Submission to DCITA
Review of the
Operation of Schedule 5
Broadcasting Services Act 1992

Internet Industry Association
www.iia.net.au

November 15, 2002
The Internet Industry Association (IIA) on behalf of its members, is pleased to make this submission to the Department of Communications, Information Technology and the Arts’ Review of the Operation of Schedule 5 of the *Broadcasting Services Act 1992*

**Introduction**

The IIA is Australia's national Internet industry organisation. Members include telecommunications carriers, content creators and publishers, web developers, e-commerce traders and solutions providers, hardware vendors, content filter providers, systems integrators, banks, insurance underwriters, Internet law firms, ISPs, educational and training institutions, Internet research analysts, and a range of other businesses providing professional and technical support services. On behalf of its members, the IIA provides policy input to government and advocacy on a range of business and regulatory issues, to promote laws and initiatives which enhance access, equity, reliability and growth of the medium within Australia.

As the industry organisation in Australia most closely involved in the issue of content regulation, and as architects and implementers of the three registered internet codes of practice permitted by the Broadcasting Services Act (the ‘BSA’), the IIA considers itself well placed to comment on the effectiveness of Schedule 5 of the BSA.

By way of background, the IIA has been working on policies in this area since 1995 and has achieved international recognition for its pioneering work in co-regulation of internet content and the protection of families online. In addition, IIA representatives have been active participants in the work of NetAlert, the ‘designated body’ under the BSA. The IIA’s current chief executive and two of its directors were appointed by the Minister as foundation directors of NetAlert in 1999. Those individuals continue to serve on that body and to support NetAlert staff to drive much of its outreach program to the community.

Prior to that, IIA representatives served on the ‘Children and Online Content’ Ministerial Taskforce in 1998, and have been invited to address international and local audiences on this subject, including those at:

- Cyberspace Law & Policy Centre Conference (Sydney October 2002)
- Berkman Center of Internet Law, Harvard Law School (Cambridge MA, March 2001)
- ISPCON (Orlando FL, May 2000)
• ISPCON (San Jose CA, November 2000)
• Economic Strategy Institute (Washington DC, October 1999)
• The Convention on Combating Child Pornography on the Internet (Vienna, October 1999): delegate invitee of Ministry of the Interior, Austria
• Internet Content Self Regulation Summit (Munich, September 1999): delegate invitee of Government of Bavaria/Bertelsmann Foundation

In terms of ISPs and content hosts, both of whom are governed by the relevant Act, the IIA has within its membership most of the major players and a substantial number of the smaller ones. Our work has been concentrated on ensuring a reasonable balance between addressing the legitimate needs of end users on the one hand, and the capacity of businesses to support requirements that Parliament has seen fit to legislate. We value the opportunity that the legislation affords to create flexible industry codes by which industry can meet its statutory obligations and at the same time, promote the interests of end users who are, after all, our market.

Because we have been given the ability to craft the rules, within the parameters set by the law, we have been able to secure co-operation with not only the letter of the law, but also its spirit. At the end of the day, we believe that informed and willing compliance coupled with a demonstrable marketing advantage for adherence to best practices, is superior to government imposed regulation. This is particularly the case in a new and still quite fragmented industry, and one which is unique in its inherent disparity and global reach. In our view, it is better for governments to create and support systems which recognise the unique features of the Net, than to apply regulatory paradigms which instantaneous and diffuse media like the internet have rendered less efficacious.

Clauses 1.1 and 1.2 of the preamble to our registered Codes of Practice state, respectively:

In relation to content control, the IIA recognises that the Internet should provide a means to enable control of access to content in certain circumstances, while acknowledging the the limitations of present filtering technologies and impracticality of filtering all Internet content.

Nevertheless, the IIA endorses end user empowerment including education, the provision of information, and filtering methods as the most practical means by which responsible adults can facilitate appropriate controls, particularly in the case of children.

We see a commonality of interest between government, industry and the community in a model which provides families with the tools and solutions by which they can effectively control access to the information which is accessible online.
Co-regulation

Co-regulation gives effect to the concept of partnership and shared responsibility between business and government. Government recognises the need for industry involvement because it is industry which largely controls and operates the infrastructure over which the internet runs. Industry will always prefer the ability to shape the regulatory environment, than have it externally imposed. Therein lies the synergy. Co-regulation is supported by the IIA in many areas of internet policy, because it can provide a flexible way of maintaining relevant and enforceable best practice standards within the rapidly changing communications environment, while retaining a meaningful role for government to respond to community concerns.

In contrast, international experience has shown that pure self-regulation is not optimal because not all businesses will voluntarily adopt best practice behaviours, leaving some users exposed. This can create a bad reputation for the industry as a whole and retard the uptake of the internet. Reputable players are concerned that non-complying competitors will use their lack of compliance to unfair advantage. It may cost less in the short term to avoid best practice compliance, but in the long term the industry as a whole suffers as consumer confidence is allowed to wane.

At the other extreme, pure government regulation is problematic because lawmaking always lags technological change. Only now it is worse because change is accelerating, and global communications force governments to confront their jurisdictional limits like never before. Where they opt to legislate, they face the conundrum of having to choose between technologically specific measures which quickly render regulation out of date, or impose a level of generality which is so open to interpretation as to create uncertainty and legal risk from a compliance perspective. The result sees end users exposed to risks which might otherwise be mitigated if rules were able to adapt more responsively to changes in circumstances.

Co-regulation provides the strengths of both systems - keeping pace with change, and providing an industry-wide safety net for consumers which is monitored and reviewed by government, for and on behalf of the people.

Better Compliance vs More Regulation

The IIA does not support any major changes to the legislation because we believe it is working, when viewed in the light of its objects, the unique nature of the medium and Parliament's intention, as stated in subclause 4(3) of Schedule 5, that regulation:

(a) enables public interest considerations to be addressed in a way that does not impose unnecessary financial and administrative burdens on Internet content hosts and Internet service providers; and
(b) will readily accommodate technological change; and

(c) encourages:

(i) the development of Internet technologies and their application; and

(ii) the provision of services made practicable by those technologies to the Australian community; and

(iii) the supply of Internet carriage services at performance standards that reasonably meet the social, industrial and commercial needs of the Australian community.

While we would like to see better compliance, additional regulation will be difficult for industry to support. It is well known that over the past two years, and unlike most other sectors of the economy, the internet industry has suffered a severe downturn, and this before it was even fully developed. The telecommunications industry remains in recession globally, investor confidence is low, capital is scarce and, with few exceptions, profitability remains elusive. While absolute customer numbers have grown, the rate of increase has slowed. Competition among ISPs in Australia has reduced margins to almost unsustainable levels. Many smaller players, and some not so small, are struggling to survive as they contemplate how they might migrate to broadband.

The state of the market has meant that ISPs and content hosts have largely had to absorb the costs of:

- putting in place technologies, systems and procedures to comply with the current content regime; and
- meeting associated internal training costs and the production of both printed and digital content for distribution to their customers.

In addition, in complying with our revised Codes, they have foregone the ability to provide filters above cost price. Some ISPs have, in good faith and in their desire to meet their obligations, entered into long term contracts with internet filter providers. Any substantial change to the regulatory environment may subject them to hardship if those arrangements are no longer capable of performance.

In view of these considerations and because the implementation of the current legislation through our Codes works extremely well we say there is no reason to impose upon the industry any toughening of obligations, when most Australians online are served by ISPs doing all that is reasonable to support the current regime.

The preservation of co-operative relations within the industry is fundamental to the continued success of the scheme, and for that reason we strongly recommend maintaining the status quo.
The IIA has a demonstrated commitment to industry responsibility and playing a key role in supporting the co-regulatory regime. We have developed strategies to increase the level of industry compliance with the Codes. To that end, we have prepared a code compliance checklist, reproduced in **Appendix 1** and developed the **Family Friendly ISP program** (discussed in more detail below).

The IIA has also attempted to ease the compliance burden for ISPs and content hosts by creating and maintain a public information resource, the **Guide to Internet Users** ("User Guide"), on our site at [www.iia.net.au/guideuser.html](http://www.iia.net.au/guideuser.html).

ISPs and content hosts who link to this resource are deemed to have fulfilled their Code obligations relating to the provision of empowerment information to their customers. The User Guide is maintained by the IIA to reflect changes in the technology and changes to the Codes, including, in particular, the addition and removal of filters from the Code Schedule. The User Guide has been developed in conjunction with the **IIA Guide for ISPs** ("ISP Guide") at [www.iia.net.au/guide.html](http://www.iia.net.au/guide.html) which mirrors relevant changes in the User Guide, and assists in the understanding of how the regime works from an industry perspective. In addition, the ISP Guide provides ISPs with access to the NetAlert Compliance Manual, a resource developed with the assistance of the IIA, which formed the mainstay of NetAlert’s industry liaison program conducted nationally during 2001. The ISP Guide covers the following information:

- **Introduction**
- IIA Family Friendly ISP Program & License Agreement
- ISP Obligations
- Compliance Checklists
- NetAlert Compliance Manual
- Scheduled Filters and Contact Details
- Future updates to the Schedule

The User Guide explains the operation of the Codes and how they fit within the co-regulatory framework, information about filters, the ABA complaints scheme, and other information requirements stipulated by the legislation. Specifically, the User Guide contains the following information:

- **Introduction**
- The IIA "Family Friendly ISP" Seal Program
- If you want to download a filter or activate a filtered service now
- What are scheduled filters?
- How does the co-regulatory regime work?
- What do Internet Service Providers and Content Hosts have to do?
- How does my ISP provide a scheduled filter software product or service?
- How do I install the filter products?
- Who bears the cost of the filter products and services?
- What material can I post on the Internet?
- List of IIA Scheduled Internet Content Filters
- Resources for Parents on Supervising Children's Access
- Unsolicited email containing offensive materials or promoting offensive sites
The IIA Family Friendly ISP Scheme

In an additional move to lift compliance, the IIA introduced the Family Friendly ISP scheme in March 2002. A news release announcing the scheme is reproduced in Appendix 2 and evidences the high level of industry support for this initiative. We are pleased that the number of ISPs who have signed on continues to grow. The seal is available under license from the IIA, free to members and for a fee for non-members, provided that licensees agree to remain compliant with the relevant IIA Codes. Where the ABA notifies the IIA that a licensee is not in its view compliant with the relevant IIA Codes, the licensee has seven days to rectify the breach otherwise the license agreement terminates and the licensee must immediately cease using the seal or otherwise represent that it remains a IIA Family Friendly ISP.

The IIA is pleased that both NetAlert and the ABA support the scheme (see for example, http://www.netalert.net.au/Files/00122_InternetIndustryAssociation.asp). We were also grateful for the public vote of confidence exercised by Minister the in his news release of March 26, 2002 which coincided with the launch of the scheme.

The message from the scheme can be distilled into a simple proposition: Internet users with concerns about online content should ‘Look for the Ladybird’.

The IIA has invested much in developing the ladybird seal program to date, and will be continuing our push to increase industry understanding of, and compliance with the scheme. Because we view government as very much a partner in end user empowerment, we would value funding and practical support from agencies and officials within government to help us extend public awareness.

A number of possibilities exist, including:

- promotion and links via government sites that already provide guidance to the public on internet related issues. We see agencies tasked with helping build online uptake as natural partners with the IIA in this enterprise, as are those with regulatory roles converging on this scheme in ways that are similarly relevant. In aggregate, the ABA, ACCC, ACA, NOIE and DCITA might all assist the IIA in promoting the scheme;
• the appointment of an industry liaison officer within DCITA to assist with awareness raising within industry, or the expansion of duties of existing staff to meet this objective
• ongoing endorsement of the scheme by government in media releases and public events would also help orient user demand towards ISPs who meeting their responsibilities, and will encourage others to join in.

Complaints Process
The IIA supports the continuation of the existing regime to the extent that it remains complaints based. The ABA has an efficient system in place and internet users in Australia have somewhere to go where they encounter content which either offends them, or they believe is likely to be illegal. Since 1995, the IIA has lobbied to ensure that ISPs and content hosts are not left to make the decision on the legality of content. That the current regime relies on the expertise of the ABA, assisted where necessary by the Office of Film and Literature Classification, is evidence that the government accepts that industry should not be the arbiters of content. This must remain.

Further, the referral system established under Schedule 5 is an appropriate adjunct to the ABA’s role. Under this system, ‘sufficiently serious’ material hosted overseas can be brought to the attention of relevant authorities by the ABA. As this material invariably involves child pornography, the procedure has the strong support of industry who, even before the inception of Schedule 5, were already assisting law enforcement agencies in this same area. However, were the emphasis to shift to proactive policing of internet content, either by ISPs, content hosts, or the regulator, no conceivable effort could effectively monitor, or regulate the vast amounts of material available on the internet.

As an indication, the search engine Google claims to currently catalogue some 3,083,324,652 pages of web based content (as at 12 November 2002). That number has grown from 2,469,940,685 pages on 30 August 2002, a staggering increase of over 613,000,000 or 24.7% in under three months. Whether the increase is as a result of more content becoming accessible to Google’s web-crawling technologies, or more content coming online is immaterial. The volume of material that already exists online, is susceptible to updating or relocation in real time and is available to anyone with an internet connection and a browser (whether fixed or mobile) is unprecedented, and is only likely to grow.

1 The IIA draft Cybercrime Code, when it is released later this year, is further evidence of our efforts to help fight criminality online.
2 www.google.com
In terms of what domestic users are accessing, the Australian Bureau of Statistics in its most recent survey of internet activity in Australia found that:

1,234 million Megabytes (Mbs) of data were downloaded by Internet subscribers during the March quarter 2002, an average of 290 Mbs per subscriber. Of this, household subscribers downloaded 713 million Mbs (average of 191 Mbs per household subscriber).

Clearly, the feasibility of tracking and evaluating content of such proportions would almost certainly exceed the capacity and budgets of anyone with the interest or inclination to do so, and for little demonstrable result or impact on the total availability of offensive content remaining online. This is precisely why the IIA favours industry-facilitated end user empowerment within a co-regulatory framework as the best response to offensive material on the Net.

Community Education

The IIA values the community education work that both NetAlert and the ABA perform. We support the continued government resourcing of this work. In relation to the synergies with exist with industry, we see an enormous capacity for both organisations to educate the community about the benefits of using a Family Friendly ISP.

As far as the ABA’s educational work is concerned, we see no difficulty with a regulator having education as part of its role, both for the benefit of end users and also for those for whom compliance is a legal obligation. To the extent that regulators are better able to inform those they regulate of their rights and responsibilities, they can ease the burden of dealing with complaints after the event. This is a preventative approach. To the extent that they can inform users of their rights and responsibilities, they promote user empowerment. The commissioning and publicising of research is also a role that the ABA has performed, and one which adds to the strength of the scheme. Its Internet@Home research project was instructive in its findings and supported many of the anecdotal observations that the IIA had made, particularly in respect of the willing acceptance by the great majority of parents of their role in directly supervising the online activities of young children. The ABA’s Cybersmart Kids Online website is also a very useful resource for families, and one which we would like to see maintained.

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. NetAlert’s support for research into the

---

3 ABS Survey 8153.0 Internet Activity, Australia for quarter ending March 2002 (see www.abs.gov.au)
efficacy of filters placed it in a better position to provide the community with up to date and informed advice.

We see the educational roles of the two organisations as complementary rather than mutually exclusive, and support the maintenance of strong, positive, cooperative relations between them.

Filters
Internet content filtering technology continues to develop and improve. The IIA codes provide a ready means by which new filters can be made more readily available to end users, and obsolete technologies can be phased out. The IIA codes current recognise 19 filters. A list of these is included in Appendix 3 of this submission.

It remains the firm and informed view of the IIA that mandatory server level filtering is not technically or commercially feasible in Australia, and that no attempt ought be made to extend the legislation, or require registered codes or industry standards, to implement such measures.

In the 18-month review of the IIA codes, as the BSA required us to do, we took on board concerns about the pricing of internet filters, which some argued was a disincentive to their uptake. Whilst we do not agree that cost is the primary reason for any lack of uptake, we nevertheless agreed to amend the code so that ISPs offering filters must do so on a cost recovery basis, having regard to the costs of obtaining, maintaining and supporting filters. (We note that the DCITA issues paper recognises this concession). This represented a change from the previous version of the Codes, where ISPs were free to decide the price they would charge for providing filters or a filtered service (though even then some chose to charge nothing at all, as some still do). We believe that to force industry to fully absorb the cost of filters will be to drive them to the lowest cost solutions, which are not always the best. Rather, the cost recovery approach recognises that value for money and performance, rather than the absolute price should be the focus if innovation in the content filtering industry is to be fostered. For this reason, we support the broadest range of customer choice, where a diverse range of filters suited to different environments can continue to be made available, and those which integrate more features, such as virus scanning and firewalling can be also made available.

Emerging challenges
We acknowledge that as the technology develops and becomes ubiquitous, new challenges will arise. In particular, the IIA is concerned about issues arising from:

- the abuse of email (‘spam’) which increasingly prevalent, almost uniformly unwelcome and often bearing viruses, material inappropriate for children, or both
• wireless internet access using convergent devices, including but not limited to the question of location sensitivity and privacy, but also involving the nature of the content itself
• internet and internet like services delivered via television
• chat rooms, message boards and live streamed content

The IIA recommends maintaining a watching brief on developments in these areas. We have already provided DCITA with our views on the spam question and believe that a combination of technological solutions and end user empowerment will address the problem in the medium term. Where necessary, and with sufficient support from the government, the industry may be willing to adapt existing codes to provide the necessary community safeguards to address these challenges in a manner which will not impede innovation, escalate end user cost, neutralise the advantages of, or otherwise undermine the uptake of these technologies.

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 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.

Likewise, the issue of chat rooms is challenging. The providers of chat facilities, whether commercial or otherwise, are not amenable, nor should they be, to the monitoring of conversations or exchange of content. We propose that education and a degree of self regulation is more likely to deliver outcomes in keeping with the intent of the legislation, and for that reason we would resist an expansion of the regime to require proactive reporting or control. This however, does not preclude industry working with law enforcement bodies, in instances where users choose to report inappropriate conduct. There are instances where such reporting has led to prosecutions, and subject to due process, industry stands ready to cooperate.

**Conclusions**

After over two years of Code implementation, and having followed advances in the debate and in technology, the IIA remains convinced that there will never be any substitute for adult supervision of children’s activities online. Education of end users is paramount and allows families who are as yet unfamiliar with the options open to them, to feel more confident about having the internet in their homes. This should therefore be the policy focus.
Industry has already demonstrated that it is willing and able to help empower end users to take control for themselves. Within 2 years, we estimate that nearly 75% of households will enjoy some form of internet connectivity, and mobile solutions will become commonplace as convergence with mobile telephony progresses. It is our view that as familiarity with the medium grows, management techniques will also develop (as they have with other forms of technology throughout history) to maximise the benefits and minimise the risks arising from its use.

Australia can be rightly said to possess one of the most advanced systems of internet governance in the world, which has come about largely as a result of the ongoing dialogue between government, industry and the community. While we acknowledge that there are no perfect solutions, the IIA is committed to the task of identifying and implementing further improvements to best practice standards as they become known.

We believe that in the next phase of internet regulation, the emphasis should shift to resourcing initiatives which will accelerate the empowerment of end users. NetAlert should remain in place with a charter to pursue community education across a wider range of internet related issues. The ABA has internationally recognised expertise in internet content regulation and remains the appropriate regulator and complaints handling agency for this regime.

Ultimately, a competent and confident internet using Australian public will generate both social and economic benefits. We would caution against moving to more restrictive regulations and heavy handed intervention which in our view are not only unwarranted, but are likely to undermine the efforts that industry has made over the last few years in pursuing improvements of its own accord. For its part, the IIA will continue to maintain and develop its Codes and encourage more industry players to participate in the effective co-regulatory scheme that exists today.
Appendix 1: Code Compliance Checklist
(this is available online at www.iia.net.au/compliance.html)

(updated May 2002 to co-incide with registration of Content Codes Version 7.2)

The following checklists have been created to assist member ISPs and content hosts (ICHs) to comply with the Internet Industry Association's registered Codes of Practice relating to internet content, pursuant to the Broadcasting Services Act 1992 (as amended). The IIA registered Codes are voluntary, until and unless you are directed to comply by the ABA. Nevertheless, many of our members are choosing to comply because they want to ensure that they are meeting best practice, and to pre-emt possible liability under the Act should the ABA issue a notice to comply. The email advice will enable you to notify the IIA that you are compliant with the Codes.

Note numbers in square brackets [ ] refer to relevant provisions of the registered Codes (version 7.2). The Codes can be viewed in full at www.iia.net.au/codes.html.

Content Code 1 Requirements Checklist

PART A: Internet Access Account Registration

(at least ONE question in this part must be answered 'Yes' to comply with the Code)

1. Does it require that the customer provide their credit card number and expiry date? [5.1(a)]
   [ ] yes [ ] no

2. Does it ask that the customer provide documentation such as a passport, driver's licence or student card with date of birth or age? [5.1(b)]
   [ ] yes [ ] no

3. Does the packaging of the Internet access account contain a notice that states that persons under 18 need the consent of a parent, teacher or other adult before using the account? [5.1(c)]
   [ ] yes [ ] no

4. Is a service, such as a closed content system, offered when the account is opened? [5.1(d)]
   [ ] yes [ ] no

5. Does the registration site ask persons under 18 to verify that they have the consent of an adult to open the account? [5.1(e)]
   [ ] yes [ ] no

PART B: Content Provider Customers

6. Is there a link on the home page to resources, made available by the IIA, the ABA, NetAlert or other approved organisation, that:
   (a) encourages the use of a labelling system been used (in relation to content unsuitable for children)? [5.2(a)]
      [ ] yes [ ] no
   (b) informs content provider customers of their legal responsibilities in relation to content? [5.2(b) and 5.4]
      [ ] yes [ ] no
PART C: Informing Subscribers

7. Is there a link on the home page to resources made available by the IIA, the ABA, NetAlert or other approved organisation to inform subscribers:

   (a) about supervising and controlling children's access to the Internet? [5.3(a) and 5.4]
   [ ] yes [ ] no

   (b) about the availability and use of filtering software? [5.3(b) and 5.4]
   [ ] yes [ ] no

   (c) that placing content on the Internet may entail legal responsibilities? [5.5(a) and 5.6]
   [ ] yes [ ] no

   (d) they may make a complaint to the ABA about prohibited or potentially prohibited content? [5.5(b) and 5.6]
   [ ] yes [ ] no

   (e) about the procedures to be taken to make a complaint to the ABA? [5.5(c) and 5.6]
   [ ] yes [ ] no

PART D: Other matters

8. Is there a complaints procedure in place to deal with complaints about unsolicited emails promoting sites containing Prohibited Content? [5.7]
   [ ] yes [ ] no

9. Is there a procedure in place (for example a contact person in your organisation with an email capability) which permits you to notify another ICH in cases where you are advised (for example by the ABA) that:
   - the ICH is hosting Prohibited Contract and
   - you know their email address? [5.8]
   [ ] yes [ ] no

   *This provision in our Code was required by legislation. For most practical purposes of course, one would expect that the ABA would notify the relevant ICH directly

PART E: Non-Code Requirements

[The IIA Code does not require these points, but it may assist in compliance with an ABA direction generally, therefor is a useful capability to have]

10. Is the ABA aware of the details of your Contact Point and that all correspondence should be directed to the Company Secretary and the Contact Point?
   [ ] yes [ ] no

11. Do the Primary Server Administrators have remote administrative access via telnet over all relevant servers?
   [ ] yes [ ] no
Content Code 2 Requirements Checklist

PART A: Designated Notification Scheme
1. Has a Supplier(s) of an Approved Filter(s) been nominated by you? [6.1(a)]
   [] yes [ ] no
2. Has you informed the ABA of your Contact Person’s details, including his/her email address and also your Company Secretary details? [6.1(b)]
   [] yes [ ] no

PART B: Access Prevention
(Part B is not applicable to subscribers appearing on a list created under Part C)
4. Has a Scheduled Filter been ‘provided for use’ to each subscriber as part of:
   (a) an online registration process; or
   (b) a disk based registration process; or
   (c) a notification with links to effect download and instructions for use? [6.2(a)]
   [] yes [ ] no
5. Are commercial subscribers provided with:
   (a) appropriate software (eg an Scheduled Filter) that prevents access; or
   (b) information that facilitates access to consultancy services with respect to firewalls or other appropriate technology? [6.2(b)]
   [] yes [ ] no

PART C: Designated Alternative Access Prevention Arrangements
1. Is there a list of:
   (a) commercial subscribers who have advised you that they have in place a form of content filtering or control (eg firewall technology); [6.4(a)]
   [] yes [ ] no
   (b) schools, educational or other institutional subscribers who have advised you that they have in place a form of content filtering or control (eg firewall technology); and [6.4(b)]
   [] yes [ ] no
   (c) other subscribers that have advised that he/she has already installed an Scheduled Filter? [6.4(c)]
   [] yes [ ] no

Content Code 3 Requirements Checklist

PART A: Internet Content Subscription Account Registration
(at least one question in this part must be answered ‘Yes’ to comply with the Code)
1. Does your Internet Content Subscription Account Registration require that the customer provide their credit card number and expiry date? [7.1(a)]
   [] yes [ ] no
2. Does it ask that the customer provide documentation such as a passport, driver’s licence or student card with date of birth or age? [7.1(b)]
3. Is there a prominent notice, on the site or promotional material which markets the Internet subscription account, that states that persons under 18 need the consent of a parent, teacher or other adult before using the account? [7.1(c)]

[ ] yes [ ] no

4. Is a service, such as an Scheduled Filter or a closed content system, offered when the account is opened? [7.1(d)]

[ ] yes [ ] no

5. If a Scheduled Filter is offered for a charge, is this charge based on a cost-recovery (having regard to your total costs of obtaining, supply, and supporting the filter), as opposed to for-profit?. [6.2(b)]

[ ] yes [ ] no

6. Does the registration site ask persons opening the account to confirm that they are not under 18? [7.1(e)]

[ ] yes [ ] no

PART B: Content Provider Customers

6. Is there a link on the home page to resources, made available by the IIA, the ABA, NetAlert or other approved organisation, that:

(a) encourages the use of a labelling system been used (in relation to content unsuitable for children)? [7.2(a)]

[ ] yes [ ] no

(b) informs content provider customers of their legal responsibilities in relation to content? [7.2(b)]

[ ] yes [ ] no

7. Is there a term in the hosting contract or an acceptable use policy that informs Content Providers not to place on the Internet content in contravention of any Australian law? [7.5]

[ ] yes [ ] no

PART C: Informing Subscribers

8. Is there a link on the home page to resources made available by the IIA (for example www.iia.net.au/contentcodeguideuser.html), the ABA, NetAlert or other approved organisation (approved by the IIA) to inform subscribers:

(a) about supervising and controlling children’s access to the Internet; [7.3(a) and 7.4]

[ ] yes [ ] no

(b) about the availability and use of filtering software ? [7.3(b) and 7.4]?

[ ] yes [ ] no

9. Is there a term or statement in the hosting contract, or an acceptable use policy, or a notice on your home page, or a link to information for the purpose of informing users about:

(a) their right to make complaints to the ABA about content; [7.6(a) and 7.7]

[ ] yes [ ] no
(b) the procedures to be taken to make a complaint to the ABA? [7.6(b) and 7.7]

[ ] yes [ ] no

PART D: Take-down notices

10. Is there a procedure in place to, within the timeframe required:

(a) remove Prohibited or Potential prohibited content? [7.9(a)(i)]

[ ] yes [ ] no

(b) take any other action requires by the Broadcasting Services Act 1992 in respect of a notice? [7.9(a)(iii)]

[ ] yes [ ] no

11. Is there a procedure in place to inform customers who place prohibited or potential prohibited content on the Internet that this conduct is a breach of the customer's service conditions? [7.9(b)]

[ ] yes [ ] no

PART E: Other matters

12. Is there a complaints procedure in place to deal with complaints about unsolicited emails promoting sites containing Prohibited Content? [7.8]

[ ] yes [ ] no

13. Are you aware that you must act in accordance with the direction of a Relevant Authority in respect of any other content (other than Prohibited or Potential prohibited content)? [7.10]

[ ] yes [ ] no

14. Is there a procedure which requires notification to another Content Host if you become aware that they are hosting Prohibited Content? [7.11]

[ ] yes [ ] no

Email advice to IIA:
Please email this advice to compliance@iia.net.au
We confirm that we are compliant with the relevant IIA Codes according to the checklist published by the IIA for that purpose.
Name of ISP/ICH:
Contact person:
Email address:
Phone:
We are [ ] are not [ ] members of the IIA
Appendix 2: Family Friendly ISP News Release

Internet Industry Association

NEWS RELEASE

Tuesday, 26 March 2002
For Immediate Release

IIA Launches Family Friendly ISP Program

The Internet Industry Association, Australia's national body for the internet, today launched a nationwide scheme aimed at enhancing the ability of families to take better control over the kind of material their children can access online.

The "IIA Family Friendly ISP Program" is an important initiative, by which internet service providers can demonstrate in a readily identifiable way, their compliance with the IIA Codes of Practice and industry best practice standards for empowering end users.

The scheme, which is the first of its kind in the world, has the support of the Australian Broadcasting Authority and the community advisory body, NetAlert.

ISPs who are compliant with the industry Codes of Practice, which also covers access to online gambling services, will be entitled to display a special seal - the "Ladybird Logo". Australian families who are concerned about online content are encouraged to use an ISP who displays this trustmark on their websites.

Under the IIA coregulatory scheme, ISPs are required to provide for use both information and tools ('filters') for those of their customers who need help and advice in how to best to protect their children online.

The IIA supports the provision of filter under the legislation as they may assist some families in managing children's access to internet content. However, filters provided by IIA Code compliant ISPs are not intended to replace parental supervision.

Major ISPs have moved quickly to welcome the scheme, along with many smaller ISPs who see this as a value added service to their customers.

In embracing the scheme, OzEmail CEO Justin Milne said: "As the internet becomes essential to more and more families it is extremely important for them to be able to recognise ISPs and Internet businesses which conform to the high standards required by the IIA's family friendly badge."

Martin Dalgleish, Managing Director, Optus Consumer and Multimedia, said 'Optus is a strong supporter of measures which allow consumers to enjoy all the benefits that the internet offers, while protecting themselves and their children against access to inappropriate material. The IIA's new scheme will help consumers in choosing an ISP which offers those protective measures.'

General Manager, Business Management in Broadband and Online Services, Omar Khalifa, said "Telstra supports initiatives like this to help internet users have a positive online experience. We
have been involved in the development of the Codes of Practice and congratulate the IIA for pushing through with this initiative."

Amanda Lacaze, CEO, **AOL Australia**, said: "At AOL, we are committed to building confidence and trust in the online medium. This is reflected in the services and tools we provide, such as AOL Parental Controls. The IIA's Family Friendly ISP initiative will help Australian families determine, at a glance, which online service providers empower them to take control of their children's online experience."

Gaynor Gravestock, Internet Services General Manager at **UQconnect** added "This is a great initiative that finally recognises the efforts of those ISPs who work hard to protect and support their clients, through compliance with the Internet Code of Practice. UQconnect will be proud to wear the 'IIA Family Friendly ISP' seal."

Luke Mackinnon, Managing Director, **Planet Netcom Pty. Ltd**, said "As a regional provider, we understand the need for our users to have access to useful tools and information about internet content. We are delighted to support the "IIA Family Friendly ISP Program", as it will enable the ISP community to demonstrate its willingness to empower users with more choice over the kind of content accessible in the home."

Internet users who click on the ladybird seal will be taken to an information page which explains how the scheme works and what they need to do to take advantage of the services offered by ISPs under the plan.

More information about the scheme can be found at [www.iia.net.au](http://www.iia.net.au).

Ends.

---

For further comment contact:  
Mr Peter Coroneos  
Chief Executive  
Internet Industry Association (IIA)  
Phone: +61 2 6232 6900  
(for TTY callers, please call 133 677 and ask for 6232 6900)  
PO Box 3986 MANUKA ACT  
AUSTRALIA 2603  
http://www.iia.net.au
Appendix 3: IIA Scheduled Filters

The following filters are currently scheduled in the IIA Content Codes.

1. AOL PARENTAL CONTROL
2. ARLINGTON CUSTOM BROWSER
3. CONTENT KEEPER
4. CYBER PATROL
5. CYBER SENTINEL
6. EYEGUARD
7. INTERNET SHERIFF
8. I-GEAR
9. INTERSCAN WEB MANAGER
10. KIDZ.NET
11. NET NANNY
12. N2H2
13. TOO C.O.O.L
14. WEBSENSE
15. CYBERSITTER
16. NORTON INTERNET SECURITY
17. SMART FILTER
18. X-STOP
19. X-STOP R2000