Australian Government

acma

Australian
Communications
and Media Authority

# Submission to the National Classification Scheme Review

NOVEMBER 2011

communicating | facilitating | regulating

**Canberra**
Purple Building
Benjamin Offices
Chan Street
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

**Melbourne**
Level 44
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

T +61 3 9963 6800
F +61 3 9963 6899

**Sydney**
Level 5
The Bay Centre
65 Pirrama Road
Pyrmont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

T +61 2 9334 7700
1800 226 667
F +61 2 9334 7799

Published by the Australian Communications and Media Authority

# Executive summary

The ACMA sees merit in the enactment of a new National Classification Scheme. Its experience suggests that this will significantly improve clarity and efficiency for citizens, industry and Government alike.

The ACMA's experience also supports the idea of one regulator being responsible for the regulation of media content under the National Classification Scheme. It is considered that there would be benefit to citizens, industry and Government in having one regulator with which to interact and transact.

In relation to specific proposals, the ACMA:

- Expresses concern about the practical implications of the proposals to require all X18+ and RC material to be classified;
- Queries the intention of including a C classification category and whether it is meant to supersede or complement the current C and P scheme under the *Children's Television Standards 2009*;
- Supports the proposal to provide for the development of industry classification codes of practice, recommending careful consideration as to how these codes would dovetail with the various current television code regimes which cover both classification and other broader matters; and
- Emphasises the challenges inherent to online content regulation and the need for technology neutral provisions in this area.

# Centrepiece proposals

## The Proposed Classification Scheme

The ACMA is an independent statutory authority with jurisdiction encompassing broadcasting, the internet, radiocommunications and telecommunications. It responds to complaints, undertakes investigations and registers industry codes of practice in relation to the classification of broadcasting and internet content. It also conducts National cybersafety educational programs (see Attachment A) and National cybersecurity programs (see Attachment B).

The ACMA sees merit in the enactment of a new National Classification Scheme. Its experience suggests that this will significantly improve clarity and efficiency for citizens, industry and Government.

The ACMA notes the ALRC's proposal to move the classification related parts of the *Broadcasting Services Act 1992* (BSA) into a new Classification of Media Content Act. This will require careful consideration of how these parts of the BSA relate to other parts of the Act such as the objects, the provisions relating to program standards and codes of practice and the broadcasting licence conditions set out at Schedule 2 of the BSA.

## The Regulator

The ACMA's experience supports the notion of one regulator being responsible for the regulation of media content under the National Classification Scheme. It is considered that there would be benefit to citizens, industry and Government in having one regulator with which to interact and transact. It considers that a single regulator would be:

> Better for citizens: a single approach to the application of community standards and protections within the new scheme.
> Better for the consumer: a one stop shop with less chance of being given 'the run-around'.
> Better for industry: superior, faster decision-making with increased expertise and a consistent approach.
> Better for Government: cost savings from economies of scale.
> More logical: converging platforms will incontrovertibly require a converged regulator.

In particular, a single classification regulator is likely to be more effective and efficient in key areas of content regulation such as:

> Complaints handling, investigations and enforcement.
> Negotiating, approving and registering codes of practice.
> Liaising with relevant Australian and overseas regulators and law enforcement agencies.
> Assisting with the development of relevant law and policy, as well as providing expert advice to government.
> Encouraging, monitoring and enforcing compliance across its regulatory remit.

The ACMA also notes that, as many issues in communications and media regulation are inherently inter-dependent and inter-connected, systems and processes would be required to ensure the smooth interaction between such a regulator and other agencies with a role in media regulation or law enforcement. For example, there are obvious synergies with the making of technical standards in relation to the transmission and reception of digital television in regard to parental locks.

Further areas where broader communications and media regulation is likely to intersect with classification regulation include the following:

> The handling of complaints, investigations and relevant enforcement are functions required in relation to all codes, conditions and standards applicable to the media and communications industry, as is encouraging, monitoring and enforcing compliance. Enforcement, and systemic industry specific issues such as poor complaints handling, will need to be dealt with effectively across all areas of regulation and with full access to all relevant enforcement measures.

> Promoting the development of industry codes of practice as well as approving and maintaining registers of such codes is currently required for a wide range of media and communications industry matters, both of a content and technical nature. There are also a large range of other registers and databases. These will need to be efficiently and effectively utilised across all areas of regulation.

> Liaison and interaction with relevant Australian and overseas media content regulators and law enforcement agencies is crucial in the areas of online content regulation, cybersafety and cybersecurity.

> Educational activities need to be undertaken in a comprehensive and holistic way across the whole range of matters that arise in a fast moving digital environment to ensure maximum integration of ideas, knowledge creation and coherent educational messages.

# Comment on specific proposals

## Classification of all content likely to be classified X18+ or RC

The ACMA has some concern with the Discussion Paper proposals that all media content that may be X18+ or RC must be classified (proposals 6-4 and 6-5). It is noted that these proposals are made despite acknowledgement that many content providers provide such a large quantity of content that this is clearly impractical (paragraphs 6.73 and 6.77 refer). With respect to X18+ material, the rationale seems to be the need to make clear Australia's standard on what may be acceptable to display in sexually explicit content (paragraph 6.73) and, in relation to RC material, the need to determine whether something should be banned entirely (paragraph 6.74).

However, in the ACMA's view, enacting a law in circumstances where it is acknowledged that it cannot be complied with, or effectively enforced, is likely to lead to a low regard for such a law and, as a consequence, a significantly diminished culture of compliance. This would significantly undermine the law's overall purpose.

It is suggested that, in relation to online content, any new model might well be based on the current system which uses the internationally recognised approach of take-down notices where the content is illegal, and close relationships with law enforcement agencies, both domestically and internationally. The ACMA's suggested approach would not be inconsistent with the Government's policy to block RC content, which is aimed at disrupting access.

The further proposal of requiring classification of content by the Classification Board that is likely to be RC before charging a person with an offence, issuing a person with a notice to stop distributing the content or adding the content to an ISP blocking list (should one exist) could work, provided the dynamic nature of such content is taken into account (for example by capturing a copy of the content and identifying its source as soon as possible) and that such classifications could be done quickly (ideally within two business days) and not involve too much by way of double handling by the regulator and Classification Board. This would be assisted by the Classification Board being co-located with and supported by the regulator. It might, however, be appropriate to have provision for interim take-down or ISP blocking notices to be issued by qualified staff for 'potential prohibited content' to avoid problems if there is delay in the Classification Board's classification.

The role of overseas lists of child abuse material such as those maintained by the Internet Watch Foundation, Interpol and the National Center for Missing and Exploited Children, in relation to either end-user filters or ISP blocking is not clear and it is suggested that this might usefully be further considered and explained.

## C and P Classification

The Discussion Paper proposes a new C classification category for programming specifically made for children (proposal 9-2). However, while referring to the requirements in the current *Children's Television Standards 2009* (CTS) and the inclusion there of the P category, the rationale, scope and policy intent of the proposal to include a C category that may be used by all classifiers for all media are not fully articulated (paragraphs 9.21-9.26).

The ACMA suggests clarification as to whether the proposal is seeking to supersede or supplement the current C and P classification system that caters to children aged under 14 years and those not yet of school age, respectively.

If the proposal is to complement the current system, it poses potential conflict with the understood C and P classification categories (and symbols) and the reliance of much of the CTS on these categories. It can be expected that consumers will be confused if a C classification for TV means one thing but a C classification on another media platform means another. Also consumers might not understand why television has a P classification while other platforms do not.

If the proposal is to replace the current system, then to achieve the aim of the BSA and CTS of not just having programming specifically made for children but quality, well-produced programs which are developmentally appropriate for either C or P aged children, it would have to keep both the C and P categories and need to incorporate criteria similar to those currently used, whereby a program needs to:

- be made specifically for children;
- be entertaining;
- be well produced using sufficient resources to ensure a high standard of script, cast direction, editing, shooting, sound and other production elements;
- enhance a child's understanding and experience; and
- be appropriate for Australian children.

## Codes of Practice

The ACMA notes and supports the proposal to provide for the development of industry classification codes of practice (proposal 11-1). In this regard, careful consideration will be needed as to how these codes would dovetail with the various existing television and online code regimes which cover both classification matters and other broader areas. This is necessary to ensure future code development does not undermine the potential benefits of the new classification scheme of clarity and cost effectiveness for both consumers and industry.

## Issues relating to regulating online content

The ACMA would like to emphasise the challenges inherent in the area of regulating online content, particularly regarding technical matters related to the dynamic cross-jurisdictional nature of the content and important Occupation Health and Safety issues.

The complexity of these issues is highlighted by paragraph 7.63 of the Discussion Paper. There it is suggested that self-classifying of X18+ content would reduce the exposure of those dealing with and classifying such material and mitigate some of the health and safety issues. However, the viewing of X18+ material by the ACMA, at least in the online space, is in response to complaints (which are likely to be just as frequent) and the most pronounced health and safety impacts are, in any case, from child abuse material and from real depictions of actual violence (for example, explicit footage of beheadings or violent sexual assault).

A typical online content investigation into child abuse material involves a technical identification of where the content is located to determine the host jurisdiction and appropriate action. This identification often requires specialised knowledge and software. The content is then assessed under the provisions within the BSA*,* which are underpinned by the National Classification Scheme, and may require referral to the Classification Board for a classification decision or reference to existing classification decisions. Depending on the exact nature of the content, secure referral may be made to industry under applicable codes of practice and the relevant jurisdictional law enforcement agency or international bodies, to effect appropriate and timely action in relation to the content.

The ACMA has long-standing and well-developed protocols for staff welfare that apply where staff are required to view offensive and/or illegal content. In the ACMA's experience, the two types of viewing do not necessarily have the same effect on staff, with high end illegal content having a significantly greater impact as it often involves explicit depictions of young children and infants being victimised or extreme acts of real violence. The ACMA's staff welfare policy also contains specific provisions around recruitment suitability that include extensive background checks and appropriate security clearances in light of the sensitivities involved in viewing illegal and other material that may be of National security relevance.

Online content delivery, storage and distribution models are constantly evolving. To effectively control access to certain high end online content, any future Act will need to be framed in a sufficiently flexible, comprehensive and technology neutral way to encompass these multiple and constantly evolving avenues of online access.

For example, current distribution models for online content can effectively involve identical content accessed via the same URL being hosted in multiple locations, both in Australia and overseas. Both the take-down of content and ISP blocking are likely to be necessary if the comprehensive prevention of access to this content from within Australia is desired.

Attachment A

## The ACMA's Role in Cybersafety Education

## Overview of Cybersmart

Cybersmart is a national cybersafety and cybersecurity education program managed by the ACMA. The program is specifically designed to meet the needs of its target audiences of children, young people, parents, teachers and library staff, and is based on research into the needs of these audiences for cybersafety information.

Cybersmart aims to:

> **Inform** children, young people, parents, teachers and library staff about cybersafety issues.

> **Educate** audiences through information, resources and practical advice.

> **Empower** children and young people to be safe online.

The program includes:

> The comprehensive Cybersmart website and a range of information and resources designed to meet the needs of children, young people, parents, teachers, and library staff.

> The Cybersmart Outreach Professional Development for Educators program – a cohesive, full day program, tightly structured to meet the needs of the teacher audience. Over 10,000 teachers have now attended these workshops.

> The Pre-Service Teacher program for trainee teachers, educating future teachers on the trends and issues that will affect their students online, in school and in the home.

> The Online Professional Development program, Connect.ed, designed to complement our face-to-face Professional Development for Educators program. Over 3,000 teachers have registered for this course since its launch in May 2011.

> Internet Safety Awareness presentations for teachers, parents, teens and children –targeted one hour presentations, available in metropolitan and regional centres throughout Australia, and attended by over 360,000 people Australia-wide.

> The new video resource for teens, *Tagged,* dealing with cyberbullying, sexting, and digital reputation.

> Interactive Shared Learning programs Cybersmart Detectives and Cybersmart Hero, educating young people in an engaging and interactive format, and encouraging them to think for themselves about solutions to cybersafety issues. Over 28,000 children have participated in these activities to date.

> The Cybersmart Online Helpline: a service for young people who have experienced issues online.

> The Cybersafety Contact Centre: a national telephone centre providing online safety information, advice and access to resources for all Australians.

Attachment B

## The ACMA's Role in Cybersecurity

## Overview of the Australian Internet Security Initiative

The Australian Internet Security Initiative (AISI) is an important component of the government's E-Security National Agenda and aims to enhance the protection of home users and small to medium enterprises from electronic attacks and fraud by reducing the number of infected computers on the Australian internet.

The AISI, developed and managed by the ACMA, is a key tool to help address the e-security threat posed by 'botnets'—networks of computers that have become compromised through the surreptitious installation of malicious software (malware). This malware enables the computer to be controlled remotely for illegal and harmful activities, including the dissemination of spam, hosting of 'phishing' sites and distributed denial of service attacks on internet infrastructure.

Under the AISI program, the ACMA provides information to participating Australian ISPs about 'compromised' computers residing on their networks. The ISPs may then contact their customers to inform them that their computers are compromised and assist them in restoring correct operation.

During 2010–11, the ACMA sent an average of 16,464 reports of compromises per day to participants in the AISI. The high level of compromise reports per day made through the AISI underscores the need for internet users to be vigilant in maintaining the security of their computers and not engaging in practices—such as visiting 'suspect' websites—that cause their computers to become infected. The solution to the botnet problem requires a coordinated international approach, as botnets are made up of computers located in multiple countries.