EXPLANATORY STATEMENT

Issued by the authority of the Australian Communications and Media Authority

Restricted Access Systems Declaration 2007

Background

The *Communications Legislation Amendment (Content Services) Act 2007* (the Content Services Act) received Royal Assent on 20 July 2007 and inserts a new Schedule 7 into the *Broadcasting Services Act 1992* (the Broadcasting Services Act).

Schedule 7 amalgamates the regulation of all content services delivered via carriage services. It extends the internet content regulatory framework established under Schedule 5 to the Broadcasting Services Act to a broad range of content services delivered on convergent devices, including mobile premium services.

The Content Services Act also repeals large parts of Schedule 5 to the Broadcasting Services Act as it applies to content services and obligations on internet content hosts.

Under subclause 4(1) of Schedule 5 to the Broadcasting Services Act, access to internet content has been regulated by the *Restricted Access Systems Declaration 1999 (No.1)* (the 1999 Declaration). Stored internet content hosted in Australia which has been classified as R18+, or has not been classified, but would likely be classified as R18+ must be subject to a restricted access system which meets the requirements of the 1999 Declaration.

The 1999 Declaration specifies that a restricted access system must require:
- provision of the name of the applicant;
- a declaration that the applicant is at least 18 years or over; and
- proof of age supplied in the form of credit card details or digital signature for online transactions.

The 1999 Declaration will cease to have effect once Schedule 7 commences.

Schedule 7 is expected to commence on 20 January 2008.

The Restricted Access Systems Declaration 2007

Clause 14 of Schedule 7 requires the Australian Communications and Media Authority (ACMA) to develop a restricted access systems declaration (RAS Declaration) to regulate access to MA15+ content and R18+ content including content with an Australian connection that is delivered via the internet and via mobile networks, and also both stored and live streamed content.

For the purposes of this Explanatory Statement, a reference to MA15+ content and R18+ content includes a reference to content that:
- is classified as R18+ or MA15+; or

- has not been classified, but if it were to be classified, there is a substantial likelihood that the content would be classified as MA15+ or R18+.

Under Schedule 7 the purpose of the RAS Declaration is not to prevent access to age restricted content (whether it is user-generated content or otherwise) via any platform, but to ensure that:

- access is limited to persons 15 years and over in the case of MA15+ content and, to persons 18 years and over in the case of R18+ content; and
- that the methods used for limiting this access meet a minimum standard.

Schedule 7 and the RAS Declaration will replace both the existing restricted access arrangements for internet content in place under Schedule 5 and the existing arrangements for mobile premium services content in place under the *Telecommunications Service Provider (Mobile Premium Services) Determination 2005 (No.1).*

The RAS Declaration will also be supported by new Industry Codes of Practice registered under clause 85 of Schedule 7.

Under subclause 14(5) of Schedule 7, ACMA must ensure that a RAS Declaration is in force at all times after the commencement of Schedule 7.

Under Schedule 7, the obligation to have in place a restricted access system in relation to particular content applies to hosting service providers, live content service providers, links service providers and commercial content service providers who provide a content service that has an Australian connection, where the content ("excluding eligible electronic publications") is:

- MA 15+ content that is provided by means of a content service which operates on a commercial basis; or
- R 18+ content.

For convenience, these content service providers are described collectively in Schedule 7 as designated content/hosting service providers.

Objectives for a restricted access system

In making the RAS Declaration, ACMA must have regard to the following matters specified in subclause 14(4) of Schedule 7:

(a) the objective of protecting children from exposure to content that is unsuitable for children; and

(b) the objective of protecting children who have not reached 15 years from exposure to content that is unsuitable for children who have not reached 15 years; and

(c) such other matters (if any) as the ACMA considers relevant.

Other relevant matters include ACMA's regulatory policy considerations under subsection 4(3AA) to the Broadcasting Services Act which, in summary, are:

- to address public interest considerations while not imposing unnecessary financial and administrative burdens on industry; and

- to accommodate technological change; and
- to encourage the development of technologies and services

Outline of Declaration

The RAS Declaration specifies the minimum requirements of an access-control system for MA15+ content that is provided on a commercial basis, and R18+ content. Different requirements exist for the different classification levels.

For MA15+ content that is provided on a commercial basis, an access-control system must:

- require an application for access to the content; and
- require a declaration from the applicant that they are over 15 years of age; and
- provide warnings as to the nature of the content; and
- provide safety information for parents and guardians on how to control access to the content; and
- limit access to the content by the use of a PIN or some other means; and
- include relevant quality assurance measures.

For R18+ content, an access-control system must:

- require an application for access to the content; and
- require proof of age that the applicant is over 18 years of age; and
- include a risk analysis of the kind of proof of age submitted; and
- verify the proof of age by applying the risk analysis; and
- provide warnings as to the nature of the content; and
- provide safety information for parents and guardians on how to control access to the content; and
- limit access to the content by the use of a PIN or some other means; and
- include relevant quality assurance measures; and
- retain records of age verification for a period of 2 years after which the records are to be destroyed.

Consultation

ACMA decided to consult as widely as possible and issued a media release on 26 October 2007 inviting comment on the draft RAS Declaration. A consultation paper and draft instrument were also posted on the ACMA website on that date. A period of 21 days was provided for public, industry and representative bodies to comment. Additionally, 33 stakeholders were emailed a copy of the consultation paper and draft instrument (the consultation draft RAS) and were invited to comment.

Twenty-six submissions were received from carriage service providers, industry associations, and content providers from across a range of media, private individuals, privacy advocacy organisations, consumer organisations, and regulatory bodies. These included the Australian Mobile Telecommunications Association, the Internet Industry Association, the Australian Interactive Media Industry Association, Internet Society of Australia, Consumers' Telecommunications Network, the Australian Privacy Foundation and the Australian Competition and Consumer Commission.

The views expressed by stakeholders were many, however there were several issues that were of concern to many of the respondents:

- the need for the access restriction threshold on commercial MA15+ content to be equivalent to that applicable to other media, in recognition of the fact that 15-17 year olds generally do not possess proof of age;
- the method or methods of access restriction outlined in the RAS Declaration must allow industry the flexibility to develop access-control systems appropriate to their business models; and
- the RAS Declaration should not be too prescriptive of internal procedures that industry should follow as such procedures would more appropriately be set out in an industry code.

All issues raised in submissions were considered and subsequently informed the drafting of the final RAS Declaration.

Regulation Impact Statement

A Regulation Impact Statement is required and attached.

NOTES ON SECTIONS

PART 1 PRELIMINARY

Section 1 - Name of Declaration

Section 1 provides for the citation of the RAS Declaration as the *Restricted Access Systems Declaration 2007*.

Section 2 – Commencement

Section 2 provides that the Declaration commences on the commencement of Parts 1 and 2 of Schedule 1 to the *Communications Legislation Amendment (Content Services) Act 2007*.

Section 3 – Definitions

Subsection 3(1) defines the terms used in the RAS Declaration. Subsection 3(2) refers to terms that have the same meaning in the RAS Declaration as in Schedule 7 to the Broadcasting Services Act.

It should be noted that under the Broadcasting Services Act, MA15+ content must be subject to a restricted access system which meets the requirements specified in the RAS Declaration where the conditions in subclauses 20(1)(c) and (d) of Schedule 7 are satisfied. To summarise the general effect of these provisions, only MA15+ content that is provided by a content service that operates on a commercial basis ("commercial MA15+ content") must be subject to a restricted access system which meets the requirements specified in the RAS Declaration.

Section 4 – Purpose of Declaration

Subsection 4(1), provides that under subclause 14(1) of Schedule 7, ACMA may declare that a specified access-control system is a restricted access system in relation to content for the purposes of Schedule 7.

Subsection 4(2) provides that the RAS Declaration declares specified access-control systems to be restricted access systems in relation to content for the purposes of Schedule 7.

Under clause 2 of Schedule 7 to the Broadcasting Services Act an 'access-control system' is defined as follows:

> ***access-control system***, in relation to content, means a system under which:
> (a) persons seeking access to the content have been issued with a Personal Identification Number that provides a means of limiting access by other persons to the content; or
> (b) persons seeking access to the content have been provided with some other means of limiting access by other persons to the content.

PART 2 MA15+ CONTENT

Section 5 – Minimum requirements of access-control system – MA15+ content

Subclause 14(1) of Schedule 7 provides that ACMA may make a declaration about a specified access-control system. Subclause 14(5) requires that such a declaration must be in place by the commencement of Schedule 7.

Under subclause 14(2) of Schedule 7, ACMA may make different provision with respect to R18+ content and commercial MA15+ content.

Subsection 5(1) sets out the minimum requirements that an access-control system must include if it is to be considered a specified access-control system for commercial MA15+ content. This is done by reference to the obligations in sections 6 – 9, which are discussed below.

Subsection 5(2) declares an access-control system that meets the specifications in sections 6 – 9 to be a restricted access system for commercial MA 15+ content.

Section 6 – Applying for access to MA15+ content

Under section 6, an access-control system must require an applicant seeking access to commercial MA15+ content to apply for access either in writing, in electronic form or orally. This means that an applicant must take proactive steps to initiate the service ('opt-in').

The applicant must also provide a declaration, in writing or in electronic form, that they are 15 years or over.

Section 7 – Provision of warnings

The access-control system must provide warnings about the nature of the commercial MA15+ content that is being accessed and must provide safety information about how a parent or guardian may control access to such content by persons under 15.

This is consistent with the objectives of Government online safety programs, which aim to ensure parents and guardians have access to online safety information and advice to assist them in managing their family's online experience.

Section 8 – Limiting access

Section 8 describes the instances in which an access-control system may provide access to commercial MA15+ content.

Under subsection 8(1), an access-control system must not provide access to commercial MA15+ content unless an applicant has:

- applied for access ('opted-in'); and
- made a declaration that they are over 15 years of age; and
- been provided with warning and safety information.

Under subsection 8(2) an access-control system may provide access to commercial MA15+ content when an applicant has been provided with a PIN or some other means of limiting access by other people, by which the access-control system can verify that the applicant has:

- previously applied for access ('opted-in'); and
- made a declaration that they are over 15 years of age; and
- been provided with warning and safety information.

The phrase 'or some other means of limiting access' is to be read broadly and may include any method a designated content/hosting service provider designs that allows an access-control system to uniquely recognise the applicant in question. This would include such systems as those operating in the mobile premium services sector which recognise the MSISDN of an applicant's telephone service.

Under subsection 8(3) an access-control system may provide access to commercial MA15+ content if an applicant has previously submitted a declaration to the designated/hosting service provider (or to a person acting on behalf of the provider). The declaration is not required to have been made in relation to an application for access to commercial MA15+ content. For example, a designated content/hosting service provider may have the capacity to cross check other instances where a person may have declared their age, as in situations where age details are declared for the establishment of an account.

In the circumstances contemplated under subsection 8(3), the access-control system must ensure that the applicant is provided with warnings and safety information on the first occasion on which they attempt to access commercial MA 15+ content.

Section 9 – Quality assurance measures

Section 9 requires an access-control system to have measures in place that will allow an applicant's access to commercial MA15+ content to be removed immediately, should the applicant be found to have been given access in contravention of section 8.

PART 3 R18+ CONTENT

Section 10 – Minimum requirements of access-control system – R18+ content

Subsection 10(1) sets out the minimum requirements that an access-control system must include if it is to be considered a specified access-control system for R18+

content, or commercial MA15+ and R18+ content. The reason for inclusion of the category for "commercial MA15+ and R18+ content" captures the situations where a designated content/hosting provider may want to use the one access-control system for both commercial MA15+ and R18+ content. This is done by reference to the obligations in sections 11 - 17, which are discussed below.

Subsection 10(2) declares an access-control system that meets the specifications in sections 11 – 17 to be a restricted access system for R 18+ content or for commercial MA 15+ content and R 18+ content.

Section 11 – Applying for access to R18+ content
Under section 11, an access-control system must require an applicant seeking access to R18+ content, or to R 18+ content and MA 15+ content, to apply for access either in writing, in electronic form or orally. This means that an applicant must take proactive steps to initiate the service ('opt-in').

Section 12 – Provision of warnings
The access-control system must provide warnings about the nature of R18+ content that is being accessed and must provide safety information about how a parent or guardian may control access to such content by persons under 18.

This is consistent with the objectives of Government online safety programs, which aim to ensure parents and guardians have access to online safety information and advice to assist them in managing their family's online experience.

Section 13 – Age verification
Subsection 13 (1) requires the access-control system to verify that the applicant is at least 18 years old by requiring the applicant to provide evidence of proof of age.

The access-control system must also verify that the applicant is at least 18 years old by applying the risk analysis in section 15.

Applying the risk analysis means considering:
- the risk of whether the proof of age evidence could be held or used by another person, or someone younger than the age which the form of evidence attributes to the person being identified; and
- the kind of evidence provided and the manner in which it is provided.

Subsection 13(2) requires that the evidence of age provided to the access-control system must satisfy the risk analysis.

Satisfying the risk analysis means ensuring that risks associated with use of evidence of proof of age that the access-control system will accept have been adequately identified and mitigated.

It is important to note that subsection 13(1) is subject to subsection 14(3) of the RAS Declaration. Subsection 14(3) provides that an access-control system may allow access if evidence of age has previously been provided to the designated/hosting service provider (or to a person acting on behalf of the provider).

Section 14 – Limiting access
Section 14 describes the instances in which an access-control system may provide access to R18+ content, or to R18+ content and commercial MA15+ content.

Under subsection 14(1), an access-control system must not provide access to R18+ content, or to R18+ and commercial MA15+ content, unless:
- the applicant has applied for access ('opted-in'); and
- the applicant has been provided with warning and safety information; and
- the access-control system has verified that the applicant is 18 years or over.

Under subsection 14(2) an access-control system may provide access to R18+ content, or to R18+ and commercial MA15+ content, when an applicant has been provided with a PIN or some other means of limiting access by other people, by which the access-control system can verify that the applicant:
- has previously applied for access ('opted-in');
- had their age verified by the access-control system; and
- been provided with warning and safety information.

The phrase 'or some other means of limiting access' is to be interpreted broadly and may include any method a designated content/hosting service provider designs that allows an access-control system to uniquely recognise the applicant in question. This would include such systems as those operating in the mobile premium services sector which recognise the MSISDN of an applicant's telephone service.

Under subsection 14(3) an access-control system may provide access to R18+ content, or to R18+ and commercial MA15+ content, if an applicant has previously submitted evidence that the person is at least 18 years of age to the designated/hosting service provider (or to a person acting on behalf of the provider). The submission of proof of age is not required to have been made in relation to an application for access to content, however the proof of age provided must be sufficient to satisfy the risk analysis. For example, a designated content/hosting service provider may have the capacity to cross check other instances where a person may has submitted proof of age as in situations where age and identification are submitted for the establishment of an account.

In these circumstances, the access-control system must ensure that the applicant is provided with warnings and safety information on the first occasion on which they attempt to access R18+ content, or R18+ and commercial MA15+ content.

Section 15 – Risk analysis
Section 15 requires that an access-control system include a risk analysis and outlines what factors that analysis must consider.

A risk analysis must identify and asses the risk of whether the proof of age could be held or used by another person, or someone younger than the age which the form of evidence attributes to the person being identified; and the kind of evidence provided and the manner in which it is provided

The RAS Declaration does not prescribe a specific method for verifying age to access R18+ content. This is both to recognise the breadth of current methods of age

verification used across various content platforms, and to ensure that there is flexibility now and into the future to allow designated content/hosting providers to develop systems that best suit their business models. ACMA is aware of a number of different methods of age verification currently operating that range from submission of proof of age in person and actual sight of the applicant and the proof of age (which may be a driver's license, passport etc) to reliance on credit card verification.

However, in the absence of a prescribed method, the risk analysis ensures that the decision of which method of age verification will be accepted, and how it will be accepted, by the access-control system has been informed by considerations of the risk of the content being accessed by a minor.

Section 16 – Quality assurance measures

Section 16 requires an access-control system to have measures in place that will allow an applicant's access to R 18+ content, or to R 18+ content and commercial MA15+ content, to be removed immediately, should the applicant be found to have been given access in contravention of section 14.

There must also to be periodic review of the effectiveness of the risk analysis and how it is applied in relation to age verification.

Section 17 – Age verification records

Section 17 requires that, for each applicant granted access to R 18+ content, the access-control system must make provision for the keeping of adequate records to demonstrate:

- that it had received an application for access to R 18+ content; and
- how it was able to verify that the applicant was at least 18 years.

A record is sufficient if it contains information that verifies the matters in section 13 (Age verification) or subsection 14(3).

Records will need to be retained in accordance with the National Privacy Principles under the *Privacy Act 1988*. The records must be retained for a period of 2 years, after which time the records are to be destroyed as soon as practicable. There is an exception to the requirement that records must be destroyed in circumstances where ACMA gives notice that it requires access to the record.

Records must be produced to ACMA, upon request, for a purpose relating to the RAS Declaration or Schedule 7.