example *www.aba.gov.au/internet/faqs/spam.htm#spam.*

organisations' brochures advise users to safeguard their email addresses and not to respond to unsolicited email as this informs the sender that the address is active. Users are also advised to contact their ISP in relation to spam email, as ISPs are required under the industry codes to provide information about managing unsolicited email that promotes offensive content. The brochures also promote the use of anti-spam filtering software.

In addition to the above measures, the Australian Government has introduced a range of anti-spam measures, aimed to provide protection against spam. These include prohibiting spam from being sent from Australia, minimising spam for Australian-end-users and extending Australia's involvement in worldwide anti-spam initiatives. Specifically, the anti-spam measures include:

- national legislation, the *Spam Act 2003*, effective from 11 April 2004, enforced by the Australian Communications Authority (ACA), prohibiting the sending of commercial electronic messaging without the prior consent of end-users unless there is an existing customer-business relationship (an opt-in regime)
- civil sanctions for unlawful conduct including financial penalties, an infringement notice Scheme and the ability to seek enforceable undertakings and injunctions
- the requirement for all commercial electronic messaging to contain accurate sender details and a functional 'unsubscribe' facility to enable people to opt-out
- banning the distribution and use of email 'harvesting' or list-generating software
- working with national and international organisations to develop global guidelines and cooperative mechanisms to combat the global spam problem.

Measures to specifically deal with chat rooms

The ABA's and NetAlert's community education activities include providing advice in relation to Internet chat. To this end, the organisations have released brochures highlighting 'stranger danger' and the potential for paedophiles to use chat facilities to gain the confidence of children. Parents are advised to discuss stranger danger with their children, use software filters that can block specified personal information being sent, and develop household rules for using chat facilities. The brochures also provide the Internet addresses for further Internet chat safety materials, such as the United Kingdom-based community education group Childnet International's Chatdanger website: *www.chatdanger.com*.

It is important to note that predatory behaviour in Internet chat rooms will not necessarily involve the distribution of offensive content that would be prohibited under Schedule 5. Moreover, chat rooms are often private, and the conduct of parties participating in chat rooms cannot be determined by simply assessing the nature of the content of communications. Research also indicates that while a predator's initial contact with a child may be through a chat room, this contact may quickly move to email, text messaging via mobile phones or voice contact via a fixed or mobile phone.[27] The Scheme is clearly unsuited to addressing online predatory behaviour and is not capable of covering offline contact.

27 Carr, John, 2002, 'Child Sex Abuse and the Internet', NetSafe: Society, Safety and the Internet, Conference Proceedings 10–12 February, p. 2. Accessible at: *www.cs.auckland.ac.nz/~john/NetSafe/Proceedings.html.*

Overseas jurisdictions are introducing measures to strengthen the capacity of law enforcement agencies to deal with online paedophile activity. In the United Kingdom, for example, the *Sexual Offences Act 2003* establishes new offences for 'grooming' of children by paedophiles, including that which takes place on the Internet.[28] Grooming is where a paedophile makes contact with a potential victim and uses a range of techniques to gain their trust and develop a relationship with the intention of sexually abusing them.

In Australia, it is generally the case that state and territory law enforcement agencies will have both the expertise and investigative powers necessary to assess and act on cases of predatory behaviour or grooming. The Australian High Tech Crime Centre (AHTCC) has been established to provide a national coordinated approach to combating high tech crimes, including sexual crimes, especially those beyond the capability of single jurisdictions.

The AHTCC is located at the Australian Federal Police Headquarters in Canberra and includes representation from all Australian Federal, state and territory police forces. It aims to leverage the capabilities of each member agency by coordinating law enforcement efforts, conducting and coordinating investigations, gathering intelligence and liaising with relevant government agencies. Where appropriate, matters are investigated by a team including a combination of federal, state or territory police or other agencies as required. The website of the AHTCC can be accessed at: *www.ahtcc.gov.au*.

A number of states and territories have established units for investigating crimes involving computers, including sexual crimes. For example, in July 2003, the New South Wales Police announced the establishment of the Child Exploitation Internet Unit to target child exploitation and serial sex abuse committed through or linked to the Internet. In the Northern Territory, the Northern Territory Police Computer Crime Unit investigates crimes where a computer is used in the commission of an offence or where a computer may contain evidence relating to an offence. The Unit also provides computer examination support to the Northern Territory Police Sex Crimes Unit.

In addition, the Parliamentary Joint Committee on the Australian Crime Commission has conducted an inquiry into trends in cybercrime, with particular reference to child pornography and associated paedophile activity, among other things. The inquiry received 31 submissions, including from a number of state and territory police authorities. A final report was tabled on 24 March 2004 and is available from *www.aph.gov.au/Senate/committee/acc_ctte/cybercrime/report/index.htm*.

Obligations on carriers and carriage service providers to do their best to prevent telecommunications networks and facilities from being used to commit offences—such as predatory paedophile behaviour in chat rooms (where it may constitute a criminal offence)—are imposed under Part 14 of the *Telecommunications Act 1997*. Carriers and carriage service providers are also required to give officers and authorities such help as is reasonably necessary for enforcing criminal law. This could include ISPs (as carriage service providers) providing assistance where law enforcement authorities request

28 The *Sexual Offences Act 2003* received Royal Assent on 20 November 2003 and is due to be implemented in May 2004. See *www.homeoffice.gov.uk/justice/sentencing/sexualoffencesbill*.

help in dealing with possible criminal behaviour by chat room participants. ISPs can provide assistance by supplying law enforcement authorities with telecommunications data about Internet chat room sessions (such as time and place of session) and access to the content of communications if an interception warrant is issued under the *Telecommunications (Interception) Act 1979*.

Key findings—spam and transitory content

Spam and transitory content such as live-streamed material or online chat are not specifically covered under the Online Content Co-regulatory Scheme, largely because these activities are not suited to regulation by a content scheme. Nevertheless, complaints may be made about Internet content associated with such material, and greater publicity should be given to the application of the Scheme in this regard.

The Australian Government has announced new offences for the possession and distribution of Internet child pornography. These offences will update and broaden offences under section 85ZE of the *Crimes Act 1914*, which make it an offence to use a carriage service in a menacing, harassing or offensive manner, and will strengthen child protection regulation of the Internet.

Increased use of filters could significantly reduce the problems associated with spam and transitory content, by blocking spam or certain streamed material, or prohibiting the sending of specified personal information.

The Australian Government has introduced a range of anti-spam measures, including legislation, to provide protection against spam by prohibiting it from being sent from Australia, minimising spam for Australian end-users and extending Australia's involvement in worldwide anti-spam initiatives. This approach is likely to be more effective than seeking to address this problem through amendments to Scheme.

Under the Scheme, the ABA and NetAlert play a valuable role in educating children and carers about the dangers of predatory behaviour within Internet chat rooms. The state and federal police, however, are the organisations with the necessary investigative and arrest powers to actively intervene to prevent such behaviour. ISPs should also be encouraged to cooperate with law enforcement agencies in relation to chatroom safety and this issue should be considered in the context of the current review of the IIA Codes.

5.4 Usenet newsgroups

A newsgroup is a global electronic noticeboard to which users may post material that can be accessed by all other readers of the newsgroup. Newsgroups usually specialise in a particular subject matter or a particular group of users. The majority of newsgroups are text-based, however, there are mechanisms for including pictures or other content. Often, the term Usenet newsgroups is used in the context of the Internet because of the technical network the groups use.

As postings on Usenet newsgroups are Internet content for the purposes of Schedule 5, the ABA uses its powers to issue take-down notices in relation to complaints about such material found to be prohibited. In its submission to the Review, the ABA stated that it is currently considering whether it would be practical to also implement arrangements whereby the Internet industry would not host Usenet groups known to contain significant amounts of paedophile material.

> While Usenet newsgroups have accounted for a relatively small proportion of complaints to the ABA, the ABA has stated that it is aware that a significant amount of child pornography is distributed through a small number of such groups. The highly transient nature of newsgroup content generally and the fact that many ISPs host such content, have created some difficulties in administering the complaint mechanism in relation to such content. In particular, the requirement that the ABA be satisfied that an ISP is hosting such content prior to issuing a take-down notice limits the ABA's capacity to take action in relation to content that may be simultaneously hosted by many ISPs. (ABA submission, p. 25)

On 13 November 2002, the United Kingdom-based complaints hotline Internet Watch Foundation (IWF) announced that it had identified 51 newsgroups known to contain significant amounts of child pornography, and a further 25 groups with names that appeared to advertise such material.[29] While content is not controlled by ISPs, copies of articles posted to newsgroups sit on every server that carries the group. There are estimated to be several hundred-thousand such servers globally.

The IWF released a discussion paper on its policy in relation to newsgroups.[30] While the paper notes that prohibiting the hosting of paedophile newsgroups would be likely to result in regulatory avoidance by paedophiles, it states that removing only a few of the thousands of available newsgroups would significantly reduce the size of the newsgroup problem.

The Review considers that prohibiting the hosting of selected paedophile newsgroups would support the objects of the Scheme, particularly in restricting access to certain Internet content that is likely to cause offence to a reasonable adult (paragraph 3(1)(l)). The IWF has developed a policy of recommending to ISPs that they not host newsgroups known to regularly contain significant amounts of child pornography. 'Regularly' is defined to mean finding an average of at least one per cent of images viewed to be illegal and additionally applying a test whereby in each of six consecutive monitoring rounds finding any illegal content. IWF has also compiled a list of newsgroups that have names that appear to advertise or advocate paedophile content or activity. More information on the practical operation

29 See *www.iwf.org.uk*
30 See *www.iwf.org.uk/about/policies/newsgroups.html*

of the IWF's newsgroup policy, including statistical analysis on the assessment and monitoring of newsgroup content, can be found at the IWF's website: *www.iwf.org.uk*.

The ABA could explore the potential for, and workability of, a voluntary scheme for Australian hosted Usenet groups. The ABA could utilise its existing relationship with IWF and the European hotline forum INHOPE to assist in developing the newsgroup lists. It would be possible for the Internet industry, through its codes of practice, to undertake not to host newsgroups notified by the ABA.[31] The ABA could implement transparent and independently audited systems for newsgroups that it notifies, and only accept referrals from counterpart hotlines that meet minimum standards. Should adequate amendments not be incorporated in the industry codes, consideration should be given to making 'online provider determinations' in this regard or amending Schedule 5 to require the ABA to make a compulsory industry standard.

Key findings—Usenet newsgroups

The ABA should continue to use its powers to issue take-down notices in relation to complaints about Usenet newsgroup content found to be prohibited under the Scheme.

During the review of the Internet industry codes, the industry should amend the codes to require ISPs not to host newsgroups that are notified by the ABA to regularly contain paedophile material.

5.5 Racist content

In its submission to the Review, the Human Rights and Equal Opportunity Commission (HREOC) argued that 'cyber-racism' has implications for the operation of Schedule 5. It argued that racist Internet material impedes the Online Content Co-regulatory Scheme objective to protect children from unsuitable Internet content. To this end, HREOC submitted:

> [T]he Australian Broadcasting Authority, which is the principle agency responsible for Internet content regulation in Australia under Schedule 5 of the *Broadcasting Services Act 1992*, is unable to act on complaints about racist Internet material even though the material is potentially unlawful under the *Racial Discrimination Act 1975*.
>
> Schedule 5 of the *Broadcasting Services Act 1992* vests the ABA with authority to investigate complaints about Internet content. The classificatory standards administered by the ABA (and the Office of Film and Literature Classification) do not deal with racially offensive material, however. Accordingly, racist material is not generally prohibited by the Internet content regulatory framework, even though such material may be unlawful. (HREOC submission, p. 3)

As noted above in section 4, when introducing the Scheme, the Australian Government was concerned to ensure that Internet content regulation is consistent with the content regulation applied to offline services. To this end, Internet content regulation was aligned with the regulation that applied to narrowcast subscription television services where, based on the national classification scheme administered by the Office of Film and Literature Classification (OFLC), RC and X material

31 While clause 60 of Schedule 5 sets out the matters to be addressed by the industry codes and does not include specific reference to regulating Usenet newsgroups, subclause 60(9) provides that the matters dealt with by industry codes and standards are not limited by Schedule 5. To this end, there would be no impediment under Schedule 5 to including provisions about Usenet newsgroups in the industry codes.

are prohibited and R material is required to be restricted to adults. The Scheme does not provide for more onerous restrictions than those that apply to conventional media.

HREOC does not suggest any specific changes to the Scheme to address the problems it identifies. The Scheme's capacity to address racist content relates to the classification of Internet content by the Classification Board, which is supported by the OFLC.

Under the national classification scheme, the National Classification Code or the classification guidelines can be amended on the agreement of all Censorship Ministers. In early 2003, the OFLC completed a review of the classification guidelines for films and computer games in accordance with the review process agreed to by Censorship Ministers. Censorship Ministers subsequently agreed to new combined guidelines for films and computer games, which came into effect on 30 March 2003.

While the combined guidelines do not include specific provisions on racial vilification, the National Classification Code provides that films and computer games that promote, incite or instruct in matters of crime or violence are to be refused classification. In addition, the Code sets out a number of principles. These principles include: that adults should be able to read, hear and see what they want; that everyone should be protected from exposure to unsolicited material that they find offensive; and the need to take account of community concerns about depictions that condone or incite violence and the portrayal of a person in a demeaning manner. If HREOC wishes to pursue a more prescriptive approach to the national classification scheme, it may wish to make a submission to Australian Government, state and territory Censorship Ministers on the issue.

On 14 March 2004, the Minister for Communications, Information Technology and the Arts and the Minister for Justice and Customs, announced that the offence of using a telecommunications service in an offensive, menacing or harassing manner—which currently applies to email and telephone services—will be extended to cover website material. The new offence would carry a penalty of two years imprisonment, double the punishment for the existing offence, to reflect the seriousness with which the Australian Government views this conduct. The new offence could in principle apply to racial vilification on the Internet, and forms part of a package of new telecommunications-related offences which include offences for the possession and distribution of Internet child pornography (see section 5.3.4).

Key finding—racist content

The Online Content Co-regulatory Scheme relies on classification decisions of the Classification Board, which is supported by the OFLC. The Classification Board makes its decisions in accordance with the National Classification Code and classification guidelines, as agreed to by Commonwealth, States and Territories. Changes to the Code or the classification guidelines require the agreement of all participating jurisdictions. As such, HREOC may wish to consult Censorship Ministers about the treatment of racist material in the national classification scheme. Such an approach would ensure that online content continues to be treated in the same manner as content in other media.

5.6 Developments in convergent devices

The issues paper sought comment on the potential impact convergent devices may have on the operation of Schedule 5. It noted that a number of devices—including certain video game consoles, Internet appliances, personal digital assistants and 3G mobile phones—may allow access to a range of services, including Internet content and other audiovisual content. In addition, these devices may not accommodate end-user filtering or a suitable alternative access arrangement. For practical purposes, the issues paper noted:

> Some but not all of these devices include parental access control technologies and in some cases the display format requirements limit general access to the Internet in favour of certain customised sites. In the cases of devices with limited storage or software-loading capacity, filtering can be addressed at the service provider level through the use of filtered proxy servers offering an alternative safe service to subscribers. It should also be noted that the screen size constraints of palm pilots and mobile phones are not well-suited to viewing offensive graphics content and that this may naturally limit the proliferation of such material on these platforms. (Review issues paper, p. 20)

In this context, the IIA and Childnet recommended monitoring of relevant technology and service trend developments.[33] The Australian Consumers' Association recommended that where devices are sufficiently sophisticated to store and display offensive content, protective measures should be put in place including encouraging industry to provide user control of unacceptable content (p. 5). The ABA recommended monitoring of developments and consideration of ISP-level filtering:

> In relation to video game consoles and other (non-personal computer) devices that allow connection to the Internet, the ABA considers that concerns about access to inappropriate content could be addressed through the use of ISP-level filtering if necessary. The ABA would support measures to encourage ISPs to provide the choice of such a service to users of these devices.
>
> With mobile Internet technologies yet to be widely used in Australia, the ABA proposes that the implementation of such services be closely monitored by appropriate regulatory agencies, and that such bodies seek information from relevant overseas bodies about the handling of such issues in markets where these services have operated for a period of time. The ABA also would propose that Internet safety concerns associated with mobile devices be addressed through codes of practice for the providers of such services, and through the provision of information to users about the potential risks associated with such technologies. (ABA submission, p. 14)

32 See submissions by Childnet and the Internet Industry Association.

5.6.1 Premium rate number services

Premium rate number services are those which charge the end-user for the delivery of content that is usually sourced from a third-party content provider and accessed via a telecommunications carriage service. These services have been described as an early example of a convergent service.

There are approximately 15.5 million mobile phones in use in Australia, most of which are able to send and receive text messages using SMS. Premium rate SMS can be used for a wide variety of purposes, including competitions, voting for television shows or interactive 'chat' services. Consumers with 2.5G and 3G phones will be able to send and receive still images and access the Internet. Consumers with 3G phones will also be able to access audiovisual content.

New premium rate mobile services will expand customer choice and are expected to provide significant growth in the revenues generated from the use of mobile phones. In particular, the development and supply of premium rate audiovisual services on mobile phones may be an important driver for the take up of 3G phones.

The ability of 2.5G and 3G mobile devices to connect to the Internet and deliver audiovisual content via other technical means raises potential content access and safety concerns, particularly given the popularity of the Internet and mobile phones amongst young people. Overseas experience indicates that adult content and services are likely to be offered as take-up of the technology increases.

The mobility, 'always on' and location tracking features of mobile technology also create opportunities for children to have contact with people they do not know, exacerbating the potential dangers to children currently posed by Internet chat rooms. In this context, it should be noted that the Crimes Legislation Amendment (Telecommunications and Other Offences) Bill 2004 contains proposed offences relating to the use of a carriage service (which would include the Internet and 3G mobiles) to groom and procure children for the purposes of engaging in sexual activity. As noted elsewhere, these provisions will update and broaden current provisions under section 85ZE of the *Crimes Act 1914*.

5.6.2 Regulatory status of service providers' content via convergent devices

The *Telecommunications (Consumer Protection and Service Standards) Act 1999* requires that personal identification numbers (or some other appropriate access control) be used for the supply of premium rate telephone sex voice services. Access control regulation for telephone sex services differs from the content classification/ complaints procedure model that applies to the content of broadcasting services under the *Broadcasting Services Act 1992*.

The *Telecommunications Act 1997* empowers the ACA to make a determination setting rules to apply to service providers on matters specified in regulations. These matters could include access to content of telecommunications carriage services.

A key issue for the treatment of content delivered via convergent devices is whether the content falls under the definition of Internet content in Schedule 5. Clause 3 of Schedule 5 defines Internet content to mean information that is kept on a data storage device and is accessed, or available for access, using an Internet carriage service (excepting ordinary electronic mail or information that is transmitted in the form of a broadcasting service).

Where a content service provider is offering stored content via an Internet carriage service, the material is Internet content for the purposes of Schedule 5. The nature of the access device (whether it is a PC, games device or 3G mobile phone) does not affect the question of whether the content is regulated by Schedule 5, provided information can be reproduced from the particular device, either with or without the aid of any other article or device. Accordingly, complaints could be made about Internet content accessible via a convergent device, and the ABA could issue take-down notices in relation to Australian-hosted content that it finds to be prohibited.

However, where service providers make audiovisual content available in a closed network environment or by accessing a MMS, the material will not be Internet content unless the particular access system used can be characterised as an 'Internet carriage service'. Under clause 3 of Schedule 5, an Internet carriage service must enable access to the Internet.

5.6.3 Options for regulating service providers' content via convergent devices

On 21 April 2004, the Minister for Communications, Information Technology and the Arts announced that he intends to require the ACA to put in place interim measures to provide appropriate consumer protections as carriage service providers make available new premium rate content services, including audiovisual content, on their networks.

These interim measures would be implemented through Regulation 3.12 of the *Telecommunications Regulations 2001* which gives the ACA powers to make service provider determinations on the supply of, and access to, premium rate services. These arrangements would also put in place sufficient controls so that inappropriate content cannot be accessed on new mobile services, while avoiding prescriptive regulation.

Further to these interim measures, a broader review should be made of the range of regulatory arrangements for content delivered over convergent devices (particularly mobile phones) which could consider:

- the scope of existing regulatory frameworks
- given the nature of the new services and the manner of their delivery, whether adequate measures exist to restrict access (particularly by children) to potentially offensive content and to address child safety concerns
- the extent to which additional measures are necessary or appropriate.

At the same time, the current review of the IIA Codes is an appropriate time to consider how well the codes address Internet content delivered on convergent devices and particularly mobile phones.

Key findings—development of convergent devices

While the Department, the ABA and NetAlert have an ongoing role in monitoring technological and market developments in convergent devices, there is a need to ensure that appropriate protections are in place for end-users, especially children, who may access this audiovisual content as it becomes available on convergent devices.

In the short-term, these protections may be achieved in relation to content delivered on SMS and MMS through service provider rules imposed under the *Telecommunications Act 1997*. In the longer term, a review should consider whether future regulatory arrangements are required and take into account the nature and availability of these and other new and emerging services. The review would be most appropriately conducted by the Department in consultation with the ABA, the ACA, industry and other stakeholders.

The current review of the IIA Codes should also consider the means for ensuring appropriate access management controls for Internet content delivered on convergent devices, especially Internet enabled 3G mobile phones

There is also a need to ensure that effective coordination mechanisms are in place between the ABA, appropriate law enforcement agencies and other relevant agencies in the event that the ABA receives complaints about convergent devices being used illegally for menacing purposes, including to address child safety issues.

5.7 Research into filters and associated technologies

The general developments in filtering technologies since the introduction of the Scheme, particularly in relation to server-side filtering, are considered separately in section 5.1 of this report.

Clause 94 of Schedule 5 empowers the ABA to conduct and commission research into issues relating to Internet content and Internet carriage services. It also empowers the ABA to inform itself and advise the Minister on technological developments and service trends in the Internet industry.

5.7.1 Filter effectiveness study

As noted in section 3.5 of the issues paper, in March 2002 NetAlert and the ABA released a jointly commissioned report into the effectiveness of existing filtering software. Entitled *Effectiveness of Internet filtering software products*, the report examined 14 software products. It found that the performance of filters varies substantially, with a key determinant of effectiveness being the type of blocking technique used by the filter.

The ABA submitted to the Review that of the 14 tested filtering products, those products that combined two or more filtering techniques generally performed better in the testing (ABA submission, p. 36). Eight of the products tested blocked in excess of 80 per cent of content that would be expected to fall within the R, X and RC classifications, although significant amounts of innocuous content also were blocked in most cases. Based on the findings, the ABA assessed the general effectiveness of types of filtering tools as follows.

> As is to be expected, products that employ 'inclusion filtering' (or 'whitelists') are the most efficient at blocking offensive content, as they allow users to access a preselected set of sites that have been assessed for their suitability. However, as a consequence, they also block a significant amount of content that may not necessarily be offensive. Filter products and services that employ this technique are likely to be most suitable for families with younger (primary school age) children, for whom access to the wider Internet may be less important than ensuring they are protected from harmful content.
>
> Products based on URL and keyword 'blacklists' are effective in blocking particular types of unwanted content in most cases. The research indicates that products that employ human verification of 'blacklist's tend to be the more accurate in blocking offensive content, and are less likely to block access to suitable content. Filters of this type are likely to be more suitable for families with older children, with requirements to access a broader range of content. (ABA submission, p. 36)

An important facility of many filters is the capacity to configure the filtering level to the age of the user. For example, young children might only be allowed access to approved sites ('whitelist'), while an older child might be allowed access to the full Internet but with a filter setting which effectively blocks most unsuitable content ('blacklist'). A higher degree of risk management might be appropriate for adolescent users for whom a high level of blocking might become an incentive to circumvent the technology.

Since publication on the ABA's and NetAlert's websites, the report has been downloaded approximately 30 000 times by Internet users in Australian and overseas. Such research is a valuable tool for Internet users and wide, user-friendly publication of the results would assist Internet users in selecting a filter that meets their requirements.

In view of ongoing developments in filtering technology, it may be timely to conduct further evaluation of the effectiveness of filter products. In this context NetAlert could participate in an Internet content filtering trial that is proposed to be a component of an extended Launceston Broadband Project (LBP). The LBP is being implemented via an agreement between the Australian Government and Telstra. Through the provision of subsidised ADSL access to the Launceston community and the operation of Telstra's Multimedia Development Laboratory a unique broadband testbed has been established to allow for the trialing of applications. NetAlert's participation in the Internet content filtering trial would provide a useful opportunity for it to examine Internet content filtering technologies and their performance in a controlled broadband environment.

5.7.2 Designated notification scheme

A key issue for the Scheme is the effectiveness of the designated notification scheme dealing with prohibited overseas-hosted content. As noted in section 2.3.2 above, the industry codes of practice require the ABA to notify prohibited overseas-hosted content to the makers of filters listed in the Schedule to the codes. The makers of these filters have agreed to

update their filter to give effect to the ABA notifications so that the filter will subsequently block the content. The code requires Australian ISPs to provide one of the scheduled filter products to their subscribers at no more than the cost of obtaining, supplying and supporting the filter.

To inform the Review process, the ABA commissioned the CSIRO to test that scheduled filters block content already subject to notifications by the ABA. While delays in processing notifications for recently notified content may explain a minor failure rate, the ABA submission noted that that certain products failed to block a significant proportion of the notified content (ABA submission, pp. 6–7). The Review welcomes the ABA's proposal to recommend to the IIA that these products be removed from the schedule to the codes unless performance of the products can be resolved to the ABA's satisfaction. It would be appropriate for the ABA to examine taking action in this regard during review of the industry codes. It is crucial to an end-user filtering regime that each product listed in the industry codes reflects the notifications of prohibited content with only a minor degree of failure.

To this end the Schedule of filters in the codes of practice should be subject to regular review to assess the compliance of these filters. The ABA should ensure that the enforcement regime is credible and effective, with sanctions for failing to comply with ABA notifications, including de-listing in the case of significant or recurrent failures. In the case of less significant failures, filters should be retested within six months of the initial testing. Failure to comply in this subsequent testing would result in de-listing.

Under clause 65 of Schedule 5, any change to the industry codes must be made by replacing and re-registering of the codes. While paragraphs 62(1)(e) and (f) provide that where changes are of a minor nature the codes will not need to go out for public consultation, a requirement to re-register the codes more regularly on the basis of amendments to the Scheduled filter list would nonetheless unduly increase the regulatory burden. Consideration should be given to amending clause 65 to allow for a schedule of filters to be updated separately to the codes, on the basis of approval by the ABA.

Key findings—research into filters and associated technologies

NetAlert should commission regular assessments of filtering and associated technologies, and widely promote this information in user-friendly brochures and reports as part of its community education and advisory role.

The ABA should conduct regular reviews of the filters listed in the schedule to the industry codes of practice, and actively enforce filters' compliance with the designated notification scheme.

Clause 65 of Schedule 5 could be amended to provide for the ABA to regularly update the filtering schedule separately to replacing the codes.

5.8 Monitoring of industry codes

Section 5.1 above identified as an option that filtering requirements in the industry codes of practice be amended to increase community education and/or to require ISPs to provide filters on an opt-out basis. These amendments would increase the community safeguards of the Scheme.

The issues paper provided detailed information about the industry codes, including the IIA's 'Look for the Ladybird' seal for ISPs that are code compliant (sections 2.3.1 and 3.2). Codes are effective regulatory instruments in a rapidly evolving sector such as the Internet industry as they can be more regularly updated than legislation or regulations to reflect technical or market developments. Codes also set transparent standards of behaviour that the public should expect to receive from the industry. In a co-regulatory framework such as the Scheme, where the codes are underpinned by legislative enforcement powers, codes provide certainty in relation to industry performance.

In December 1999, the ABA registered three codes developed by the IIA in consultation with the community and industry. The ABA registered the codes, which took effect on 1 January 2000, after consideration of a number of factors including whether consultation had been undertaken with the community, industry and the community advisory body, NetAlert, and whether the codes contained appropriate community safeguards.

The IIA content codes 1 and 3 deal with a range of customer advice and content management issues. Specific provisions include procedures for ensuring online accounts are not provided to children without the consent of a parent, teacher or responsible adult, for creating awareness about the way to make a complaint about Internet content, and for informing producers of Internet content of their legal responsibilities in relation to that content. Content code 2 details the designated notification Scheme for dealing with overseas-hosted prohibited content, as discussed in the previous section.

In March 2001, the ABA registered replacement codes that contained minor amendments to the list of Scheduled filters. In May 2002, the ABA registered further revised codes, which replaced the provision allowing ISPs to determine the charge for filtering services with a requirement that, where ISPs seeks to charge for a filter, they must not charge more than the cost of obtaining, supplying and supporting the filter.

The ABA recommended monitoring and regular review of the Internet industry codes to ensure they meet their objectives (ABA submission, p. 10). The Review supports this recommendation for the reasons outlined above.

Key finding—monitoring of industry codes

Internet industry codes should be reviewed at least every three years to ensure the Scheme appropriately deals with technological and market developments.

5.9 International liaison

When the then Minister requested the Department to undertake the required review of the Online Content Co-regulatory Scheme, he requested that international liaison under the Scheme be examined.

Clause 94 of Schedule 5 empowers the ABA to liaise with regulatory and other relevant bodies overseas about cooperative arrangements for the regulation of the Internet industry including collaborative arrangements to develop multilateral codes of practice and Internet content labelling technologies. In performing this function the ABA has participated in a range of relevant policy and regulatory forums.

Through the ABA, Australia is an associate member of INHOPE. Partly funded by the European Community's Safer Internet Action Plan, INHOPE members deal with complaints about illegal Internet content, predominantly child pornography. INHOPE members include hotlines from Austria, Belgium, Denmark, France, Germany, Iceland, Republic of Ireland, the Netherlands, Sweden, Spain and the United Kingdom, with the Cybertip Line in the United States also an associate member.

Among other things, INHOPE provides a forum for exchange of information in relation to hotline operation, including complaint investigation techniques and occupational health and safety, particularly for the officers who deal with Internet content subject to complaints. INHOPE is overseeing the member hotlines' implementation of the ART1 and ART2 hotline management principles, which establish six criteria for effective hotlines: availability, reliability, transparency, accountability, responsibility and whether the hotline is trustworthy.

The ABA submission provided detailed information about the ABA's complaints hotline in relation to each of these criteria (ABA submission, pp. 18–21). These criteria, together with making available data relating to the processing of Internet content complaints, provide an appropriate framework for assessing the performance of the ABA's Complaints Hotline. In the context of the ART1 and ART2 principles, the Review notes that the ABA intends to undertake a number of refinements to the operation of the hotline, including:

- increasing the amount of information about the hotline provided in community languages
- greater prominence of the hotline on popular search engines
- an advertising campaign promoting the hotline and general Internet safety information
- placement of a link to the ABA's privacy policy on the complaint form itself
- expanded information about the complaint investigation process, including graphical illustration of the ABA's investigation procedures and sample investigation reports.

The ABA has been represented on the Bertelsmann Foundation's International Network of Experts on Content Self-Regulation since 1999. This group is a forum for the development of regulatory models for Internet content, and assisted in the development of the ART1 and ART2 principles for evaluating hotline operation. Participation in other forums, including Internet hotline workshops and EC filter technology workshops will further assist in maintaining international

cooperation to manage content in the international context of Internet regulation.

The Review notes the submissions by the United Kingdom-based organisations Childnet International and Internet Content Rating Association (ICRA). Childnet expressed support for Australia's international involvement in online regulation forums, and recommended this involvement continue.

> It has been a feature of Australia's work on internet content regulation that the agencies involved have been very concerned to learn internationally and to share their own experience. We have already commented on the ABA's involvement with INHOPE, and we would commend them for not letting distance prevent them from taking a valuable role. For example, ABA staff have played an important part in INHOPE's working groups especially that looking at issues of illegal content and new technological developments. We welcome cooperation with NetAlert as we have with other bodies, and we are looking forward to exchanging good practice and contacts, and sharing resources at their conference.
>
> Since the Australian legislation was introduced in 1999, discussions about Internet content regulation worldwide have not decreased. Indeed, the Australian model has become one of the approaches for countries to consider and compare themselves against. (Childnet submission, p. 4)

ICRA is a non-profit organisation with the aim of enabling parents to protect their children from potentially harmful Internet material while protecting the free speech of online content providers. ICRA has developed and provides free of charge a filtering system based on content labelling, which enables content producers to label content and users to select the type and level of content they would like to filter.

ICRA submitted to the Review that it is working with the ABA to develop a template that would enable parents to select a pre-defined level of content along the lines of the categories of the existing OFLC-administered national classification Scheme. ICRA recommended that the ABA build on its linkages with international organisations, particularly ICRA itself.

> The ABA has had a very lengthy and supportive role in the emergence of ICRA both as a system and as an organization. We have enjoyed good working relationships with a number of senior officials of the ABA since 1996 and the ABA's input has been critical in establishing ICRA as a credible and effective labelling Scheme.
>
> What we would like to propose is that we build on these informal relationships to create a more formalized co-operation so as to assist the ABA in developing your Scheme beyond what it currently has to offer. While parents rightly are concerned about the content covered by the ABA Scheme, there is a much wider body of material that also concerns them which is currently not covered by the Co-Regulatory regime. This includes legal material, but which is potentially harmful, particularly to young children. Examples of this include 'soft' porn, violent sites (such as online computer games), sites promoting alcohol, tobacco, guns and gambling. In addition, chat sites, which are perfectly legal, however contain potential dangers for children. All of this legal material can also be seen as harmful by parents. The ICRA system includes all and more of these in its labelling vocabulary. And the ICRA filter provides a means to filter out any or all of these categories of content. We feel that the ICRA system could be of enormous

> benefit the current ABA Scheme, complimenting it in the areas that the Scheme does not currently cover…
>
> More specifically, we would welcome a much greater involvement by the ABA in the future direction of the ICRA system. Likewise, we would like to see the ABA Scheme further enhanced through the promotion of the ICRA labelling system to all content providers in Australia, the creation of Australian-specific filtering templates and the promotion of the ICRA filter to parents, teachers and librarians within Australia. With these measures in place, we believe Australian parents will have a comprehensive range of tools to ensure their children enjoy a safe, educational and entertaining experience online, whether at home, at school or out and about. (ICRA submission, pp. 6–7)

If broadly taken up and applied to the Australian context by labelling content consistently with the OFLC-administered national classification scheme, the ICRA system would assist Australian users in choosing content that is appropriate for them and their children and, therefore, provide greater community safeguards. In this context, the Review notes that Australian Children's Television Foundation's submission that there should be a uniform, technology neutral approach to the classification of media, utilising the existing Australian classification categories for Internet content (Australian Children's Television Foundation submission, p. 5).

The ABA's involvement in the ICRA scheme seems entirely appropriate. It would also seem desirable for the Internet industry to support this initiative and to encourage Australian Internet content developers to contribute to the take-up of this scheme by appropriately labelling their content.

Key findings—international liaison

ABA participation in INHOPE and similar forums assists in the achievement of International best practice for administration of the ABA's complaints mechanism and should continue.

The ABA's participation in the exchange of information between hotlines within INHOPE is an important means of responding to some forms of illegal content not sourced from Australia.

The ABA and the Internet industry should promote the take-up of the labelling system developed by the Internet Content Rating Association and the modification of the system for the Australian context.

ATTACHMENT A

Abbreviations

ABA	Australian Broadcasting Authority
ABS	Australian Bureau of Statistics
ACA	Australian Communications Authority
the Act	the *Broadcasting Services Act 1992*
AHTCC	Australian High Tech Crime Centre
blacklist	filtering which blocks access to listed content
the Department	the Department of Communications, Information Technology and the Arts
HREOC	Human Rights and Equal Opportunity Commission
ICH	Internet Content Host
ICRA	Internet Content Rating Association
IIA	Internet Industry Association
INHOPE	International Hotline Providers in Europe Association
IP	internet protocol addresses—32-bit numbers identifying points on the Internet
IRC	Internet Relay Chat
ISP	Internet Service Provider
IWF	Internet Watch Foundation
MB	Megabyte
NOIE	National Office for the Information Economy
OFLC	Office of Film and Literature Classification
PC	personal computer
R	established under the *Classification (Publications, Films and Computer Games) Act 1995*—it is explained in the National Classification Code
RC	established under the *Classification (Publications, Films and Computer Games) Act 1995*—it is explained in the National Classification Code

the Scheme	the Online Content Co-regulatory Scheme, established by Schedule 5 to the *Broadcasting Services Act 1992*
spam	unsolicited (commercial) electronic messages
URL	uniform resource locators—alpha-numeric web addresses
whitelist	filtering which allows access to predetermined lists of content
X	established under the *Classification (Publications, Films and Computer Games) Act 1995*—it is explained in the National Classification Code

ATTACHMENT B

Submissions to the review

The then Minister for Communications, Information Technology and the Arts issued a press release on 27 September 2002 inviting submissions to the review and advising of the release of the issues paper.

Twenty-six submissions were received and posted on the Department's website, from the following individuals and groups:

LIST OF SUBMISSIONS	DATE RECEIVED
1. Adultshop.com	8 November 2002
2. Austar	15 November 2002
3. Australian Broadcasting Authority	23 November 2002
4. Australian Children's Television Foundation	7 November 2002
5. Australian Consumers' Association	8 November 2002
6. Australian Library Information Association	15 November 2002
7. Australian Vice Chancellor's Committee	29 October 2002
8. Caradoc-Davies, Dr Ben	3 November 2002
9. Chen, Dr Peter	8 November 2002
10. Childnet International	8 November 2002
11. Communications Law Centre	15 November 2002
12. Convergent Communications Research Group	8 November 2002
13. Dimension Data	1 November 2002
14. Electronic Frontiers Australia Inc	9 November 2002
15. Federation of Australian Commercial Television Stations	8 November 2002
16. Griffith University	30 October 2002
17. Human Rights and Equal Opportunity Commission	15 November 2002
18. Internet Content Rating Association	20 November 2002
19. Internet Industry Association	15 November 2002
20. Internet Society of Australia	15 November 2002
21. NetAlert Limited	8 November 2002
22. Optus	18 November 2002
23. Redland Shire council	7 November 2002
24. Telstra	15 November 2002
25. Vodafone	15 November 2002
26. Young Media Australia	15 November 2002

Review of the operation of Schedule 5 to the *Broadcasting Services Act 1992*

September 2002

ISSUES PAPER

CONTENTS

Abbreviations

AAT	Administrative Appeals Tribunal
ABA	Australian Broadcasting Authority
the Act	the *Broadcasting Services Act 1992*
AFP	Australian Federal Police
Classification Act	the *Classification (Publications, Films and Computer Games) Act 1995*
the Department	the Department of Communications, Information Technology and the Arts
the Explanatory Memorandum	The Revised Explanatory Memorandum to the *Broadcasting Services Amendment (Online Services) Bill 1999*
FOI Act	*Freedom of Information Act 1982*
ICHs	Internet content hosts
ICRA	Internet Content Rating Association
IIA	Internet Industry Association
INHOPE	Internet Hotline Providers in Europe Association
ISPs	Internet services providers
NOIE	National Office for the Information Economy
OFLC	Office of Film and Literature Classification
PC	personal computer
R	Established under the *Classification (Publications, Films and Computer Games) Act 1995* – it is explained in the National Classification Code
RC	Established under the *Classification (Publications, Films and Computer Games) Act 1995* – it is explained in the National Classification Code
the Scheme	the Online Content Co-Regulatory Scheme, established by Schedule 5 to the *Broadcasting Services Act 1992*
SIAP	the European Union's Safer Internet Action Plan
spam	unsolicited bulk email
X	Established under the *Classification (Publications, Films and Computer Games) Act 1995* – it is explained in the National Classification Code

1 OVERVIEW

1.1 Required review

As set out in section 3 of the *Broadcasting Services Act 1992* (the Act), the objects of the Online Content Co-Regulatory Scheme are to:

- provide a means for addressing complaints about certain Internet content;
- restrict access to certain Internet content that is likely to cause offence to a reasonable adult; and
- protect children from exposure to Internet content that is unsuitable for children.

Under clause 95 of Schedule 5 to the Act, before 1 January 2003 the Minister for Communications, Information Technology and the Arts must cause to be conducted a review of the operation of Schedule 5, which establishes the Online Content Co-Regulatory Scheme.

Subclause 95(2) provides that the following matters are to be taken into account when conducting the review:

- the general development of Internet content filtering technologies;
- whether Internet content filtering technologies have developed to a point where it would be feasible to filter R-rated information hosted overseas that is not subject to a restricted access system; and
- any other matters relevant to Internet content regulation.

Subclause 95(5) requires that, in the event that filtering technologies are developed that can in practice prevent end-users from accessing overseas-hosted R-rated content not subject to a restricted access system, legislative amendments should be introduced to extend the prohibited content categories to include such R category overseas-hosted content.

The Explanatory Memorandum to the Broadcasting Services Amendment (Online Services) Bill 1999 also states that the review will assess 'the effectiveness of the framework in meeting objectives and providing sufficient deterrents against any irresponsible industry behaviour'.

The Minister for Communications, Information Technology and the Arts, Senator the Hon Richard Alston, has requested the Department of Communications, Information Technology and the Arts (the Department) to undertake the required review of Schedule 5. In addition, the Minister requested that the review examine Commonwealth community education initiatives under the Scheme.

1.2 Review process

The process for the review includes:

- preparation of an issues paper by the Department;
- posting of the issues paper on the Department's website with a call for submissions;
- contracting an independent technical expert to undertake the analysis of Internet content filtering technology required under clause 95 of Schedule 5;

- receipt and analysis of submissions;
- further consultation with key stakeholders;
- report to the Minister for Communications, Information Technology and the Arts; and
- tabling of the report in both Houses of Parliament.

This issues paper provides the central basis for public consultation in the required statutory review of the operation of Schedule 5. It sets out key issues to the operation of the Scheme, together with background information to assist submitters in considering the issues.

The Department invites comments on the general operation of Schedule 5 to the Act and, in particular, on the issues specifically identified in this paper.

1.3 Making a submission

Public submissions on the issues paper, preferably in electronic format, are sought by COB Friday 8 November 2002. Submissions may be emailed to *online.review@dcita.gov.au*. Alternatively, submissions may be faxed to 02 6271 1700 or sent on disk or hard copy to:

Manager, Broadcasting and Online Content

Department of Communications, Information Technology and the Arts

GPO Box 2154

CANBERRA ACT 2600

The Department proposes to post all submissions on its website unless otherwise indicated.

Contact Officers:

Rhyan Bloor	02 6271 1869
Matthew Pearce	02 6271 1204

2 BACKGROUND

2.1 Objects of the Act

The objects set out in section 3 of the Act specify the outcomes Parliament intended from the regulation of online services which are to:

- provide a means for addressing complaints about certain Internet content;
- restrict access to certain Internet content that is likely to cause offence to a reasonable adult; and
- protect children from exposure to Internet content that is unsuitable for children.

2.2 Regulatory policy

The regulatory policy applying to Schedule 5 is provided for in section 4 of the Act which sets out Parliament's intention that Internet content hosted in Australia, and Internet carriage services supplied to end-users in Australia, be regulated in a manner that:

- enables public interest considerations (particularly those relating to offensive or unsuitable Internet content) to be addressed in a way that does not impose unnecessary financial and administrative burdens on Internet content hosts (ICHs) and Internet services providers (ISPs);
- readily accommodates technological change;
- encourages the development of Internet technologies and their application and the provision of services made practicable by those technologies to the Australian community; and
- encourages the supply of Internet carriage services at performance standards that reasonably meet the social, industrial and commercial needs of the Australian community.

The Explanatory Memorandum indicates the government does not intend the regulation of Internet content to result in a degradation of network performance to a point where the Internet no longer meets the needs of the Australian community.

Schedule 5 also ensures that ISPs and ICHs are not held liable for content of which they are not aware. To this end, clause 91 indemnifies ISPs and ICHs against liability under state, territory or common law that would have the effect of requiring an ISP or ICH to monitor content accessed through or hosted on their services.

With regard to the operation of an Internet complaints hotline, the government decided it would not be reasonable for ISPs to be the first point of contact for the lodgement and investigation of complaints. In order to ensure that complaints are resolved in a timely and cost-effective way with minimal burden on the Internet industry, complaints are made directly to the Australian Broadcasting Authority (ABA).

2.3 Outline of the Scheme

The Online Content Co-Regulatory Scheme, which commenced on 1 January 2000, has three main components as set out in clause 1 of Schedule 5 to the Act:

1. The regulation of ISPs and ICHs through the industry codes of practice and complaints mechanism provided for by Schedule 5.
2. State and territory laws that impose obligations on producers of content and persons who upload or access content, and the Commonwealth *Crimes Act 1914* which makes it an offence to intentionally use an Internet carriage service with the result that another person is menaced or harassed, or in such a way as would be regarded by reasonable persons as offensive.
3. Non-legislative measures including community education.

2.3.1 Industry codes of practice

Part 5 of Schedule 5 to the Act provides for the development and operation of Internet industry codes of practice that are registered by the ABA. The codes require ISPs and ICHs to take appropriate steps to protect the public from 'prohibited and potentially prohibited' Internet content (see section 3.2 below).

As defined in Part 3 of Schedule 5, Internet content is 'prohibited' if it has been classified RC or X by the Classification Board or, if it is Australian-hosted, classified R by the Classification Board and access to the content is not subject to a restricted access system. Internet content is 'potentially prohibited' if it has not been classified by the Classification Board but if it were to be classified there is a substantial likelihood that it would be prohibited.

Under Schedule 5, if the Internet industry codes of practice are not developed, or if a registered code is deficient, the ABA may develop an industry standard. Compliance with an industry standard is required under the Act. The Scheme, however, emphasises the desirability of the industry itself developing programs to deal with the matters specified in the legislation. This co-regulatory framework forms the practical operation of what is known as the Online Content Co-Regulatory Scheme.

In December 1999, the ABA registered three codes developed by the Internet Industry Association (IIA) in consultation with the community and industry. Taking effect on 1 January 2000, IIA content codes 1 and 2 cover the activities of all Australian ISPs, while content code 3 applies to all Australian ICHs. On 10 May 2002, the ABA registered revised Internet industry codes of practice which can be accessed at *www.iia.net.au*.

Clause 58 of Schedule 5 provides that the Minister may declare a specified body or association to be the *designated body* for community oversight of the industry codes and standards. Under Schedule 5, the ABA must be satisfied that the designated body has been consulted on industry codes or standards developed under that Schedule before registering the codes or standards. On 6 December 1999, the Minister declared NetAlert, an independent body established by the Government to promote a safer Internet experience and research Internet access technologies, to be the designated body.

2.3.2 Complaints mechanism

The cornerstone of the Online Content Co-Regulatory Scheme is the complaints mechanism established by Part 4 of Schedule 5 to the Act. This allows the ABA to take action to investigate complaints about Internet content. Schedule 5 provides for the classification of Internet content by reference to the classification system for films and computer games under the *Classification (Publications, Films and Computer Games) Act 1995* (Classification Act). If investigated material is found to be prohibited, as defined in Part 3 of Schedule 5, the ABA may order it to be taken down if it is hosted in Australia or, if it is hosted overseas, referred to the makers of certain Internet content filters so that the filters are configured to block access to the content.

The ABA has established an Online Complaints Hotline which adopts conventions that are agreed and used by international Internet complaint hotlines. The ABA's Hotline enables any person to complain to the ABA if they believe Australians can access prohibited or potentially prohibited online content using an Internet carriage service or that such material is being hosted in Australia by an ICH. The Hotline is accessible at: *www.aba.gov.au* (see section 3.1 below).

The investigation of a complaint involves determining the actual or likely classification of the content, the location of the ICH and, if the ICH is located in Australia, the identity of the ICH.

If it is ascertained that Internet content is hosted in Australia and the ABA considers that the content is likely to be classified X or RC, the ABA issues an interim 'take-down' notice to the ICH, directing it not to host the content.

At the same time, the ABA applies to the Classification Board to classify the content concerned.

If the ABA considers the content is likely to be classified R (restricted to adults 18 and over) and not subject to a restricted access system which complies with criteria determined by the ABA, the ABA applies to the Classification Board to classify the content and advises the ICH of this request, for its information.

Upon receipt of a classification and in the event that the Classification Board finds the content to fall within the prohibited categories under Schedule 5, the ABA issues a final take-down notice to the ICH. The take-down notice advises the ICH of the location and classification of the content and the requirements under the Scheme. The ICH must comply with both interim and final take-down notices by 6.00 pm on the business day after each notice was issued. The ABA checks to ensure that the ICH has complied with the notice after this time. Failure to comply with such a notice may result in a maximum penalty per day of $5 500 for an individual and $27 500 for a corporation.

If the content is hosted outside Australia, the ABA determines the likely classification of the content. If the ABA considers the content is likely to be classified X or RC, it is notified to makers of the filter software products that are listed in the Schedule to the registered *codes of practice* for ISPs. The makers of these products have agreed to update their products to give effect to the ABA notifications. The codes require Australian ISPs to provide one of these products to their subscribers.

In the case of 'sufficiently serious' content such as child pornography, such material that is hosted in Australia is also notified to the appropriate state or territory police service in line with Memoranda of Understanding (MOU) between the ABA and the police services, for investigation of the content for criminal liability. In the case of overseas-hosted content, 'sufficiently serious' material is referred to the Australian Federal Police (AFP) or to the Internet complaints hotline in the host country, for the attention of law enforcement officials in that jurisdiction.

The ABA has taken the view that information which could enable people to access content that is the subject of ABA take-down notices should not be made publicly available in order to protect the integrity of the Scheme. On 12 June 2002, the AAT announced its decision to affirm the ABA's decision, in response to a freedom of information request, not to release the details of material identified under the Scheme as prohibited and potentially prohibited.

2.3.3 Community education

Subclauses 94(b) and (c) of Schedule 5 provide for the ABA to undertake community education and advisory activities. ABA activities in this context include providing advice and assistance to families about the supervision and control of children's access to Internet content and conducting community education programs about Internet content and related issues.

NetAlert was established by the Government as an independent body to encourage and promote the use of the Internet by all Australians, particularly young people and their families. NetAlert works to achieve this through its advisory services, a toll-free national Help Line (1800 880 176), information kits, a website (*www.netalert.net.au*) and research into Internet content filters.

2.3.4 Research

Management tools and technologies for the Internet are constantly developing. In this context, subclauses 94(d) and (f) of Schedule 5 to the Act empower the ABA to conduct research into issues relating to Internet content and Internet carriage services, and to inform itself and the Minister on technological developments and service trends in the Internet industry. This provides valuable information to shape the Scheme's community education program and to support monitoring of the Internet industry codes of practice.

In addition, NetAlert was established to, among other things, undertake research into Internet access management technologies. In this context, the ABA and NetAlert have jointly commissioned major research projects and undertaken complementary research activities under the Scheme (see sections 3.3 and 3.5).

2.3.5 International liaison

The global nature of the Internet, including the ability of users to access content throughout the world almost instantaneously, means that any serious effort to manage content must include international cooperation.

Subclause 94(e) of Schedule 5 to the Act empowers the ABA to liaise with regulatory and other relevant bodies overseas about cooperative arrangements for the regulation of the Internet industry. Such arrangements may include, but are not limited to, collaborative arrangements to develop multilateral codes of practice and Internet labelling technologies.

While the ABA has an MOU to refer sufficiently serious content to the AFP for forwarding to overseas law enforcement agencies, the ABA has also developed arrangements with Cybertipline in the United States and the International Hotline Providers in Europe Association (INHOPE) for referring illegal content to law enforcement agencies in those jurisdictions.

NetAlert's objectives include developing reciprocal arrangements with counterpart groups and other organisations overseas to exchange information on relevant Internet content issues.

2.4 State and territory laws and the Commonwealth Crimes Act

As discussed in section 2.3 above, clause 1 of Schedule 5 makes clear that state and territory laws and the *Crimes Act 1914* (section 85ZE) are integral components of the Online Content Co-Regulatory Scheme.

With regard to the state and territory laws, the Explanatory Memorandum sets out that it was intended that states and territories would be responsible for enacting legislation to regulate the activities of persons who create, upload or access content.

The Commonwealth has encouraged the states and territories to enact laws that will create offences for the publication and transmission of proscribed material by producers of content on the Internet or for persons who upload or access such content. To this end, model state and territory Internet content legislation was agreed to in 2000. To date, only Victoria, Western Australia and the Northern Territory have legislation dealing with objectionable material on the Internet. The legislation is not identical across jurisdictions and, in each case, the legislation pre-existed the Commonwealth's Scheme and was not based on the agreed model legislation.

Legislation regulating Internet content was enacted – although not commenced - in New South Wales. However, on 6 June 2002, the Committee on Social Issues in the New South Wales Legislative Council released a report on Schedule 2 of the NSW *Classification (Publications, Films and Computer Games) Enforcement Amendment Act 2001*. This legislation made it an offence either to make material that would be classified X or RC available on the Internet or to make material that would be classified R available without an approved verification system in place.

The Committee's report recommends that Schedule 2 of the Classification Enforcement Act should be repealed and that the New South Wales *Crimes Act 1900* should be reviewed in order to determine the adequacy of the provisions for punishing those who make available particularly dangerous or offensive content.

The Commonwealth *Crimes Act 1914*, which falls under the portfolio responsibilities of the Attorney-General, is also a component of the Online Content Co-Regulatory Scheme. Section 85ZE of the Crimes Act makes it an offence to intentionally use a carriage service supplied by a carrier in an offensive way or to menace or harass another person.

3 ISSUES

3.1 Complaints process—performance

In the first 24 months of the operation of the Online Content Co-Regulatory Scheme, the ABA received 937 complaints. Two complaints were deemed to be vexatious, frivolous or not made in good faith and, accordingly, were not investigated by the ABA. The ABA terminated investigations into 168 complaints, typically due to insufficient information being provided by the complainant. The ABA completed investigations into the 765 remaining complaints, of which 487 led to the legal finding of prohibited content. Two complaints were current at the end of this two-year period. Detailed complaints statistics are provided in Table 1.

The ABA issued take-down notices in relation to 227 Australian-hosted items that were found to be prohibited during the first 24 months of the Scheme's operation. Under the anti-avoidance provisions of clause 36 of Schedule 5, nine special take-down notices were issued to Australian ICHs for Internet content considered to be substantially similar to that which the ABA had issued an interim or final take-down notice.

Pursuant to clause 92 of Schedule 5, an application may be made to the Administrative Appeals Tribunal (AAT) for review of a number of decisions under the Scheme, including a decision to give an ICH a take-down notice and a request to the Classification Board to classify Internet content. No such appeals were made in the first 24 months of the Scheme's operation.

The ABA notified 529 items of overseas-hosted content to the suppliers of Scheduled filters. Revised Internet industry codes of practice, registered by the ABA on 10 May 2002 (see section 2.3.1 above), include a requirement on filter software manufacturers or agents to supply the following information to the IIA when seeking inclusion for their product or service in the Schedule:

- an outline of the process involved in updating the Internet filter product or service
- the expected maximum time it will take to give effect to a notification
- the means by which an end-user of the Internet filter product or service may obtain and implement a version updated as a result of a notification.

In addition, the ABA referred 485 items of Internet content to the relevant police authorities under the Scheme, consisting of 132 referrals of Australian-hosted content to state and territory police authorities and 353 referrals of overseas-hosted content to the Australian Federal Police. In this context, 492 items actioned by the ABA during the first 24 months of the Scheme's operation involved exploitative/offensive depiction of a child or child pornography.

These arrangements are set out in the MOUs between the ABA and individual Australian police services (see 2.3.2 above). The ABA currently has formalised agreements with police services in Queensland, Tasmania, New South Wales, Western Australia and Victoria, as well as the AFP to cover the Australian Capital Territory and overseas-hosted Internet content referrals. Discussions with the South Australian Police Service commenced in July 2001 and an informal arrangement for the exchange of information about Internet content exists for the Northern Territory. Each MOU provides for periodic review of its operation.

The ABA also has the discretion to defer action about prohibited or potentially prohibited Internet content if a member of an Australian police force satisfies it that action should be deferred for a specified period in order to avoid prejudicing a criminal investigation.

Comment is sought on the complaints process and outcomes, and the referrals of 'sufficiently serious' content to the relevant police authorities.

Table One: Complaints about Internet content

	Period 1 Jan-June 2000	Period 2 July-Dec 2000	Period 3 Jan-June 2001	Period 4 July-Dec 2001	Total
Complaints received	201	290	215	231	937
Investigations completed	160	221	185	199	765
Investigations terminated[1]	37	56	29	46	168
Complaints not investigated[2]	2	0	0	0	2
Investigations current at the end of the reporting period	2	15	16	2	N/A
Investigations leading to finding of prohibited or potentially prohibited content	93	139	98	157	487
Items actioned (Australian hosted)[3]	62	64	34	67	227
Items actioned (overseas hosted)	94	136	153	146	529
Items referred to State or Territory police force.	44	45	23	20	132
Items referred to Australian Federal Police	51	105	104	93	353

1. Investigations are terminated when information provided by the complainant).
2. A complaint will not be investigated by Content Co-Regulatory Scheme.
3. Some investigations involve consideration of more than one item of content. For example, where a complaint relates to an entire newsgroup, rather than a single posting on it, the ABA investigates a sample of the postings contained in the newsgroup, applies to the Classification Board to classify the content concerned and takes appropriate action according to the classification. For the purpose of reporting, each of the postings sampled is then counted as an item in the ABA's statistics. Similarly, the ABA may investig statistics. However, investigations re content generally pertain to a specific page of content.

The release of material from an ABA investigation identifying prohibited or potentially prohibited content, or the means of accessing such content, could undermine the policy and object of the Scheme. Once material is released, the subsequent use or dissemination of that material cannot be controlled. In this context, it has become apparent that an amendment to the *Freedom of Information Act 1982* (FOI Act) is necessary to ensure that such material in the possession of the ABA is adequately protected. Accordingly, amendments to the FOI Act were introduced in the Parliament on 27 June 2002 to ensure that material containing prohibited, or potentially prohibited, online content or the means of accessing such content is specifically exempt from disclosure under the FOI Act.

In addition, on 30 September 1999, the Australian Senate passed a motion calling on the Government to table a report, at six-month intervals, on the effectiveness and consequences of Schedule 5. The requirement remains effective until the Senate passes a motion repealing this reporting requirement on the Government.

In accordance with that resolution, four reports have been tabled. The reports have provided detailed updates with regard to the Internet industry codes of practice; complaints investigated under the Scheme; community education initiatives and research undertaken by the ABA and NetAlert; and the role of international liaison and collaboration under the Scheme.

Comment is sought generally on the performance of the complaints process.

Sections 2.3.1 and 2.3.2 above outline the prohibited categories under the Scheme and the procedure for referrals of potentially prohibited Australian-hosted content to the Classification Board for classification. In this context, the Classification Board classifies Internet content according to the Classification Act, the National Classification Code and, as appropriate, the Guidelines for the Classification of Films and Videotapes or the Guidelines for the Classification of Computer Games.

Under the Guidelines for the Classification of Films and Videotapes, material classified RC may include material containing detailed instruction in crime, violence or drug use; child pornography; bestiality; excessively violent or sexually violent material. Material classified X may include real depictions of actual sexual activity and no depiction of violence. Content classified R may deal with issues or contain depictions that require an adult perspective.

The OFLC is currently undertaking a combined review of the classification guidelines for computer games and films and videotapes.

Comment is sought on the scope of Internet content that is addressed under Schedule 5. Note that this request for comment is not intended to encompass the issues addressed by the OFLC's guidelines review.

3.2 Co-regulatory approach—industry codes of practice

Schedule 5 establishes a co-regulatory scheme for the regulation of Internet content, based essentially on the development and operation of industry codes of practice that are registered by the ABA and apply to all Australian ISPs and ICHs (see section 2.3.1 above).

In accordance with the co-regulatory framework of the Act, compliance with the Internet industry codes of practice is not compulsory in the first instance. Schedule 5 provides that once the ABA directs an ISP or ICH to comply with a registered code, however, they must then do so. If codes of practice are not developed by the Internet industry or if a registered code of practice is found to be deficient, the ABA may itself develop an industry standard. This framework is similar to the regulatory scheme currently operating in the broadcasting industry.

Clause 60 of Schedule 5 sets out that Internet industry codes must include ways that ISPs and ICHs can:

- ensure that online accounts are not provided to children without the consent of a parent or responsible adult;
- give parents and responsible adults information about how to supervise and control children's access to Internet content;
- assist parents and responsible adults to supervise and control children's access to Internet content;
- inform producers of Internet content of their legal responsibilities in relation to that content;
- inform customers about their right to make complaints about Internet content;
- inform and assist customers to make complaints about Internet content;
- assist customers to deal with complaints about unsolicited electronic mail (spam) that promotes or advertises an Internet site or distinct parts of Internet sites that enable, or purport to enable, end-users to access information that is likely to cause offence to a reasonable adult;
- assist in the development and implementation of Internet content filtering technologies (including labelling technologies);
- give customers information about the availability, use and appropriate application of Internet content filtering software;
- ensure that customers have the option of subscribing to a filtered Internet carriage service; and
- ensure that, in the event that an industry member becomes aware that an Internet content host is hosting prohibited content in Australia, the host is told about the prohibited content.

For the ISP section of the Internet industry, a code must also deal with:

- a means of notifying ISPs about prohibited content; and
- procedures for ISPs to follow to filter prohibited content hosted overseas, although a code of practice may provide that an ISP is not required to deal with overseas-hosted prohibited content if the ISP has taken steps to prevent particular end-users from accessing prohibited content under an arrangement that is declared by the code to be a 'designated alternative access-prevention arrangement'.

As noted in section 2.3.1 above, the ABA has registered three codes developed by the IIA in consultation with the community and industry.

In this context, the obligations imposed on ISPs in content code 2 are centred on filtering and the processes for dealing with overseas-hosted content. The code provides that if the ABA is satisfied that Internet content hosted outside Australia is prohibited or potentially prohibited, the ABA must notify the content to the makers of filter software in accordance with the 'designated notification scheme' outlined in the codes. The makers of the filter products listed in Schedule 1 to the codes 'scheduled filters' have agreed to update their filter to give effect to the ABA notifications so that the filter will subsequently block the content. The code requires Australian ISPs to provide one of the scheduled filter products to their subscribers.

In this context, filters play a dual role in the operation of the Scheme. First, they are a useful tool to be used in conjunction with parental supervision and household rules to manage access to Internet content generally. Secondly, filters underpin the designated notification scheme contained in the codes, for dealing with prohibited and potentially prohibited Internet content that is hosted outside Australia.

The revised codes that were registered by the ABA on 10 May 2002 replaced the previous requirement allowing ISPs to determine the fees for filter products or services with a requirement that the filter software or products be provided on a cost-recovery basis. That is, the charge to the user must now not exceed the total cost incurred by the ISP in obtaining, supplying and supporting that filter.

However, ISPs may be relieved of some obligations in relation to overseas-hosted content (e.g. the provision of filters and the requirement to deal with prohibited overseas-hosted content notified by the ABA) if the end-user is subject to an arrangement that is likely to provide a reasonably effective means of preventing access to prohibited or potentially prohibited content. Known as 'designated alternative access-prevention arrangements', these arrangements may include commercial subscribers, schools or other institutional subscribers that have advised their ISPs that they have in place a form of content filtering or control, whether by means of firewall technology or otherwise.

Comment is sought on the operation of the codes, in particular the 'designated notification scheme' under code 2, the scheduled filters and the designated alternative access-prevention arrangements.

With regard to Australian ICHs, the main requirement is that they remove prohibited or potentially prohibited content hosted in Australia upon notification by the ABA. To this end, in the first 24 months of the Scheme's operation, ICHs complied with ABA take-down notices in the prescribed time limits. The ABA has not had to use its 'enforcement powers' to obtain compliance in this regard.

Surveys conducted by the IIA during the first 24 months of the Scheme's operation indicate that all major ISPs that are members of the IIA are also fully compliant with the codes. The major ISPs account for approximately 80 per cent of end-users. With regard to smaller ISPs, the IIA surveys suggested that the level of compliance increased to 85 per cent of those surveyed after two years of the operation of the Scheme.

Nonetheless, code compliance matters are raised with individual ISPs as they come to the ABA's attention. As part of its compliance monitoring activities, the ABA has met with several ISPs to discuss legislation and code compliance matters, with matters subsequently resolved to the ABA's satisfaction.

As required under clauses 62 and 77 of Schedule 5 to the Act, the ABA has been satisfied that NetAlert has been consulted on the IIA codes of practice prior to each registration by the ABA.

On 10 May 2002, the IIA launched its Family Friendly ISP seal program—ISPs that are fully compliant with the Internet industry codes may display the IIA-endorsed 'ladybird logo' on their website. The IIA has advised that users who click on the logo will go to an information page informing them of the program and how to use the family friendly services offered by participating ISPs. The program is supported by the ABA and NetAlert.

Comment is sought on the level of responsibility taken by industry under the Schedule 5.

Comments are sought generally on the co-regulatory approach established by Schedule 5 to the Act, including the Internet industry codes of practice and whether the registered codes have operated to provide adequate community safeguards.

Comments are also sought on compliance costs and related issues associated with the Online Content Co-Regulatory Scheme.

3.3 Co-regulatory approach—community education and advice

Community education and advice are central to the Online Content Co-Regulatory Scheme. To this end, the Internet industry codes detailed above require ISPs to provide information, or links to information provided by the IIA, about:

- supervising and controlling children's access to Internet content;
- procedures that parents can implement to control children's access to Internet content, including the availability, use and appropriate application of Internet content filtering software, labelling systems and filtered Internet carriage services;

- subscribers' rights to make complaints to the ABA about prohibited content or potentially prohibited content and the procedures by which such complaints can be made; and
- methods by which receipt of unsolicited email (spam) that promotes offensive material may be minimised.

In addition, ISPs are required by the codes to encourage subscribers who are content providers to use appropriate labelling systems for material considered unsuitable for children, and to inform the content providers of their legal responsibilities under the Act or complementary state or territory legislation.

Comments are sought on the industry's obligations and activities with regard to community education.

Under clause 94 of Schedule 5, the ABA has the following educational functions for the purposes of the Online Content Co-Regulatory Scheme:

- to advise and assist parents and responsible adults in relation to the supervision and control of children's access to Internet content; and
- to conduct and/or co-ordinate community education programs about Internet content and Internet carriage services, in consultation with relevant industry and consumer groups and government agencies.

The ABA's strategy for community education has aimed to ensure that its activities are targeted and appropriate, and that they compliment rather than duplicate the activities of other players in the management and regulation of Internet content, in particular NetAlert and the IIA. Relevant ABA activities in this regard include:

- developing the Australian Families' Guide to the Internet website to provide an online starter kit for parents and responsible adults. The website was launched on Online Australia Day, 27 November 1998, prior to the introduction of the Scheme and was regularly updated to provide relevant and accessible information about Internet safety;
- promotion of the ABA's Internet Complaints Hotline through activities such as the provision of information to the media, distribution of posters to schools and libraries and advertisements in relevant magazines;
- presentations at national and international conferences;
- development and distribution of information materials for distribution to parents, teachers and children, primarily through school and libraries. A series of posters and brochures outlined the Scheme and promoted the ABA's Internet Complaints Hotline;
- redesign of the Australian Families' Guide to the Internet website to provide up-to-date information in a contemporary format. The redesigned *Cybersmart Kids Online website* was launched on 18 December 2001; and

- launching research into use of the Internet by Australian families with children—the *Internet@Home* research project—and, with NetAlert, the results of a jointly commissioned study into the effectiveness, from a user's perspective, of Internet content filtering software.

Comments are sought on the role and activities of the ABA with regard to community education.

In December 1999, the Government established NetAlert as an independent body to, among other things, embark on education campaigns to raise public awareness of the ways that parents and other concerned Australians may create a safer Internet experience. The NetAlert Board—currently consisting of 12 members—represents diverse community interests.

NetAlert's objects as outlined in its Constitution are to encourage and promote the use of the Internet by all Australians, particularly young people and their families, and in particular to:

- provide users with sensible, helpful and reliable advice and information about potential problems, dangers and threats present on the Internet and ways in which users can act to minimise or avoid these problems;
- provide assistance to ISPs and ICHs in relation to filtering technologies;
- develop and promote information and technological solutions that assist Australians to better manage Internet content;
- encourage ISPs and ICHs to act responsibly and reasonably when dealing with prohibited content and potentially prohibited content;
- work closely with Commonwealth and State agencies, Internet users, industry representatives and community bodies in order to promote responsibility and effective self-regulation of Internet content; and
- operate email and telephone advisory services to receive concerns about offensive Internet content and to pass any appropriate information to the ABA or relevant enforcement authorities.

To this end, NetAlert has been allocated $4.5 million in Government funding over the four years 1999–2000 to 2002–03.

In order to achieve its objects, NetAlert has undertaken a range of educational and promotional activities under the Scheme, including:

- the design and implementation of a website (*www.netalert.net.au*) to provide information for parents and children on safe Internet use;
- the implementation of a national toll-free Help Line and email advisory service to provide easily accessible information on how people can manage their access to the Internet. The Help Line commenced on 6 September 2000;
- the development and distribution of an information kit for Help Line callers, including fact sheets on various Internet issues. The information kit was also distributed to schools and community organisations, and through retail chains and computer stores, during the period;

- appointing a NetAlert Ambassador to promote NetAlert's 'safe surfing' message;
- organising and conducting an Industry Liaison Seminar Series in metropolitan and regional centres throughout Australia, advising ISPs and ICHs of their obligations under the Scheme. The two-hour seminars were presented in 27 metropolitan and regional centres; and
- conducting a series of Regional Forums across Australia to promote awareness of NetAlert in regional areas and identify Internet issues of concern to parents and students in these areas.

Comments are sought on the role and activities of NetAlert with regard to community education.

Comment is sought generally on community education under the Online Content Co-Regulatory Scheme.

3.4 International developments and cooperation

Of the prohibited or potentially prohibited overseas-hosted Internet content identified under the Online Content Co-Regulatory Scheme, over 70 per cent was hosted in the United States, with Eastern European countries hosting an increasing amount of the material since the commencement of the Scheme. While the ABA notifies the makers of scheduled filters of such content, it may also refer sufficiently serious overseas-hosted material to the AFP.

This issues paper has already noted that in the first 24 months of the Scheme's operation the ABA referred 353 items of overseas-hosted content to the AFP (see section 3.1 above). Under the Scheme, the AFP may then contact law enforcement agencies overseas notifying them of the prohibited content.

Under clause 40 of Schedule 5, the AFP is able to authorise the ABA to notify sufficiently serious content directly to an Internet complaints hotline in another country. Such arrangements exist with the National Centre of Missing and Exploited Children for content hosted in the United States, and INHOPE association that covers Austria, Belgium, Denmark, France, Germany, Iceland, Ireland, Spain, Sweden, the Netherlands and the United Kingdom. Through the ABA, Australia is an associate member of INHOPE.

Comment is sought on the effectiveness of referrals of overseas-hosted material to the AFP and to certain Internet complaints hotlines.

Clause 94 of Schedule 5 empowers the ABA to liaise with regulatory and other relevant bodies overseas about cooperative arrangements for the regulation of the Internet industry including collaborative arrangements to develop multilateral codes of practice and Internet content labelling technologies.

In February 1999, the then Deputy Chairman of the ABA was invited to join the International Network of Experts on Content Self-Regulation, an initiative of the German-based Bertelsmann Foundation. Subsequently, the ABA maintained membership of the Network.

The Network aims to facilitate the development of an integrated system of approaches for dealing with harmful and illegal content on the Internet through the development of codes of practice and rating and labelling systems and also through the establishment of complaints hotlines.

During the second half of 2000, the ABA became an associate member of INHOPE. INHOPE provides a forum through which Internet hotlines are able to exchange information and experience on matters such as complaints investigation processes, occupational health and safety for hotline staff, and standardised reporting of hotline statistics. The network is also a mechanism for dealing with specific complaints and enhancing and complementing existing arrangements with law enforcement agencies. In December 2000, the Chair of INHOPE visited the ABA hotline premises and attended an ABA hotline workshop. The Chair provided information on the United Kingdom's Internet Watch Foundation hotline as well as on INHOPE itself.

The ABA has maintained the involvement with the Internet Content Rating Association (ICRA) that it developed prior to the introduction of the Online Content Co-Regulatory Scheme. ICRA is an international, non-profit organisation that develops ratings systems to make the Internet safer for children. The ICRA system consists of a coded label created by the content provider and included as part of the metadata for the site, together with a decoder and filter in the browser of users' PCs that can read the labels and apply each user's values in deciding whether to access the content.

In addition, the ABA has provided responses to requests for information from international authorities and non-government organisations, including the:

- Singapore Broadcasting Authority;
- Commission on Youth Protection, Office of the Prime Minister, Republic of Korea;
- Independent Broadcasting Authority, South Africa;
- Internet Watch Foundation, United Kingdom;
- Child Online Protection Act Commission, a United States congressionally appointed panel;
- International Institute of Communications Regulators' Forum;
- Council of Europe's Steering Committee on Mass Media;
- Childnet International, based in the United Kingdom;
- National Centre for Missing and Exploited Children, United States;
- INHOPE; and
- Korean Broadcasting Corporation.

Under the its Constitution, NetAlert's objectives include developing reciprocal arrangements with counterpart groups and other organisations overseas to exchange information on relevant content issues. In line with its role in promoting Internet safety under the Online Content Co-Regulatory Scheme, NetAlert has fostered linkages with Childnet International and Cyberangels.

Established in 1995, Childnet International's aim is to facilitate the Internet as a safe and enjoyable place for children and to promote children's interests. Cyberangels is a large, global Internet safety organisation staffed by volunteers from over 70 countries. Cyberangels deals with cases of cyberstalking, harassment, online fraud, child pornography and provides advice on using the Internet for all levels of users.

Comments are sought on the role and functions of international cooperation under the Online Content Co-Regulatory Scheme and, in particular, the international liaison activities undertaken by the ABA and NetAlert in this regard.

Comments are also sought on international best practice models and developments and trends in international Internet content regulation.

3.5 Research – filtering technologies

On 26 March 2002, NetAlert and the ABA released a jointly commissioned report into the general effectiveness of existing filtering software. The report, undertaken by CSIRO and entitled *Effectiveness of Internet filtering software products*, examined fourteen software products. The report found that the performance of filters might vary substantially, with a key determinant of effectiveness being the type of blocking methodology used by the product.

In launching the report, the ABA and NetAlert emphasised that parents need to choose the filter appropriate to the age and access requirements of their children, and that filter software may most effectively prohibit access to unwanted material when used in conjunction with parental supervision and household rules for Internet access.

Prior to the commencement of the Online Content Co-Regulatory Scheme, the National Office for the Information Economy (NOIE) commissioned the CSIRO to undertake analysis of the technical aspects of blocking Internet content and access prevention techniques for Internet content filtering. CSIRO reported on these studies in June 1998 and December 1999. In addition, NetAlert commissioned the CSIRO to provide quarterly reports—from December 1999 to February 2001—evaluating new Internet content filters as they came onto the Australian market.

The Explanatory Memorandum states that because technology is developing so rapidly, it is important to have a clear assessment of what is technically available in terms of filtering offensive Internet content. To this end, this review is required under subclause 95(2) of Schedule 5 to take into account the development of Internet content filtering technologies and whether they have developed to a point where it would be feasible to filter R-rated information hosted overseas that is not subject to a restricted access system.

As noted above (section 1.1), subclause 95(5) of Schedule 5 sets out the requirement that, in the event that Internet content filtering technologies develop to a point where it is practicable to use those technologies to prevent end-users from accessing R-rated information hosted overseas that is not subject to a restricted access system, legislation will be introduced into the Parliament to extend subclause 10(1) which deals with prohibited Internet content hosted overseas.

In this context, the Department intends to contract an external technical expert to undertake the required analysis.

Comment is sought on the development of Internet content filtering technologies and whether they have developed to a point where it would be feasible to filter R-rated information hosted overseas that is not subject to a restricted access system.

There have been calls for filters to be made available at no charge to Internet users in Australia. Some ISPs offer filtered services, while other ISPs do not charge subscribers separately for access to Internet content filtering products or services. On 10 May 2002, the ABA registered revised Internet industry codes of practice that require ISPs to provide filtering services or products on a cost recovery basis.

Comment is sought on the provision of Internet content filtering services under the Scheme.

3.6 Scope and coverage of Schedule 5

Definition of Internet content

The Minister has determined that any service that makes television or radio programs available using the Internet and without using broadcasting services bands spectrum is not a broadcasting service (see *Gazette* GN 38 of 27 September 2000). Accordingly, a service that made available streaming audio or video over the Internet would not be regulated by the Act as a broadcasting service.

Schedule 5 to the Act provides for the regulation of 'Internet content'. Clause 3 of Schedule 5 defines Internet content as information that is kept on a data storage device and is accessed, or available for access, using an Internet carriage service. A data storage device is any article or material (for example, a disk) from which information is capable of being reproduced. Accordingly, Internet content includes material on the World Wide Web (the Web), postings on newsgroups and bulletin boards, and other files that can be downloaded from an archive or library.

For the purposes of the Scheme, however, Internet content does not include ordinary emails, information transmitted in the form of a broadcasting service or information that has not been kept on a data storage device.

The Explanatory Memorandum states that 'information transmitted in the form of a broadcasting service' was intended that where material is transmitted over the Internet in the form of a broadcasting service, under the Act it will be treated as a broadcasting service subject to the rules applying to such services and not as Internet content subject to regulation under Schedule 5.

With regard to ordinary email, the Explanatory Memorandum states that it was intended that personal email not be caught by the definition of Internet content.

In respect of live-streamed content, it is unclear whether such content may be considered to be kept on a data storage device and therefore included in the definition of Internet content.

Comment is sought on the application of the Schedule to live-streamed Internet content.

Spam

NOIE has been tasked by the Minister to undertake a general review of unsolicited bulk email (spam). The terms of reference for the review include investigating and assessing the nature and extent of spam and identifying possible new or improved measures to counter spam.

The interim report to the review states that spam accounts for approximately 20 per cent of all email sent, and that this rate is growing rapidly. Spam is noted to be a global problem, with the United States, Eastern Europe, Asia and Australia being the source countries for the majority of spam received by Australian ISPs. The bulk of spam relates to 'get rich quick' schemes and direct sales of health cures or miscellaneous products, while up to 35 per cent of spam emails are estimated to contain or relate to pornography and gambling (*www.noie.gov.au/Projects/consumer/Spam/index.htm*).

The interim report proposes a series of measures to combat spam including the development of industry guidelines, encouraging greater application of existing legislation such as the *Privacy Act 1988* and conducting community education on ways to minimise the receipt of spam.

The interim report recommends that the question of offensive content contained in spam should be considered as part of this review of the operation of Schedule 5. The Internet content provisions in the Act may apply to the content of a website the URL for which is included in an email. Accordingly, any person may complain to the ABA about illegal or offensive Internet content that is linked or referred to in a spam email. If the Internet content is found to be prohibited, it is issued with a take-down notice or referred to filter makers as appropriate.

Typically, spam is not hosted nor is it generally accessible on the Internet. The question arises, therefore, of the method by which the complaints scheme and system of take-down notices could apply to offensive spam email or how the existing Scheme could be amended to apply specifically to offensive spam.

Comment is sought on the application of the Online Content Co-Regulatory Scheme to offensive spam.

Convergent devices

A number of convergent devices that allow access to Internet content do not accommodate end-user filtering. Such devices may include certain video game consoles, Internet TV and Internet appliances. They may also include palm pilots and 3G mobile phones which contain email functionality and the ability to access specially formatted web channels, or to browse ordinary websites.

In this context, the convergent devices have the potential to allow users access to Internet content in a way that is not specifically addressed by the Online Content Co-Regulatory Scheme. As noted in section 3.2 above, filters play a dual role in the Scheme by underpinning the designated notification scheme in the industry codes and by assisting in the management of access to the Internet.

However, some but not all of these devices include parental access control technologies and in some cases the display format requirements limit general access to the Internet in favour of certain customised sites. In the cases of devices with limited storage or software-loading capacity, filtering can be addressed at the service provider level through the use of filtered proxy servers offering an alternative safe service to subscribers. It should also be noted that the screen size constraints of palm pilots and mobile phones are not well-suited to viewing offensive graphics content and that this may naturally limit the proliferation of such material on these platforms.

Comment is sought on the potential impact that convergent devices may have on the operation of Schedule 5 to the Act.

Comments are sought generally on the scope and coverage of Schedule 5.