



Australian
Mobile Telecommunications
Association
ABN 98 065 814 315
First Floor
35 Murray Crescent
Griffith ACT 2603 Australia
PO Box 4309
Manuka ACT 2603 Australia
Ph +61 2 6239 6555
Fax +61 2 6239 6577
Web www.amta.org.au

AMTA Submission to ACMA Discussion Paper

Restricted Access Systems Declaration 2007

16 November- 2007

1 Executive summary

AMTA welcomes the opportunity to provide comment on the draft Restricted Access Systems (RAS) Declaration under Schedule 7 to the Broadcasting Services Act 1992 (BSA).

AMTA agrees in principle with the objects of the draft RAS Declaration and acknowledges that ACMA has liaised closely with the industry on these changes. However, AMTA is concerned that the content of the draft RAS Declaration does not reflect the discussions between ACMA and the industry. In particular, AMTA is of the view that instead of the draft RAS Declaration being a high-level regulatory framework document (as discussed with and expected by industry), in practice it is very prescriptive and process orientated.

AMTA believes its concerns can be addressed through further consultation with ACMA and amendments to the draft RAS Declaration.

In summary AMTA's concerns and recommendations are as follows:

- **Access Key**

The "access key" requirements in the draft RAS Declaration is highly prescriptive and process-orientated and goes well beyond the requirements under the current Mobile Premium Services Determination (MPSD).

AMTA recommends that ACMA's definition of an access control system should:

- ***reflect the definition in clause 2 of Schedule 7 to the BSA in the Content Services Act and***
- ***draw upon clauses 3.4 (1) (2) (3) and (4) of the MPSD***

- **Age-verification evidence**

It would appear that sections 7 (1) (b), 7 (2) (a) and 7 (3) and sections 8 (1) (b), 8 (2) (a) and 8 (3) when read together impose an extra layer of age-verification where an applicant who has previously provided evidence of age must again provide that evidence when applying for access to age-restricted content.

Further, the introduction of a timing linkage between the verification of the customer's age and the customer's request for access to the relevant content goes beyond the current requirements under the MPSD.

AMTA believes that sections 7 and 8 of the draft RAS Declaration should be removed and redrafted based on clauses 3.4 (1) (2) (3) and (4) of the MPSD with sufficient flexibility to permit 15,16 and 17 year olds to access MA15+ content. AMTA supports the submission made by the Internet Industry Association in response to the draft RAS Declaration, in particular in relation to the granting of access to MA15+ content.

- **Risk analysis**

The proposed risk analysis requirements in the draft RAS Declaration goes well beyond the requirements under the current MPSD. It would appear that an analysis is required for each type of identification document and for each manner in which evidence is received.

AMTA recommends that paragraph 10 of the draft RAS Declaration be removed and redrafted based on the provisions in clause 3.4 (1) of the MPSD.

- **Quality assurance measures**

AMTA is concerned that the age-verification and quality assurance measures as described in the draft RAS Declaration are overly prescriptive and onerous.

AMTA believes that the Restricted Access System must incorporate an age-verification compliance plan that is outcome-based providing greater flexibility for the industry.

2 Introduction and overview

2.1 Introduction

The Australian Mobile Telecommunications Association (**AMTA**) is the Australian mobile industry's peak body. AMTA's members include mobile phone carriers, handset manufacturers, retail outlets, network equipment suppliers and other suppliers to the industry. AMTA's mission is to promote a socially, environmentally and financially responsible and successful mobile telecommunications industry in Australia. For more details about AMTA, see <http://www.amta.org.au>.

AMTA is committed, as always, to working cooperatively with Government agencies to achieve a balanced policy outcome for the industry and a workable regulatory framework to facilitate policy objectives.

2.2 Overview of AMTA's position

AMTA submits that it generally supports the objects of the draft RAS Declaration. However, the proposed amendments have serious implications for the telecommunications industry. AMTA is keen to achieve a more balanced policy outcome for the industry.

AMTA's support for the draft RAS Declaration assumes that ACMA will carefully work through the operational and implementation issues with industry to ensure that the draft RAS Declaration's requirements are drafted in a clear and achievable way. This will allow the requirements to be met by industry in the most efficient manner possible.

Since the introduction of the Communications Legislation Amendment (Content Services) Act in July 2007, the industry has actively participated in reviewing the Mobile Premium Services Industry Scheme (MPSI) and the development of a new Content Code under Schedule 7 of the Broadcasting Services Act 1992. As a part of these discussions the industry was under the understanding that the draft Declaration would reflect the objects of the MPSD and seek to replicate, where possible, the required high-level outcomes of the MPSD.

In its consultation paper, ACMA states that it has tailored the draft RAS Declaration to accommodate the MPSD however, AMTA is concerned that the content of the draft RAS Declaration does not reflect the substance of discussions between ACMA and the industry.

AMTA's concerns are detailed below.

3 Specific Concerns

3.1 Access Key

AMTA is concerned by and opposed to the "access key" requirement contained in the draft RAS Declaration for the following four key reasons:

- It goes well beyond the scope of the Content Services Act and imposes an unworkably (and unjustifiably) narrow interpretation of the Act on industry;
- It imposes a prescriptive and process-orientated obligation on industry (contrary to all indications from ACMA preceding the draft RAS Declaration's release);
- It goes beyond the existing obligations contained in the MPSD and, consequently, ignores the RAS investments already made and procedures already developed by mobile carriers; and
- It would not guarantee that the key policy objective of protecting children would be met any more than effectively than is already being achieved under existing arrangements.

Based on ACMA's description of an "access control system" in the consultation paper to its draft RAS Declaration and its definition of an "access key" in the draft Declaration, it appears that ACMA has either misread the definition of "access control system" in clause 2 of the new Schedule 7 to the BSA contained in the Content Services Act or interpreted it in an unworkably narrow manner.

The definition of "access control system" in clause 2 of Schedule 7 to the BSA in the Content Services Act states that it is "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.*¹

However, in its consultation paper to the draft RAS Declaration, ACMA states that "an 'access control system' is a system under which the person seeking access to content has been **issued with** a Personal Identification Number (PIN) or password or **some other means by which a person who has sought access can be identified but which provides a means of limiting access** by other persons to the content."² Furthermore, clause 3 of the draft RAS Declaration states that an "access key means:

- (a) *a password; or*
- (b) *a Personal Identification Number; or*
- (c) ***any other means by which a person who has been granted access by the restricted access system can be identified.***³

As is demonstrated by the direct quotes above, there is a fundamental difference between the definition of an access control system in the Content Services Act and how it is described by ACMA in its consultation paper and how an access key is defined in its draft RAS Declaration:

- Clause 2(b) of Schedule 7 to the BSA contains a broad statement that persons need to "have been provided with some other means of limiting access" as an alternative to being "issued with" a PIN. In creating its access key concept as defined, ACMA has removed any ability for industry to develop its own processes and safeguards to limit access to age-restricted content as envisaged by clause 2(b).

¹ Schedule 7 – Content Services, Part 1 – Introduction, 2 Definitions, *Communications Legislation Amendment (Content Services) Act 2007*, p16

² ACMA consultation paper to its draft RAS Declaration (released 26 October 2007), pp11-12

³ Draft RAS Declaration (released 26 October 2007), pp1-2

- Moreover ACMA's definition of an access key in 3(a) and 3(b) of its draft RAS Declaration goes to 'access' (that is, the issuing of a password or PIN), whereas its requirement in 3(c) goes to 'identity'. There is nothing in the definition of an access control system in the Content Services Act that requires such a system to 'identify' a person. The requirement in the Content Services Act is quite explicitly on "limiting access". ACMA's requirement would be unworkable in practice.
- Furthermore, while clause 2(a) of Schedule 7 to the BSA uses the expression "issued with" with respect to a PIN, in 2(b) it explicitly uses the broader "provided with" expression with respect to "some other means of limiting access". However, the entire construction of ACMA's access key concept in its draft RAS Declaration excludes the Content Services Act's broader application, for example using the narrow terms "allocate" (in clause 5(2)(b), 7(1) and 8(1)) and "entered" (in clause 6(1) and 6(2)).

The MPSD articulates the outcomes required of industry while providing industry with the flexibility to determine the most efficient and effective ways of doing so. For example, sections 3.4(1) and 3.4(2) of the MPSD state the specific conditions that must be met before age-restricted content can be provided to a customer. This stands in stark contrast to the prescriptive and process-focused access key concept in ACMA's draft RAS Declaration.

ACMA's access key concept appears to ignore the RAS investments already made and procedures already developed. Moreover the concept does not necessarily provide any greater support to the policy objective of protecting children than is provided under current arrangements.

AMTA believes that a reasonable and workable approach by ACMA to defining an access control system would be to:

- 1) Adopt a broad interpretation of the definition in clause 2 of Schedule 7 to the BSA in the Content Service Act; and
- 2) Draw upon clauses 3.4 (1) (2) (3) and (4) of the MPSD which, while wordy, clearly articulates outcomes-orientated requirements that industry must meet.

3.2 Age-Verification Evidence

AMTA is concerned that, when sections 7(1)(b), 7(2)(a) and 7(3) and/or sections 8(1)(b), 8(2)(a) and 8(3) of the draft RAS Declaration are read together, it appears that an applicant for age-restricted content may need to provide evidence of their age at the same time as making the application – regardless of whether the provider already has this evidence.

Were such a prescriptive and process-orientated requirement to be imposed, it would go considerably further than the obligations in place under the MPSD and currently complied with by mobile carriers. Given previous assurances by ACMA to mobile carriers and ACMA's statement in its consultation paper that the "new RAS Declaration has been tailored to accommodate...differing approaches [such as mobile carriers'] 'one-off' age verification for ongoing entitlement to access to content"⁴, we consider that ACMA is unlikely to have intended that there be a timing linkage between an application for age-restricted content and presentation/collection of evidence of an applicant's age and identity.

For example, if a designated content/hosting service provider can determine that a particular customer is aged 15-17 or 18+ by virtue of evidence previously provided by that customer and held by the designated content/hosting service provider, there is some ambiguity as to whether the designated content/hosting service provider would be compliant with sections 7 and/or 8 of

⁴ ACMA consultation paper to its draft RAS Declaration (released 26 October 2007), p11

ACMA's draft RAS Declaration if the customer was not required to produce evidence a second or subsequent time and for the designated content/hosting service provider to verify (for a second or subsequent time) when the customer applied for access to age-restricted content.

Further, sections 7 and 8 of the draft RAS Declaration make statements that "the restricted access system receives a request...", that "the restricted access system has verified..." and "the restricted access system is taken to have verified...". Mobile carriers are concerned that this language may impose an unworkably arbitrary distinction between a provider of age-restricted content and the RAS used by that provider. For example, if a mobile carrier can determine that a particular customer is aged 18+ by virtue of evidence previously provided by that customer and verified by the carrier, it is unclear whether the carrier would be compliant with sections 7 and/or 8 of ACMA's draft RAS Declaration if it did not require the customer to provide evidence again and verify it again at the point at which the customer applied for access to age-restricted content.

Given the above concerns, AMTA would propose that ACMA should remove sections 7 and 8 of its draft RAS Declaration and, as above, redraft clauses 3.4(1)(2)(3) and (4) based on the MPSD with sufficient flexibility to permit 15, 16 and 17 year olds to access MA15+ content which, while wordy, clearly articulate outcomes-orientated requirements that industry must meet.

In relation to access by those aged 15-17 to MA15+ content, AMTA supports the comments and suggested measures made by the Internet Industry Association ("IIA") in its submission. Mobile carriers are currently required to restrict MA15+ content to customers who are 18+. Providing access to this content to those who are 15+ brings the mobile industry in line with other industries such as television, films and games. Consistency between access to content on a carrier's portal and via the open internet is also necessary to create an understandable user experience for customers who access content in both ways.

AMTA agrees with the IIA that there should be a different approach when looking at an appropriate access-control system for the provision of MA15+ content. AMTA notes that the use of content filters suggested by the IIA is not necessarily relevant to content accessed on a mobile carrier's portal. What is relevant to mobile carriers is the contractual arrangements that they have in place for the supply of content to their portals. In this way, mobile carriers can exercise a level of control over the content by requiring providers to supply content that falls within certain classifications.

The MPSD foreshadows this type of arrangement as it contains provisions outlining the circumstances in which a mobile carrier would be taken not to have contravened the age verification requirements. These have not been adopted in the proposed RAS Declaration, however the provisions of the MPSD indicate a previous intention by ACMA (then the ACA) that mobile carriers should be able to rely on contractual arrangements with content providers for the supply of content appropriate for the service being provided. These provisions should be retained in order to provide consistency for mobile carriers who currently rely on them.

3.3 Risk Analysis

AMTA believes that the difficulty with the proposed risk analysis requirements is that they place a more onerous burden on industry than exists currently under the MPSD. An analysis is required for each type of evidence (eg passport, birth certificate, credit card, student card) and for each manner in which evidence is received (eg electronic, in person, in writing, over the phone) whether the evidence could be used by a person other than the person it purports to identify or a person younger than the age the evidence attributes.

Requiring every provider to undertake such a risk analysis creates the potential for different conclusions on the suitability or otherwise of evidence types and methods of receipt. For example one provider might make an assessment that a student card would be an acceptable form of age verification given it is issued by a university after complying with enrolment procedures. However another provider might decide to only accept evidence of age, such as a passport, which itself can only be issued after the applicant has produced a range of other forms of identification and proof of age. Another provider may only accept forms of evidence that originate in Australia in reliance on a perceived superiority in issuing of identifying documents.

AMTA feels that the risk analysis requirements appear to draw on the current chat services risk analysis requirements in the MPSD in relation to safety measures. A risk analysis process for chat services is more appropriate given the variety of services available and the range of target audience. An analysis in relation to each service, or type of service, allows the differences between services to be taken into account to measure in each case the risk of illegal contact between adults and children. In this way appropriate measures can be taken into account given the nuances of each service.

However the range of evidence types and the methods of receipt are essentially static categories. Given that the kinds of evidence and the manner in which they may be received would be relevant to every provider of a RAS, it is a burdensome requirement that every provider should conduct their own risk analysis on the same types of evidence and the same methods of receiving evidence.

The current requirements in relation to age verification in the MPSD are not as onerous as the proposed risk analysis requirements. Under the MPSD, there is essentially only a requirement that the nature of the evidence and the way in which it is given is such that it would be improbably or difficult for it to be held by a person other than the customer, and where age is not known at the time of the request, the person is at least 18.

However the risk analysis requirements for age verification under the RAS Declaration make the providers pseudo investigators, particularly given the assessment relates to whether or not they evidence *could* be held or used in the relevant ways. Whether or not evidence *could* be used in a particular way requires an assessment about whether documents are, or are likely to be, fraudulent and whether the person presenting the evidence is, or is likely to be, acting in a fraudulent manner. Providers should be entitled to rely on face value on the evidence that is produced. If the applicant produces a passport, a provider should not have to determine the likelihood that the passport could have been obtained using other false identification or that the passport is a forgery.

As is the case with the new 'access-key' concept, the new risk analysis requirements would require a complete review of the carrier's current procedures which would appear to be unnecessary given the smooth operation of current RAS's to date in the mobile industry.

As mentioned above, the MPSD also contains provisions relating to the circumstances in which a provider would be taken not to have contravened the age verification requirements. These have not been adopted in the proposed RAS Declaration and therefore protection that has been previously offered has been removed. Given ACMA's desire to retain consistency in some areas, it is odd that this desire has not been maintained across protections as well as obligations.

AMTA believes that a reasonable and workable approach by ACMA would be to remove paragraph 10 of the draft RAS Declaration and draw upon clause 3.4 (1) the MPSD. This clause clearly articulates the high level principles to be achieved, namely that:

- (a) an age-restricted service must not be supplied unless the provider first receives a request for access; and
- (b) before actioning the request, the provider must verify that:
 - (i) the customer is at least 18 years old (or 15 years old in the case of MA 15+ content); and
 - (ii) the person making the request is the customer

These high level principles could then be supported by more detail in the Content Services Code.

AMTA members who participate in the committee currently drafting the Content Services Code have proposed wording that is designed to sit under a principles based RAS Declaration. This wording is set out in Annexure A. Paragraphs 8.2 and 8.3 would be suitable for use within the RAS Declaration. The remainder of the paragraphs would then operate under these high level requirements.

It should be noted that the committee has not had opportunity to review this wording as discussion was put on hold given the need to address the content of the proposed RAS Declaration. However the wording is similar to that already contained in the Guidelines developed in relation to the MPSD and the current IIA Content Code in relation to access to restricted content via mobile devices.

3.4 Quality Assurance Measures

AMTA is concerned that the age verification and quality assurance measures as described in the draft RAS Declaration are overly prescriptive and too onerous, therefore, placing an unnecessary burden on industry. It is also questionable whether they will provide additional benefits to consumers.

A principles and outcome based approach to the types of measures that must be documented for the age verification plan would allow a greater level of flexibility in industry's approach to the development of these plans.

The obligations described in the measures section are more onerous than the current requirements of the MPSD, extending the requirements to include measures around the allocation of 'access keys'. This is particularly concerning given that the access obligations are also much more prescriptive than in the MPSD.

During its consultation with industry, ACMA provided industry with assurances that its intention was to develop a high level, outcomes focussed RAS Declaration. The mobile industry believes an example of an alternative, principles-based approach to describing the age verification and quality assurance measures requirements that must be captured could state:

The restricted access system must incorporate an age verification compliance plan that specifies the following:

- The measures to be adopted by the designated content/hosting service provider to ensure that an application has been received and that the age of the applicant has been verified as at least 15 Years to access to MA15+ content and 18 years for access to R18+ content;
- The procedures to be followed by employees and agents of the designated content/hosting service provider to implement the age-verification measures;

- The measures that will be taken so that the designated content/hosting service provider removes, without delay, an applicant's access to age restricted content, if the applicant's access is given in contravention to the requirements for access only via a restricted access system, the receipt of a request for access and verifying the age of the applicant;
- The procedures for conducting periodic internal review of the measures in the above paragraphs.

AMTA believes that a more suitable approach to describing the age verification and quality assurance measures to be included in an age verification compliance plan would be to adopt the above, principles and outcome based description

4 Conclusion

AMTA reiterates its commitment to ensuring that children are protected from accessing inappropriate material and that access to adult material is also appropriately controlled.

AMTA recognises the importance of working cooperatively with relevant government agencies to develop shared outcomes and achieve policy objectives and is keen to preserve the current objectives under the Mobile Premium Services Industry Scheme.

In the context of the draft RAS Declaration, AMTA's interest is to maintain the balance the Government has currently drawn between obligations on the industry and its legitimate commercial and business imperatives.

AMTA thanks ACMA for the opportunity to comment on the draft RAS Declaration and looks forward to working with ACMA to address its concerns.

Annexure A

Extract from wording proposed by carriers for the Content Services Code

- 8.1 Access to a Content service that provides MA15+ Content and/or R18+ Content (“age-restricted service”) must be provided in accordance with ACMA’s Restricted Access Declaration.
- 8.2 The Restricted Access System may vary depending on whether the Content to be restricted is MA 15+ Content or R18+ Content. Unless otherwise stated, the remainder of this section operates on the basis that the age verification process will verify that the applicant is of an age appropriate to view the Content or service to which access is being sought (“appropriate age”).
- 8.3 A Designated Content/Hosting Service Provider must not supply an age-restricted service to a End User unless:
- (a) the Designated Content/Hosting Service Provider receives a request (whether orally, electronically or in writing) that the End User be given access to age-restricted services; and
 - (b) the Designated Content/Hosting Service Provider has verified that:
 - (i) the End User is an appropriate age;
 - (ii) the person making the request is the End User.
- 8.4 For paragraph 8.3(b), a Designated Content/Hosting Service Provider is taken to have verified the matters mentioned in subparagraphs (b)(i) and (ii) only if:
- (a) all of the following apply:
 - (i) at the time the Designated Content/Hosting Service Provider receives the request, the Designated Content/Hosting Service Provider knows, with reasonable certainty, that the End User is an appropriate age;
 - (ii) the Designated Content/Hosting Service Provider has received evidence from the person making the request that he or she is the End User; or
 - (b) all of the following apply:
 - (i) at the time the Designated Content/Hosting Service Provider receives the request, the Designated Content/Hosting Service Provider does not know, with reasonable certainty, whether the End User is an appropriate age; and
 - (ii) the Designated Content Service Provider has received evidence from the person making the request that he or she is the End User and is an appropriate age.
- 8.5 For the purposes of obtaining evidence from the person making the request that he or she is the End User, a Designated Content/Hosting Service provider may collect:
- (a) the name of the End User;
 - (b) the account number; and
 - (c) other information required by the Designated Content/Hosting Service Provider’s processes to verify End User identity.
- 8.6 For the purposes of obtaining evidence the End User is an appropriate age, a Designated Content/Hosting Service Provider may obtain:

- (a) a valid credit card number in the name of the End User; or
 - (b) evidence of some other form of identification by which the age of the End User can reasonably be ascertained. Examples of identification that would satisfy this clause include a valid drivers licence, proof-of-age card, passport or birth certificate in the name of the End User;
 - (a) and may also obtain:
 - (c) a declaration, (whether orally, electronically or in writing), by the End User, or the End User's parent or guardian, that the End User is an appropriate age.
- 8.7 Where the nature of the evidence and the way it is given is such that there is a reasonable risk that the evidence provided to the Designated Content/Hosting Service Provider by the applicant does not relate to the person making the request, the Designated Content/Hosting Service Provider will send a confirmation to the End User to who the evidence relates, in a way that will ensure that the End User is informed that he or she is being given access to age-restricted services. Confirmation may be by way of a printed message on the End User's telephone account or credit card statement. Confirmation should not only be sent by SMS to the End User's mobile phone.
- 8.8 A Designated Content/Hosting Service is taken not to have contravened clause 8.3 if the Designated Content/Hosting Service:
- (a) does not know; and
 - (b) could not, with reasonable diligence, have ascertained;
 - (c) that it is supplying an age-restricted service to a End User other than a End User who has requested the service and is an appropriate age.
- 8.9 For clause 8.8, in determining whether a Designated Content/Hosting Service Provider could, with reasonable diligence, have ascertained that it is supplying an age-restricted service to a End User other than a End User who has requested access to the service and is an appropriate age, it can be taken into account whether the content service provider who supplied the age-restricted service is under any contractual obligation to notify the Carriage Service Provider of the nature of the content supplied.