



**Australian
Broadcasting
Authority**

Australia
**A Case Study on Internet
Content Regulation**

**UNESCO Symposium
Paris
15/16 November 2002**

**Andree Wright
Director, Industry Performance and Review
Australian Broadcasting Authority
Sydney**

Abbreviations

ABA:	Australian Broadcasting Authority
the Act:	the <i>Broadcasting Services Act 1992</i>
ICH:	Internet content host
ICRA:	Internet Content Rating Association
IIA:	Internet Industry Association
INHOPE:	Internet Hotline Providers in Europe Association
ISP:	Internet services provider
OFLC:	Office of Film and Literature Classification
PC:	personal computer
R:	Restricted category (18+) under the National Classification Code
RC:	Refused Classification category under the National Classification Code
the scheme:	the co-regulatory scheme for Internet content, established by Schedule 5 of the <i>Broadcasting Services Act 1992</i>
SIAP:	the European Commission's Safer Internet Action Plan
spam:	unsolicited commercial bulk email
X:	Consensual sexually explicit material category under the National Classification Code

Introduction

Internationally, approaches to Internet content regulation have combined a range of measures in comprehensive strategies, with responsibility shared by government, industry and the community. For example, the European Commission's Safer Internet Action Plan, now known as eSafe, contains initiatives in the areas of hotlines, content rating and filtering, user education and awareness, and industry codes of practice, with scope for government, industry and community involvement in each area.

Australia has had similar initiatives in place since 1 January 2000 through a co-regulatory scheme that also has roles for government, industry and the community. Australia's scheme provides a case study that endeavours to balance adults' rights to freedom of expression with protection of children from illegal and unsuitable content on a global medium. It is a scheme that incorporates formal review points and mechanisms in order to maintain flexibility in adapting to technological and social changes.

It is the view of the Australian Broadcasting Authority (the ABA) that the scheme has operated effectively to address community concerns about Internet content, identified in research prior to the scheme's introduction, in a way that has not placed unnecessary burden on the Internet industry, and has encouraged Internet take-up in Australia. At the time of the scheme's introduction, around one-fifth of Australian households had access to the Internet. This figure has now grown to over one-half, with many more users having access through school or the workplace.

This paper sets out the component parts of the scheme, explains how it has worked to date and draws out particular principles and actions for consideration by this symposium. The scheme's key components are:

- a complaints hotline,
- industry developed codes of practice, and
- community education.

The scheme supports an international co-operative approach to these key elements and gives the ABA a statutory role in relation to international liaison and co-operation.¹ In implementing the scheme we have been guided by the maxim "Think globally. Act locally".

¹ The Broadcasting Services Act assigns the ABA the function of liaising with regulatory and other relevant bodies overseas about co-operative arrangements for Internet content regulation, particularly through the development of multilateral codes of practice and content labelling technologies (clause 94(e)).

Scope of scheme

The scheme:

- defines certain types of Internet content as prohibited content (or potential prohibited content);
- provides for the development of industry codes of practice or ABA Standards for Internet service providers (ISPs) and Internet content hosts (ICHs), and gives the ABA power to direct compliance where necessary;
- creates a mechanism through which members of the public may complain to the ABA about Internet content which they believe is, or may be, prohibited content;
- applies to the activities of ISPs and ICHs, requiring them to take certain action in relation to categories of Internet content that are defined as prohibited content;
- empowers the ABA to investigate complaints and, where appropriate, issue notices to ICHs/ISPs directing them to take action in relation to such content; and
- makes non-compliance with a notice an offence.

It is important to note that while the Broadcasting Services Act (the Act) provides a legislative framework and a ‘safety net’ for regulation, the emphasis of the scheme is on the desirability of the industry developing measures for addressing the availability of illegal, offensive and harmful material.

Internet content

Clause 3 defines Internet content as:

Information that:

(a) is kept on a data storage device; and

(b) is accessed, or available for access, using an Internet carriage service;

but does not include:

(c) ordinary email; or

(d) information that is transmitted in the form of a broadcasting service.

In practice, the scheme applies to information on world wide web (WWW) sites, Usenet newsgroups, File Transfer Protocol (FTP) sites, and other stored content. The definition of Internet content does not cover ‘live’ material such as chat services or voice over the Internet.

Prohibited content

The scheme is based on the principle that what is illegal offline should also be illegal online.

The Government decided that proscribed Internet material would include content that, if published in another format, would be illegal or restricted in its availability. The Government therefore considered it a logical step to legislate to extend certain elements of the existing classification system, established to provide guidance to the community and already familiar to the community through its application to film, television and other media, to the Internet.

This system flows from the principles set out in Australia's National Classification Code:

- adults should be able to read, hear and see what they want;
- minors should be protected from material likely to harm or disturb them;
- everybody 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, particularly sexual violence; &
 - the portrayal of persons in a demeaning manner.

Accordingly, the R, X and RC classifications used by the Office of Film and Literature Classification (OFLC) serve as reference points for the assessment of Internet content in relation to illegal material or material of adult nature, and the following categories of Internet content are prohibited content²:

- Content which is classified RC or X, which includes:
 - ⇒ material containing detailed instruction in crime, violence or drug use;
 - ⇒ child pornography;
 - ⇒ bestiality;
 - ⇒ excessively violent or sexually violent material; and
 - ⇒ real depictions of actual sexual activity.

² Content that has not been classified by the OFLC but which would, if classified, be likely to be prohibited content, is known as potential prohibited content and in most cases is dealt with as though it were prohibited content.

- Content hosted in Australia, which is classified R *and not subject to a restricted access system*³. Content classified R is not considered suitable for minors and includes:
 - ≡ material containing strong violence or sexual violence;
 - ≡ material containing implied or simulated sexual activity; and
 - ≡ material that deals with issues or contains depictions which require an adult perspective.

The OFLC's Guidelines For Classification of Films and Videotapes⁴ provide further information about the types of material contained in each of these categories.

Industry codes of practice

The IIA Codes of Practice

The Internet industry in Australia, through the Internet Industry Association (IIA), has developed three codes of practice. Content Codes 1 and 2 cover the activities of ISPs while Content Code 3 deals with the responsibilities of ICHs⁵. While the codes were developed by the IIA, whose ISP⁶ and ICH members account for the majority of Australian Internet users, the codes apply to all participants in these sections of the Internet industry. The IIA codes were first registered by the ABA in December 1999 and, following an industry review, replacement codes were registered on 9 May 2002.

Taken together, the IIA codes contain a range of measures to assist end-users to manage access to Internet content for themselves and their children. A specific provision, which I would draw your attention to is the mechanism - known as the 'designated notification scheme' - for dealing with prohibited content hosted outside Australia.

Under the procedures set out in Content code 2, ISPs are required to offer end-users one of the filter products or services that are listed in the Schedule to the code (unless satisfied that a user has made alternative arrangements that are effective in preventing access to such content). The IIA and the ABA agree that no-one who would like to use a filter is impeded from doing so because of problems with cost, availability or ease of use. Accordingly, the IIA codes specify that while ISPs may charge for such a

³ The criteria for a restricted access system are set out in Restricted Access Systems Declaration 1999 (No. 1), tabled in Parliament on 3 December 1999.

⁴ The guidelines can be obtained from the OFLC's web site at http://oflc.gov.au/PDFs/FilmVid_Guidelines.pdf

⁵ The current codes are available on the Internet Industry Association's web site at <http://www.iaa.net.au/contentcode.html> or on the ABA's web site at <http://www.aba.gov.au/internet/>.

⁶ There are approximately 600 ISPs in Australia today.

product or service, such a charge will not exceed the cost to the ISP of obtaining, supplying and supporting the filter.

Under this ‘designated notification scheme’, the ABA notifies the details of prohibited and potential prohibited content to the maker or distributor of each of the scheduled filters. The makers or distributors of these scheduled filters have agreed to update the products to give effect to notifications received from the ABA, thereby preventing users of the products from accessing the content. The maker or distributor of each product is also required under the code to provide the ABA with information about their procedures for receiving and actioning the ABA’s notifications.

It should be noted that the specific role of filters as part of this mechanism is distinct from their general role as a tool to help manage access to Internet content, particularly for families with children. The ABA acknowledges that current filtering technologies do not by themselves provide sufficient protection from potentially offensive and harmful content. It considers that, however, when used in conjunction with appropriate supervision by parents and household rules for Internet access, filters are effective tools to help manage access to Internet content and to control access by children to Internet content.⁷

In the ABA’s view, the industry codes requirement that ISPs provide users with a scheduled filter for the purpose of the designated notification scheme has helped to raise community awareness of the use of filters for managing access to Internet content generally.

Code compliance

Compliance with the codes is monitored by the ABA. The IIA has advised the ABA that the majority of its ISP members, which together account for some 80 per cent of Internet users, are fully compliant with the codes. The ABA has received no complaints about non-compliance with the codes, but has raised compliance issues with a small number of ISPs that have come to the ABA’s attention. Most matters have been promptly resolved to the ABA’s satisfaction.

The ABA also notes the recent initiative of the IIA to promote compliance with the codes through its ‘Look for the Ladybird’ program, which entitles ISPs who are fully-code compliant to display the IIA’s ‘family friendly’ ladybird seal. Users who click on this logo will be able to view an information page informing them about the scheme and how to use the family friendly services offered by participating ISPs. The ABA understands that seven ISPs now display the logo.

⁷ As part of its statutory role in monitoring developments in Internet technologies, the ABA has had regard to projects funded by the European Commission’s Safer Internet Action plan to develop more reliable and effective filtering technologies. As part of this process, the ABA was represented at a workshop convened by the European Commission, where a range of prototype technologies was presented. Subsequently information about these developments has greatly assisted the ABA’s own work in evaluating the effectiveness of existing filter products, analysing likely future trends in the availability of filter products and making this available to the IIA and users.

International perspectives

Parallel to the development of the Australian codes of practice, considerable work has been done internationally on possible best practice models. These matters have been discussed for example, by the Bertelsmann Foundation's International Network of Experts on Content Self-Regulation⁸, of which the ABA was a member. From such discussions the ABA suggests that the criteria for successful content-related codes are likely to include:

- A. Development of a code by the relevant industry body, taking into account the particular circumstances of different sections of the Internet industry;
- B. Voluntary subscription to codes, backed by regulatory mechanisms to encourage their adoption by industry members;
- C. Participation of relevant regulatory authorities in the development of a code;
- D. Consultation with users and the community in development of a code, and in regular review of a code's operation;
- E. Inclusion in a code of procedures for dealing with illegal material, and measures dealing with the provision of information and tools to users that will assist them in managing access to content that is potentially offensive or harmful
- F. Regular review of the code's operation to take account of changing technologies and community views.

The ABA considers that the Australian codes of practice meet these best practice criteria to a high degree.

Complaints hotline

Research on ways to deal with illegal Internet content has identified significant community support for complaint 'hotlines' and the investigation of Internet content under the Australian scheme is primarily complaint driven.

Safeguards for industry

In considering possible options for operation of a hotline, the Government decided that it would not be reasonable for Internet service providers to be the first point of

⁸ Machill, M and Rewer, A (2001), Internet Hotlines – Evaluation and Self-regulation of Internet Content, Verlag Bertelsmann Stiftung, Gutersloh 2001; and Price, M. E. and Verhulst, S. G. (2000), Codes of Conduct and Other Self-regulatory Documents, paper presented at Bertelsmann Foundation Workshop on Self-regulation of the Internet, Hannover on 30 June 2000.

contact for resolution of complaints and that, to ensure that complaints were resolved in a timely and cost-effective way with minimal burden on the Internet industry, complaints would be made directly to the ABA.

Consistent with this approach, the Government also decided that ISPs and ICHs would not be required to monitor content accessed through or hosted on their services and the scheme includes a provision that indemnifies ISPs and ICHs against liability they may otherwise have under any 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.

Complaint handling

The ABA investigates all valid complaints about prohibited or potentially prohibited material and, as part of an investigation, the ABA may request the OFLC to classify the content.

(The investigative process is set out at attachment A.)

To facilitate easy lodgement and prompt investigation of complaints, an online complaint form is available on the ABA's web site at <http://www.aba.gov.au/internet/>. The form enables complaints to be lodged online at the time the user encounters problematic material, and helps to ensure that complaints contain all information required by the ABA to undertake an investigation.

If the content is hosted in Australia and is prohibited, or is likely to be prohibited, the ABA will direct the ICH to remove the content from their service⁹. The Act requires that an ICH must comply with a notice by 6.00pm on the business day after the notice was issued, and makes non-compliance an offence. The ABA has a range of options for enforcing compliance with a notice, including seeking an order from the Federal Court that the ICH cease hosting Internet content, and prosecution.

To date, all ICHs have complied with notices applying to them within the required timeframe, and the enforcement powers available to the ABA have not been required.

If the content is not hosted in Australia and is prohibited, or is likely to be prohibited, the ABA will notify the content to the suppliers of scheduled filters in accordance with the registered IIA code of practice. If the content is also sufficiently serious (for example, illegal material such as child pornography), the ABA refers the material to the appropriate law enforcement agency, or another hotline (see below).

Activity to date

The ABA received over 1500 complaints about Internet content since 1 January 2000. Around 65% of the complaints investigated were found to be 'prohibited content'.

⁹ Where content has not been classified, the ABA issues an interim take-down notice to the ICH and asks the OFLC to classify the content. When the content has been classified, the ABA advises the ICH of the classification and, if necessary, issues a final take-down notice to the ICH.

Some 85 per cent of complaints have concerned content on the world wide web, with the remainder being concerned with content in Usenet newsgroups (14 per cent) and other stored content (less than 1 per cent).

Over half of all items¹⁰ actioned by the ABA to date have constituted child pornography. As child pornography is a trans-national crime and each image is potentially that of a crime scene, the ABA refers such items to the appropriate INHOPE (Internet Hotline Providers in Europe Association) hotline or enforcement agency. At 30 June 2002, the ABA had referred about 550 items of such content hosted outside Australia to the Australian Federal Police and/ or the hotline in the relevant country, and 135 items of Australian-hosted content to the relevant State or Territory police service. Some items were referred to two or more agencies.

INHOPE

Internet hotlines can play a vital role in ensuring prompt action in investigating illegal material such as child pornography, particularly when they operate as an international network and have close working relationships with law enforcement agencies¹¹. Prompt investigation of such material is important from the point of view of restricting its availability and addressing child abuse situations associated with the production of such material.

In addition to being an effective mechanism for dealing with specific complaints, INHOPE is a valuable forum for exchange of information and expertise in a range of areas of hotline operation, including complaint investigation techniques and occupational health and safety.¹²

An INHOPE accredited hotline is defined as one that:

- provides a mechanism for receiving complaints from the public about alleged illegal content;
- has effective transparent procedures for dealing with complaints; and
- has the support of government, industry, law enforcement and Internet users in their country.

INHOPE is partly funded by the European Commission under the hotline component of its Safer Internet Action Plan (now called eSafe), to deal with complaints about

¹⁰ Some investigations involve more than one item of content.

¹¹ Machill, M and Rewer, A (2001), Internet Hotlines – Evaluation and Self Regulation of Internet Content, Verlag Bertelsmann Stiftung, Gutersloh.

¹² INHOPE hotlines also work out of session through working groups, which were established earlier this year to develop operational guidelines and resources for member hotlines. The ABA chairs the working group on content issues, which has developed guidelines for investigating content peer-to-peer content. Other working groups have established guidelines for exchange of information between member hotlines, raising community awareness of hotlines, and statistical reporting.

illegal Internet content, predominantly child pornography. Current membership of INHOPE¹³ includes 16 hotlines from 14 different countries: Austria, Belgium, Denmark, France, Germany, Iceland, Ireland, The Netherlands, Sweden, Spain and the United Kingdom, with the ABA and the Cybertip Line in the United States as associate members. Some INHOPE hotlines, such as the Internet Watch Foundation (UK) are industry initiatives; others such as the Cybertipline (USA) are community-based and privately sponsored. Others such as the ABA hotline are government-based or child welfare initiatives such as Save the Children (Denmark).

Hotline evaluation

Criteria for assessing the effectiveness of hotlines have been developed internationally in order to guide their operation and assist evaluation of their performance. The ART and ART2¹⁴ principles have been developed by the Bertelsmann Foundation and implemented through INHOPE. They establish six criteria for effective hotlines:

- **Available** – demonstrated by the visibility and accessibility of the hotline.
- **Reliable** – with reference to the effectiveness of the hotline in managing security, confidentiality, and privacy.
- **Transparent** – having regard to the organisation administering the hotline, the criteria used to assess material, the investigation process used by the hotline, and the hotline's relationships with other agencies and stakeholders.

And

- **Accountable** – to the public, the Internet industry, the community and other agencies and stakeholders with whom the hotline works.
- **Responsible** – for educating the industry and Internet users, upholding civil liberties, and for responding to complaints formally and effectively.
- **Trustworthy** – in operating according to the ART principles, upholding professional standards and ensuring the quality of hotline responses.

The ABA has been guided by these criteria in establishing and operating its complaint hotline.

Community education

There is international recognition that community education and awareness raising is a core component of an effective strategy to deal with Internet content issues. This is in part due to recognition that the vast and global nature of the Internet diminishes the effectiveness of traditional regulatory responses to content related issues.

¹³ See www.inhope.org

¹⁴ The ART and ART2 principles have been developed by the Bertelsmann Foundation and Internet Hotline Providers in Europe Association (INHOPE), in association with Professor Herbert Burkert.

Within this context, the Australian scheme aims to encourage the take-up of Internet services and give users confidence in the Internet by providing resources that are appropriate to the needs of users. Reflecting the co-regulatory nature of the scheme, responsibility for community education is shared between government, the Internet industry and a community/industry body known as NetAlert.

ABA Action

Research has played an important role in informing the development and implementation of the co-regulatory scheme. The community education activities of the ABA have been 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.

Following commencement of the scheme, the ABA commissioned the “Internet@home”¹⁵ research project. Its findings have been a key input to community education activities undertaken by the ABA, for example, distributing information through schools and libraries and advertising in relevant publications and, in particular, the development of its Cybersmartkids web site, www.cybersmartkids.com.au which replaces the ABA’s Australian Families Guide to the Internet website.

In response to the findings of this research, the ABA has also undertaken a range of other initiatives to meet the information needs of the community; for example, the Cybersmartkids website is complemented by a range of offline materials that support its messages and target parents as well as children. A series of brochures contains general Internet safety tips, information about filter software¹⁶ and avoiding and managing unsolicited email (Spam).

These brochures are currently being distributed by the major Education Department in Australia as a community education initiative.

¹⁵ Copies of the report can be downloaded from the ABA’s web site at <http://www.aba.gov.au/internet/research/>.

¹⁶ The ABA and NetAlert jointly commissioned a 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. In framing and analysing the results of this research, the ABA had regard to international developments in the area of filtering, particularly initiatives being undertaken in Europe to objectively measure the effectiveness of existing products and services, and develop more effective and reliable filtering technologies. The full report can be accessed at <http://www.aba.gov.au/internet/research/filtering/index.htm>

Preserving freedom of expression

It is important to note at this point that the key decision points under the co-regulatory scheme are subject to review processes in order to ensure that protection of minors is well balanced by the right to freedom of expression. An ICH for example can apply to the Classification Review Board to review a classification decision as to whether material is prohibited as can an ISP, the Minister, the ABA and a person aggrieved by the decision.

An ISP or ICH can also apply to the Administrative Appeals Tribunal for review of a decision by the ABA to issue a take-down notice or to request the Classification Board at the OFLC to classify Internet content hosted in Australia. Under section 5 of the *Administrative Decisions (Judicial Review) Act 1977* a person aggrieved by an administrative decision under schedule 5 may seek review in the Federal Court.

None of these appeal mechanisms have been exercised to date.

Other accountability measures built into the scheme from its inception include reports on the operation of the scheme that are tabled in Parliament every six months, regular review of the industry codes of practice, and a statutory review of the scheme after 3 years of operation.¹⁷ The scheme is therefore subject to ongoing scrutiny and, like the technology it regulates, will no doubt evolve over time.

¹⁷ see discussion paper calling for submissions on the operation of the scheme at http://www.dcita.gov.au/download/0,6183,4_111735,00.doc

Concluding remarks

The Australian scheme embodies a co-regulatory approach that acknowledges that the protection of children online requires a comprehensive and co-ordinated package of initiatives. It also emphasises the importance of informed user communities and of a global approach, mindful of cultural considerations.

In this regard the ABA notes that policy initiatives developed through international co-operation, such as the Bertelsmann Foundation's experts group, have been operationalised through organisations such as INHOPE. INHOPE has been able, through the ART principles, for example, to encourage hotline best practices in a context that respects the different legal and cultural values that different countries observe. The association with INHOPE has been one co-operative initiative that has kept Australia up to date not only with the work of other hotlines but also with eSAFE initiatives generally.

Based on the experience of the Australian scheme to date we believe the following principles to be important:

- Build on best practice initiatives and guidelines already developed (such as the ART best practice principles for hotlines).
- Encourage partnerships between industry, government and the community with roles clearly defined roles and mindful of cultural considerations.
- Material that is illegal offline such as child pornography should be illegal online, but have checks and balances in place via appeal mechanisms, regular reviews and transparent processes in order to balance freedom of expression and protection of individual and collective rights in cyberspace.
- Endorse the principles:
 - ✓ adults should be able to read, hear and see what they want;
 - ✓ minors should be protected from material likely to harm or disturb them; &
 - ✓ everybody should be protected from exposure to unsolicited material that they find offensive.
- Promote awareness and education initiatives that are carefully targeted to particular audiences, address their needs and reach those audiences effectively in order to foster an informed Internet user community.
- Review and adapt to take account of technological and social changes.
- Think globally, act locally.