

23 November 2007

Manager
Education and Telephone Content Section
Australian Communications and Media Authority
PO Box 13112 Law Courts
Melbourne VIC 8010

By email to: NewContentRegulation@acma.gov.au

Dear Sir/Madam

Proposed Restricted Access Systems Declaration for regulating access to MA15+ and R18+ content

The Australian Subscription Television and Radio Association ('**ASTRA**') is the industry body representing, among others, companies allocated subscription television broadcasting licences by the Australian Communications and Media Authority ('**ACMA**') under Part 7 of the Broadcasting Services Act 1992 (the Act).

ASTRA welcomes the opportunity to respond to the Draft Restricted Access System Declaration (the **Proposed Declaration**) relating to the implementation of a Restricted Access System (**RAS**), issued by ACMA. ASTRA's members are broadcasters, distributors and producers of audio-visual content. The majority of this content is made available by cable and/or satellite. However, ASTRA's members also supply this content for use on other distribution platforms including mobile telephones and via the Internet. In providing comment upon the Proposed Declaration, ASTRA has focused upon areas of greatest concern to its members.

ASTRA notes that restricted access systems are a feature of its members' businesses.

Restricted Access to age restricted content

The Proposed Declaration has amalgamated the requirements under the existing Restricted Access Systems Declaration 1999 for Internet content and the Telecommunications Service Provider (Mobile Premium Services) Determination 2005 (No.1). ASTRA's main concern is the difficulty with devising an effective age-verification system for 15, 16 and 17 year olds, without jeopardising the objectives of the Proposed Declaration.

Restricting Access to R18+ content

As ACMA would be aware, there have been a number of measures introduced by content providers to ensure that viewers of content on mobile telephones or over the Internet are 18 years or over. In particular for content provided over the Internet, many providers have implemented a system whereby customers must provide credit card details to the content provider before they can access



content that is rated R18+. The provision of credit card details provides evidence that the customer is 18 years or older. Upon the provision of credit card details, the customer is provided with a PIN, access number or password with which they can access content on a particular site. The PIN, access number or password is entered each time they visit the relevant site to access all content. This method of verification is presently contemplated by the Restricted Access Systems Declaration 1999 for Internet content providers and is a primary means of age identification for a number of established Internet content providers throughout the world.

ASTRA believes that this method of verification is one that is recognised by both content providers and end users as a valid means of identifying the end user as a person over the age of 18. ASTRA believes that this method should continue to operate under the final RAS declaration issued by ACMA, as a valid method of age verification for people 18 years or older. A requirement that content providers require customers to physically provide evidence of their age, particularly in the context of Internet content services, would, in ASTRA's view give rise to a significant risk that the customer will not proceed with the verification process on the content provider's site and will seek to find this content by other, less regulated (or, unregulated) means.

Restricting Access to MA15+ content

ASTRA is not aware of any mechanism implemented anywhere in the world that seeks direct verification of a person's age where that person is between the ages of 15 and 17. This is possibly due to the difficulty in establishing a successful age verification method for this age bracket.

In Australia, there are limited means by which people under the age of 18 can verify their age. Many people within the age bracket do not possess a passport, drivers' licence or identity card. To ASTRA's knowledge, there is no meaningful electronic verification method for people between the ages of 15 and 17.

Digital signatures have been put forward as one option for electronic age verification, however the technology to authenticate them is costly and complicated, and 15, 16 and 17 year olds rarely have them. Credit card numbers are also unsuitable given their general availability to people aged 18 and over.

The only way of a content provider verifying whether someone is between the ages of 15 and 17, is by requiring hard copy age verification. This approach would not work, at least in an online context, because the relationship between Internet content providers and customers is typically characterised by one-off electronic transactions. Even where there is an ongoing subscription element to the relationship, Internet content providers do not generally have the same level of back office support available to manage the administration of hard copy age verification and all contact is typically electronic.

Requiring an Internet content provider to obtain hard copies of age verification documents would impose a significant, new administrative burden on Internet content providers. It would also deter otherwise eligible applicants from using Australian Internet content services to access MA15+ content and encourage them to go elsewhere for the same content. The present barriers to accessing MA15+ content on television, at cinemas, DVD retailers and rental businesses are far less onerous and, in the case of overseas Internet content providers, non-existent.

For these reasons, in its present form, ASTRA is concerned that the Proposed Declaration will mean that Internet content providers are unable to provide MA15+ content to 15, 16 and 17 year olds.

The practical difficulties associated with 15-17 year old age verification will have the unintended consequence of denying 15-17 year olds access to content which is legally and more readily available to them from other sources and encourage them to seek this content via the Internet from overseas.

Recommendation

ASTRA recommends that the Proposed Declaration adopt a high level ‘principles’ approach, which allows industry the flexibility to introduce Restricted Access Systems within the context of their businesses.

Specific Comments on Restricted Access Systems for MA15+ and R18+ Content

While ASTRA’s preference is a ‘principles’ approach, should ACMA’s intention be to adopt a more prescriptive approach, ASTRA recommends that this approach accommodate the existing means by which Internet service providers verify the age for persons over 18, namely by the provision of credit card details. ASTRA also recommends that, in order to overcome the difficulties with verifying the ages of 15, 16 and 17 year olds, the Proposed Declaration enable age verified applicants, who are 18 years or older, to permit someone between the ages of 15 and 17 to access MA15+ content, in the following ways:

1. Authorised Access Key usage

One option would be for the age verified applicant to be issued with two Access Keys: one for MA15+ content and one for R18+ content. The age verified applicant could then pass their Access Keys on to other members of their household, on the condition that they do not pass the MA15+ Access Key onto anyone under the age of 15 or the R18+ Access Key onto anyone under the age of 18. ASTRA notes that this approach is similar to the approach under section 4.3 of the Restricted Access Systems Declaration 1999 for Internet content. That section provides:

4.3 Upon valid registration, a PIN or password is to be issued to the registered user. It should be a condition of use that the allocated PIN or password should not be passed on to a third person under the age of 18.

Enabling age verified applicants to share their Access Keys, would overcome the problems associated with verifying the ages of 15, 16 and 17 year olds. ASTRA submits that it is fitting for the age verified applicant to be responsible for this allocation as they are in the best position to authorise appropriate users.

2. Adult Verification

A second option would be to require 15, 16 and 17 year old applicants to have their age verified online by an age verified adult user. This then allows effective verification of 15, 16 and 17 year olds who, in order to access content, must become a member of a site and then be issued with their own unique Access Key creating an additional visibility to content providers about their on-line activities.

3. Authorised Additional Users

A third option would be for the 18 year old (or over) account holder to authorise additional users on their account, giving each additional user their own login and password. During registration of an “authorised user”, the adult account holder would be asked to verify the age of their authorised user. For example, if the account holder verified that the authorised user was aged 15-17 the user would then be tagged as permitted to access MA15+ content from the service but not R18+ content. It would then fall to the age verified adult to determine appropriateness of access.

This therefore provides three processes to permit a 15, 16 or 17 year old to view content they are legally able to access by placing obligations for age verification upon the original account holder or customer. This is consistent with current practices in the home. Without the involvement of the original account holder or customer, ASTRA does not believe that MA15+ content will be able to be provided to 15,16 or 17 year olds over the internet given the absence of viable alternatives.

Under either of these approaches, the Internet content service provider will have, by virtue of the verification process, verified that the account holder is over 18. That person is in a far better position than the Internet content provider to confirm the age of people accessing content in their household or otherwise through an account for which they are liable.

The process that ASTRA is seeking to adopt is analogous to that which is presently in place for the subscription television services offered by a number of its members. Under the terms of subscription narrowcasting opinions obtained from ACMA, with respect to the adult erotic service offered on subscription cable and satellite services, subscribers must enter a PIN in order to access R18+ rated content. The control of the PIN remains with the subscriber, who must be over the age of 18. The subscriber can provide access to this content to other members of their household by providing them with the PIN or by inputting the PIN on the relevant program. ASTRA believes that this process has worked effectively for its subscription television services for an extended period of time without complaint from subscribers. ASTRA believes that adopting a similar approach for Internet content providers is an effective means of protecting minors from content that is unsuitable for their age group and provides a familiar means of restricting content.

Quality Assurance Measures

The Quality Assurance Measures (**QAM**) detailed in section 12 of the Proposed Declaration appear to require a content provider to document the procedures it has in place to give effect to the overall objective of ensuring children are not able to access content deemed unsuitable for their age group. These requirements are highly administrative and prescriptive, affording little flexibility for content providers to integrate the QAM into their business structures.

In particular, the requirements that content providers have specific procedures for those within the business who are implementing the age verification measures and, additionally, measures to assess how these procedures are actually being implemented under subsection 12(a) and (b), are in ASTRA’s view, excessive.

Recommendation

ASTRA submits that the Proposed Declaration should be amended to remove the requirement for Quality Assurance Measures, and to instead take an outcomes-based approach, allowing each content service provider or hosting service provider to develop its own set of procedures to ensure

compliance with the requirements of the RAS. To impose prescriptive obligations on providers has the potential to reduce the ability of providers to integrate the requirements of the RAS into their business processes, such as staff training and education, and does not, in ASTRA's opinion, give rise to a greater level of certainty that unsuitable content will be inaccessible by people under the age of 15. ASTRA believes that the Risk Analysis requirements set out in Section 10 adequately address the issues of quality assurance.

Age Verification Records

Section 13 of the Proposed Declaration sets out the record keeping requirements that content providers must adhere to when operating a Restricted Access System. It is unclear from section 13 whether content providers are required to retain the evidence provided by applicants as part of the age verification process.

ASTRA submits that it is unnecessary for content providers to retain this evidence. It should be sufficient for content providers to record which type of evidence was provided by each applicant allocated an access key.

Requiring content providers to retain the evidence itself imposes additional obligations not only under the Privacy Act 1998 (Cth), but also under the Payment Card Industry Data Security Standard (**PCI DSS**). The PCI DSS is a guideline created by the major credit card companies, to address issues like credit card fraud and identity theft. Organisations processing transactions from these major credit cards (American Express, Visa and Master Card) must comply with the PCI DSS. The penalties for non-compliance vary depending on the number of transactions the organisation processes per year and can result in an organisation being barred from processing transactions from major credit cards.

Many content service providers use credit card numbers as a form of evidence in the age verification process. Recording these credit card numbers, in order to comply with section 13 of the Proposed Declaration, would create additional obligations under the PCI DSS.

Recommendation

ASTRA submits that the Proposed Declaration should be amended to clarify that content providers do not need to retain the age verification evidence as part of their records under section 13. Content providers should be provided with the flexibility to record which type of evidence was produced by each applicant allocated an access key.

We look forward to discussing further with ACMA the issues we have raised. In the meantime, please do not hesitate to contact ASTRA should you require further information.

Yours sincerely



Debra Richards
Chief Executive Officer