



EUROPEAN COMMISSION
Information Society and Media Directorate-General

**BACKGROUND REPORT
ON
CROSS MEDIA RATING AND CLASSIFICATION,
AND AGE VERIFICATION SOLUTIONS**

Safer Internet Forum

25 – 26 September 2008

Luxembourg

1.	Introduction	3
2.	Cross Media Rating and Classification	3
2.1.	Classification and labelling – the rationale	3
2.2.	Terms	4
i.	Classification, rating and labelling.....	4
ii.	Pan European and Cross media	5
iii.	Convergence	5
2.3.	Overview national classification, rating and labelling schemes	6
i.	Offline content and offline distribution channels	6
ii.	Online, new media content	9
2.4.	Cross media rating and classification	9
i.	Kijkwijzer (The Netherlands)	10
ii.	The Mobile sector.....	10
2.5.	Pan European rating schemes	11
i.	PEGI and PEGI online for videogames	11
iii.	ICRA (FOSI).....	13
iv.	The quarto+ project	14
2.6.	Stakeholders view –from the online consultation and the Safer Internet Forum ..	14
3.	Age Verification Solutions	16
3.1.	Introduction	16
3.2.	Methods, implementation and national policies on age verification.....	17
i.	Self Certification.....	18
ii.	Credit and debit cards.....	19
iii.	Electronic Identity Cards (eID).....	19
iv.	Semantic analysis	21
v.	Social Security Numbers and similar identifiers.....	22
vi.	Biometrics	22
vii.	Offline verification, physical and parental control.....	23
3.3.	Media and service specific solutions.....	24
i.	Age Verification Solutions on Mobile platforms	24
ii.	Video on demand	26
iii.	Social Networking Sites	26
3.4.	Stakeholders view –from the online consultation and the Safer Internet Forum ..	26
3.4.	Age Verification Solution Providers and services	29
	Denmark	29
	Germany	30
	UK	32
	Belgium	32
4.	Conclusions.....	33
Annex 1.....		34
Resources and research projects.....		34
Annex 2.....		35
The Public Consultation.....		35
Cross media rating and classification		36
Age Verification.....		37

1. Introduction

The purpose of this background report is to give an overview of practices and solutions in Member States on Cross Media Rating and Classification and Age Verification Solutions. The report is based on desk top research and input from stakeholders to the online consultation launched by the European Commission in preparation of the Safer Internet Forum 2008¹ and the presentations and the debate at the Forum itself. As such, it does not set out to give a complete overview of all Member State policies and practices related to Cross Media Rating and Age Verification Solutions. There might be other Age Verification Solution providers and services than those that are referred to in this report, for instance.

This report is organised in two parts. The first part gives an overview of Rating and Classification practices. The second part looks at Age Verification Solutions. These issues are, however, linked. Age Verification Solutions take as a conceptual starting point that there are already rules outlining the type of content and services that are suitable to specific age groups. If the suitability of content and services were not linked to specific age groups, Age Verification Solutions would not exist in their current form. Media Rating has traditionally focused on audiovisual content. Age Verification Solutions are also discussed in relationship to Social Networking Sites, and in connection with eCommerce solutions for the sale of certain products, such as alcohol and pills, which are usually age restricted.

A distinction also needs to be made between authentication and verification. Authentication only proves that the user is who he says he is, but it says nothing about the age of said person. The lines between authentication and verification can be blurred, however, depending on the methods used for Age Verification – credit cards and biometrics, for example, may be effective methods of authentication, but may not provide accurate information about the age of the user for age verification purposes.

Finally, rating and classification cannot be separated from the labelling of content.

2. Cross Media Rating and Classification

2.1. Classification and labelling – the rationale

The process of rating, classification and labelling of audiovisual content is a response to the different moral, religious and otherwise cultural values of a society, whereby audiovisual content is assessed according to its suitability for specific age groups or for society as a whole. The rationale for rating, classification and labelling is linked to the protection of individuals from unsuitable content containing (or depicting) sexually explicit images, violence, and

¹Contributions to the online consultations can be downloaded from
http://ec.europa.eu/information_society/activities/sip/public_consultation/index_en.htm

crude or offensive language – but also involving an overall respect for the principle of human dignity.

2.2. Terms

Classification, rating and labelling are three distinct, but integrated steps, in the process of categorising content according to its suitability for minors and making the relevant criteria and age recommendations available through some type of textual, visual or sound signalling, or a combination thereof.

Some of the terms relating to the discussion on cross media and pan-European rating solution are not commonly defined. Drawing on the replies to the online consultation, an attempt has been made to clarify some of these terms, bearing in mind that there might be alternate views on how they are used and understood by those that are involved in classification, rating and labelling practises in the EU.

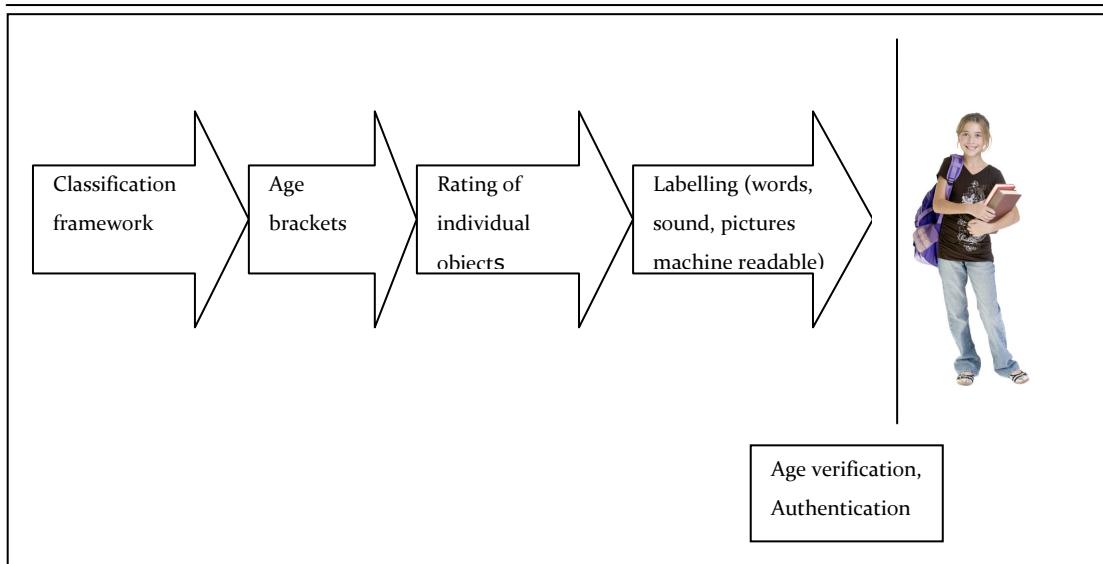
i. Classification, rating and labelling

Classification refers to the general process of categorising content into classes according to its suitability for certain age groups.

Rating refers to the process of evaluating single content objects such as a film, a video game, a web service etc. against the general classification framework.

Labelling refers to the visible mark attached to a specific film, broadcasted, on DVD, delivered online etc. There are numerous labelling schemes in use with the type of information they give and the method varying between different media platforms and countries. In broadcasting, for instance, films are often labelled by means of a visual symbol and/or in combination with a tonal signal.

Since any agreement or move towards a cross media rating mechanism also needs to consider the general classification framework and the labelling regime, a distinction is often made between these different steps – as referred to in the introduction above, and illustrated in the figure below:



ii. Pan European and Cross media

A *cross media rating system* refers to a rating system using the same rating for the same content independently of available distribution channels. In a cross media rating system a film would be rated according to a classification scheme and issued with an age bracket, plus additional information on the specific content of the film.

A *pan-European rating system* refers to a system where rating and labelling schemes are the same for similar and comparable categories of content across Europe.

A *pan-European cross media rating system* then refers to a rating and labelling regime applying a one stop rating mechanism independently of distribution platform and similar for comparable categories of content across Europe.

iii. Convergence

Convergence, or the act of converging and especially moving towards union or uniformity in the media sector, refers to the unification of all earlier media forms (print, audio, video, animation, and telephone) in a single medium brought about by digital technologies. In the broader sense convergence is also referred to in the context of network convergence (the efficient coexistence of voice, video and data communication within a single network) and platform convergence. Convergence has been the driving force behind many of the recent changes in the regulatory landscape affecting the audiovisual sector.

2.3. Overview of national classification, rating and labelling schemes

i. Offline content and offline distribution channels

In 2003 the European Commission published an empirical study on the Practices of Films Distributed in Cinema, on Television, on DVD and on video cassettes in the EU and EEA Member States². With regard to rating of audiovisual works the study showed great differences between Member States in how the rating process is organised, the type of criteria applied and format and distribution of specific features, including the use of labels, packaging, screen icons, tonal signals and watershed times.

The table below gives an overview of some of these practices related to national classification and rating schemes. Information provided has been taken from the 2003 empirical study and updated, where appropriate, based on the replies to the online consultation and other available online resources. Where no information has been available, relevant sections related to specific distribution formats have been left open.

The purpose of including this overview, in this background report in Cross Media Rating in the EU, is that awareness of the differences that exist with regards to classification and rating practices in Europe, is essential when any move towards a pan-European and cross media solutions is discussed.

Country	DVD	Theatrical release	Broadcasting	Video games ³
France	Films previously classified for theatrical release: same classification applies. Films directly released in video format: the Syndicate of Video Publishers (SEV) implements a self-regulation scheme including 4 age categories: “forbidden under 18”, “adults-not recommended under 16”, “not recommended under 12” and “all public”	All, 12, 16, 18, Pornographic films and films of extreme violence	All, 10, 12, 16, 18 - Watershed, visual and tonal	PEGI
Finland	Same legal provisions as for films	All, 7, 11, 15, 18	Tonal signal	Following an amendment in 2007 age rating of video games no longer corresponds to the age rating of other audiovisual programmes. Instead the PEGI system is used

² http://ec.europa.eu/avpolicy/docs/library/studies/finalised/studpdf/rating_finalrep2.pdf

³ A more detailed overview on the implementation of PEGI is provided in section i

Cross Media Rating and Classification and Age Verification Solutions

– Safer Internet Forum 2008

Country	DVD	Theatrical release	Broadcasting	Video games ³
Belgium	All, 12, 16	All, 16	Pictograms on age brackets (10, 12, 16, 18) and tonal signal	PEGI
Norway	Same legal provisions as for films	7, 11, 15, 18 (Accompanied by adults children 3 years younger than the set age limit are allowed)	Prohibition against content that may seriously impair the physical, mental or moral development of minors, in particular programmes of a pornographic and violent (gratuitous) nature. Watershed 21.00.	PEGI
UK	Same as for film	Uc, U, PG, 12A, 12, 15, 18, R18	Watershed, announcement	PEGI + the use of the British Board of Film Classification
Latvia		V, VP-10, VP12, N-12, N14, N-16, N18 . (N=Not recommended)		No foreseeable introduction of PEGI
Malta		U (Suitable for all), PG , 12, 14, 16, 18		No rating or classification system in use
Poland		BO, suitable for all, 6, 12, 15, 18, 21	Use of coloured symbols to indicate age suitability	PEGI
Portugal	Same as for theatrical release	M4, M6, M12, M16, M18.	Watershed 22.00 + visual symbol	PEGI
Austria	DVDs are not rated	6, 10, 12, 14, 16	Watershed (Until 20.15, 20.15 - 22, after 22) and visual symbol (K+, X, o)	Many games carry the German FSK labelling
Greece	Same as for theatrical release	13, 17, 18	Watershed 21.30 and 24.00	PEGI
Netherlands	All, 6, 12, 16	All, 6, 12, 16	All, 6, 12, 16	PEGI
Bulgaria	Same as for theatrical release	A (Recommended to children) , B (No age restriction), C (Not recommended to children under the age of 12) , D (Under the age of 16 not permitted), X (No people under the age of 18 permitted)		
Sweden	Same as for theatrical use. DVDs for private use classification is optional	Btl (Children allowed), 7, 11, 15,	Watershed 21.00, tonal signal	PEGI
Czech Republic		U, 12, 15, 18		PEGI used by big publishers
Cyprus				No age or content rating system in place
Luxembourg	DVDs are not labelled by any	For all, 14,17,	Choice between	No age or

Country	DVD	Theatrical release	Broadcasting	Video games ³
	authority in Luxembourg. Luxembourg use labelling schemes applied by neighbouring countries as is.	unsuitable for all	tonal and visual	content rating system in place
Romania		A.G, I.C.- 14, I.M.-18, xxx		No age or content rating system in place
Slovenia				No age or content rating system in place
Ireland	Categories G, PG and 18 the same as for theatrical release, however, there is no 16, and categories 12 and 15 are mandatory, not advisory.	G, PG, 12A, 15A, 16, 18	Watershed 9, tonal signal	PEGI
Spain	Same as for theatrical release	All, 7, 13, 18, Pornographic and extremely violent films	Watershed, visual and tonal signal	PEGI
Hungary		12,16,18		PEGI
Germany	Same classification as for theatrical release	FSK0, FSK6, FSK12, FSK16, FSK18	Watershed, age restrictions, choice between tonal or visual	Specific measures for age rating and labelling of video games.
Estonia		L (For everyone), Pere (For families, MS-16 (Not recommended for children under the age of 6), MS-12, K-12 (Restricted for children under the age of 12), Restricted for, K-14, K-16		PEGI
Denmark	Additional rules labelling and packaging	A, 7, 11, 15. Accompanied by an adult, children 7 or older can view any film	Watershed (21.00), spoken announcement	PEGI
Slovakia				PEGI
Iceland	Similar to classification for theatrical release, but with fewer categories (all ages, Not for younger, 12 and 16)	L, 7, 12, 14, 16,18		PEGI
Italy	Same classification applies for theatrical release	T, VM14, VM16, VM18	Self regulatory, Content marked according to suitability, coloured symbols + watershed	PEGI

Since the 2003 study, not much appears to have changed at the national level with regards to how audiovisual content is rated and classified for offline distribution. There are, however, ongoing discussions in countries like the UK, Belgium, Finland and elsewhere on what effects media and platform convergence should have on how audiovisual content is classified, rated and organised. The cross media rating solution used in the Netherlands is considered as a

model by other national media authorities, as one way of approaching the issue of rating and classification against the backdrop of media convergence.

ii. Online new media content

Digital content distributed over the internet, or to mobile platforms and video games has not been subjected to particular rating and labelling schemes by national media authorities. Those initiatives that exist are mostly industry driven, attempting to find practical and workable solutions for the protection of minors in an environment where time shifting makes traditional methods like watersheds unworkable.

For video on demand, an initiative like the Guidance Content Labelling System developed by the BBC puts more focus on the use of labelling and textual description of the depiction of sex, violence and unsuitable language in films than on the use rating and age limits. Based on independent research the BBC has found that parents prefer to make individual and informed choices about the suitability of films for their children. Parents did not consider that age rating properly accounted for the individual maturity level of a child.

Labels and age rating symbols are also used by a number of sites offering adult content to indicate the presence of explicit sexual material. There are also numerous so-called safe search tools, and filtering technologies that exclude unwanted content from being accessed⁴.

One example is the [Mybee.nl](http://www.mybee.nl)⁵ site that was launched by the Dutch foundation My Child Online⁶ in 2008. Mybee is a web browser intended to allow children up to the age of 10 to surf the web safely and easily. Access to sites is based on two white lists, one made by Mybee editors and the other by the parents themselves. The parental rating is based on a segmentation of parents into three categories based on their level of tolerance, and these are: tolerant, average and strict. This effectively allows parents to rate web pages according to how they judge the suitability of those pages for their own children, in what is described as a collaborative rating practice – as taken from the Safer Internet Forum.

2.4. *Cross media rating and classification*

As mentioned above, a *cross media rating system* refers to a rating system using the same rating for the same content independently of available distribution channels. In a cross media rating system a film would be rated according to a classification scheme, then issued with an age bracket, plus the additional information on the specific content of that film.

A cross media rating and classification scheme is only found in the Netherlands. In some Member States the same rating is applied across similar distribution channels for the same

⁴ See for example www.rulespace.com

⁵ <http://www.mybee.nl>

⁶ <http://www.mijnkindonline.nl/>

content. There are initiatives and debates on the effects of media and platform convergence that could lead to efforts in that direction in the future in other areas.

A number of different media formats are available on mobile platforms. Hence, the approach by mobile operators to regulate content access can be viewed as a sector specific solution to cross media rating and classification.

i. Kijkwijzer (The Netherlands)⁷

Launched by NICAM (the Nederland's Institute for the Classification of Audiovisual Media) in 2002, Kijkwijzer is a uniform cross media system for the classification of content for television, cinema, DVD distribution and mobile platforms. On Mobile platforms Kijkwijzer is limited to passive content distribution. The classification criteria are based on research into the effects on minors of audiovisual material.

Kijkwijzer is a collaborative effort. All sectors within the audiovisual industry in the Netherlands are involved in the development and the functioning of the system. One uniform labelling scheme is used across all media channels, consisting of an age rating recommendation, and a content description.

NICAM has conducted several consumer surveys on the usability, and acceptability of the labelling scheme used by Kijkwijzer. They found that as much as 90 percent of those targeted by the system, mainly parents with children under the age of 16, were satisfied.

NICAM is a foundation jointly established by Public Sector Broadcasters and commercial broadcasters, and is seen by many as a successful example, among others, of an effective co-regulation initiative in the media sector.⁸

Some countries have implemented a similar model to that of the Kijkwijzer, and there are others that are in the process of implementation; Turkey launched an equivalent in 2006, and Iceland is in the process of adopting one. Discussions are ongoing in Belgium, and in the Czech Republic on the possible implementation of a similar cross media rating solution in these countries.

NICAM is currently working on a project to prepare Kijkwijzer for use with online content.

ii. The Mobile sector

In 2007 the European Mobile Operators signed the “Safer Mobile Framework” – The European Framework for Safer Mobile Use by Younger Teenagers and Children⁹. This framework is a self-regulatory approach to the classification and rating of commercial content on mobile

⁷ <http://www.kijkwijzer.nl/index.php>

⁸ Study on Co-Regulation Measures in the Media Sector, http://www.hans-bredow-institut.de/forschung/recht/co-reg/Co-Reg-Draft_Final_Report.pdf

⁹ http://www.gsmworld.com/gsmeurope/documents/safer_children.pdf

phones and is designed to operate on an cross-media basis in each national market of the 27 Member States of the European Union.

Rating under this Framework is done by commercial content providers, and mobile operators present in individual national markets – based on an agreed cross media classification scheme. As pointed out by the GSMA¹⁰ Europe in their response to the online consultation, this approach reflects a reality where commercial content available over mobile phones is adapted and rarely produced originally for the mobile format. The implementation and use of national classification frameworks also allows for differences in cultural and religious values in separate markets, with respect to the protection of minors, to be reflected in the rating process. One national example within the Safer Mobile Framework is the UK Independent Mobile Classification Body who provides classification of content based on standards that are used in other media.

The cross media aspect of content delivery on mobile platforms relates to media formats such as games, text, film and pictures, including access to social networking platforms that are delivered on mobile platforms, to which a single rating and classification scheme is applied, against the background of existing rating and classification schemes applied for delivery in other channels.

Labelling of content in the mobile environment is not practical, and access control is based on Age Verification Solutions (Identity checks at the point of sale and the issuing of pin codes for example). In most countries mobile phones can only be purchased by persons over the age of 18, or by minors with explicit parental consent.

2.5. Pan European rating schemes

i. PEGI and PEGI online for videogames

The use and uptake of video games has seen a great increase in popularity in recent decades and the video game industry in the EU is the fastest growing and the most dynamic sector in the European Content industry¹¹.

After close consultation with industry, civil society – including parental and consumer associations and religious groups – the Video Game industry¹² adopted and launched in 2003 the so-called PEGI information age rating system. As a self-regulatory and an industry driven initiative the system was designed to protect minors from exposure to games unsuitable for

¹⁰ GSMA Europe is the European interest group of the GSMS Association (GSMA), representing 167 members in 50 European countries/areas serving 600 million customers. The GSMA is the global trade association representing more than 700 GSM mobile phone operators across 218 countries and territories of the world. In addition, more than 200 manufacturers and suppliers support the Associations initiatives as key partners.

¹¹ Communication on the protection of consumers, in particular minors, in respect of the use of video games, http://ec.europa.eu/avpolicy/reg/minors/video/index_en.htm

¹² The system is supported by major console manufacturers, including Play station, Xbox and Nintendo and by publishers and developers of interactive games throughout Europe.

their particular age group, at the same time replacing a number of existing age-rating systems at the national level. The uptake of PEGI in many of the Member States, replacing existing national age-rating systems is partly explained with reference to the varying cultural standards and attitudes considered when the system was developed¹³.

Rating is based on a self assessment form, after which the age rating is given automatically within the following age brackets: 16+, 18+, 12+, 3+, and 7+. A more detailed description of the system and the different symbols used for labelling purposes can be found at <http://www.pegi.info/en/index/id/176/>

The PEGI rating scheme was initially launched for console games in 2007 and expanded to include on-line video games. This so called PEGI-online, was an initiative co-funded by the European Commission under the Safer Internet Programme. PEGI online is using quality labelling and not age rating.

Since 2003 a majority of video games sold in Europe have been PEGI classified.

Supported by the major console manufacturers, PEGI applies in the vast majority of EU Member States, but not all countries have specific legislation in place.

The table below gives an overview of the implementation of PEGI with reference to its legal base:

Country	Applicability	Legal base
Finland, Greece, Italy, Latvia, Netherlands, Poland, Portugal, Slovakia, United Kingdom ¹⁴ , France ¹⁵ ,	Applied	Specific legislation ¹⁶
Belgium, Bulgaria, Denmark, Estonia, Hungary, Ireland, Spain, Sweden	Applied	No specific legislation
Germany	Not applied	German law on the protection of young people include specific measures for age rating and labelling of video games.

¹³ <http://www.pegi.info/en/index/id/176/>

¹⁴ Following one of the key recommendations on the Byron report commissioned by the UK government, the UK is in the progress of implementing a two tier system for rating and classification of video games. In addition to PEGI, video games will also be rated and classified according to the BBFC (The British board of Film Classification). The classification, rating and approval by BBFC concerns games with material of a sexual nature or portraying gross violence.

¹⁵ Amendments to French Criminal Law in 2007 provide for age classification and labelling according to age groups

¹⁶ Where specific legislation is indicated it refers to such acts as Act on Classification of Audiovisual Programmes, Video Recording Act, Law on Consumer Protection or Law on Public Information

Malta	Not applied	Video games fall under general legislation
Cyprus, Luxembourg, Romania and Slovenia	Not applied	No age or content rating system in place and no related legislating
Czech Republic	PEGI is used by large publishers, but not for the distribution of all video games	No system officially in place

The European Commission considers that “*there remains considerable room for improvement as regards the take-up of the PEGI system of classification in EU Member States and the compatibility of applicable national provisions with PEGI*”⁷.

Based on the large number of Member States using the PEGI for classification, rating and labelling of video games, and in spite of certain formal differences in, or lack of a legal base for its implementation, PEGI is still seen by most as successful – in terms of its wide geographical and cross border use. According to NICAM, this can be attributed to the following factors:

- The use of classification criteria based on concrete research
- Uniformed information tags and visual icons that are easily recognisable
- User friendly online classification software
- An expert help desk
- A well thought out complaints procedure for consumers
- The set-up of an independent complaints committee with extensive sanctioning powers
- System transparency

iii. ICRA (FOSI)¹⁸

The ICRA system, administered by the Family Online Safety Institute is a self regulatory initiative – where content providers, based on the ICRA questionnaire, label their own web content according to suitability for different groups of online users. Content is labelled according to a number of broad topics such as the presence (or absence) of nudity, the presence (or absence) of sexual content, the depiction of violence, the language used, the presence (or absence) of user-generated content (and whether this is moderated), as well as the description of other potentially harmful content – such as gambling, drugs or alcohol. The questionnaire contains more detailed questions about the use of specific terms under each category.

The use of the ICRA label and the underlying meta-data descriptions of the content on specific sites enables filtering systems, and other machine based tools to efficiently filter out content unsuitable for the different age groups.

¹⁷ Communication on the protection of consumers, in particular minors, in respect of the use of video games http://ec.europa.eu/avpolicy/reg/minors/video/index_en.htm

¹⁸ <http://www.fosi.org/>

FOSI will launch an updated version of the ICRA system in 2008, which will focus more on the involvement of the end-user, and give room for a more fine grained classification of content; embracing the social media revolution.

The ICRA system was initiated with the support of the European Commission and in the EU, but its use is not limited to sites hosted in the EU.

iv. The Quattro+ project¹⁹

Traditional quality labels and Trustmark's are logos that are visible to humans but undetectable by machines. Quattro plus is an EU funded project which has created a platform for delivery and authentication of interoperable, machine readable quality labels. The project builds on the Quattro project, which identified a demand for and the usefulness of machine readable quality labels. By allowing users to contribute to both to the creation of labels and the trust that other user may put in them, this has extended significantly, and aims to increase the number of labelling authorities using the system to promote a labelling culture.

The aim of Quattro plus is to make labelling of digital content easier for organisations, and for people authorised to award quality labels/Trustmark's. Adding social networking functionality to labelling, users will also be able to express their opinions about labels and be able to view aggregated information about these options.

2.6. Stakeholders view –from the online consultation and the Safer Internet Forum

The replies to the online consultation and the views presented at the Safer Internet Forum indicate that a move towards a cross media pan European rating system is considered difficult, unfeasible and unnecessary by most stakeholders. This confirms the evidence found by the 2003 Empirical Study, where little support was found for a push towards a pan-European cross media rating solution. What is referred to as a technological push towards a pan-European cross media rating system in the 2003 report, has not given way to a more positive view on the potential for a cross border approach in 2008, despite the increased availability of online content, the growth of online social networking, and platform convergence. National approaches are still preferred, and, with the exception of the Kijkwijzer, Member States have not moved significantly towards the implementation of cross media solutions. Discrepancies between media content regulation on different platforms is, however, an increasing source of public and political concern and the debate continues on how these challenges can be met.

One frequently mentioned argument against harmonisation is that rating and classification practices reflect national and regional differences, with respect to cultural and religious

¹⁹ <http://quattro-project.org/>

values. Whilst these differences are not seen as ultimate stumbling blocks, any move towards a pan-European policy must consider these differences to gain acceptance.

There are also those who view PEGI as a successful example of what may be achieved on platforms other than video games. In the view of NICAM, an agreement on a cross media rating system for passive content should be feasible: Classification schemes for films do not vary as much as one might think. Others view PEGI as a system that was established in the context of a major new medium, that was not previously subject to national regulation, and that the PEGI, for this reason, cannot be used as a model for initiatives to create a pan-European system, that would replace existing national ones.

And even PEGI has room for further improvements and could, according to some, include other rating elements²⁰ such as the presence of placed advertisement, similar in game marketing efforts and betting and gambling elements included in the storyline.

Consumer expectation and trust is also used as an argument against a pan-European cross media rating solution. Consumers are accustomed to existing Member State practices. Different audiences in different countries will have different expectations, as pointed out by the BBC at the Safer Internet Forum. Gaining their trust in a new system would be a huge challenge and require significant efforts. There is also the likelihood that a new system would cause more confusion and create less clarity than is provided by the existing systems.

Cultural differences, the potential threat to existing systems and that a new system will not develop trust with consumers were the three main objections raised by the Broadband Stakeholders Group in the panel debate at the Safer Internet Forum.

During the debate FDI said that cultural diversity, and how to capture these differences in a single system, is an issue. Even with PEGI they still encounter this debate. It should also be recognized that content on the internet is much more difficult to classify. The issue of a cross border pan-European rating and classification scheme also raises a number of other questions such as what is the aim and how will it be organised and controlled?

Instead of creating a new European Model, the Quattro plus project said that more attention should be given to machine readable solutions that are capable of integrating the many media rating systems that already exist. Increased use of quality labels and content descriptors could also remove the need for age rating practices all together, also on the national level.

Another argument against a cross media system is that there are differences between media platforms in how content is perceived by the viewer, and that these differences must allow for different rating schemes to be applied. The flexibility in having various age rating practices

²⁰ In the Byron report, the author concludes that the PEGI system is unhelpful and confusing for UK consumers, the logos are not well understood and the age ratings are sometimes interpreted to correspond with skill levels rather than suitability of content.

adapted to the distribution platforms should not be lost by the introduction of a one size fits all solution.

Future research should also consider actual cross border media consumption. If media consumption primarily concerns national resources, aiming at cross border solutions will not have the intended effect on the protection of minors.

There are also a number of other questions that must be addressed, such as how a pan-European system would be controlled, how complaints would be dealt with and not least what is the overall aim of the scheme.

At the Safer Internet Forum, the European Commission said that following the debate there are no immediate plans to push ahead with a pan-European cross border solution, and that they are indeed aware of the many differences that exist at the Member State level and the arguments presented against such a move. The European Commission still believes that there is room for continuous discussions on the issue, and that the Commission should continue to act as a facilitator of solutions to new media challenges. There are many avenues that could be further explored, such as white lists for filtering and the rating of web content for children at the EU level.

3. Age Verification Solutions

3.1. Introduction

This part of the report gives an overview of Age Verification Solutions. The aim is not to evaluate the efficiency of these solutions, which would require an individual assessment of a variety of technologies measured against a number of parameters, similar to the assessment of filtering technologies funded by the Safer Internet Programme.²¹ The Internet Safety Technical Task Force, organised by the Berkman Centre at Harvard University, announced earlier this year (2008) a request for technical submissions relating to child safety on the internet, with the purpose of evaluating the efficiency of technologies currently used. The Internet Safety Task Force report will be published in December 2008²², according to the Berkman Centre.

The purpose of any Age Verifications Solution is, by various methods used, to confirm and verify the identity and subsequent age of individuals attempting to use the services where age limitations are imposed for the protection of minors. Age Verification Solutions are, for the most part, implemented as a voluntary measure, but they are also mandated by law in some jurisdictions. They are also used for a wide range of online services, including:

- 1) e-commerce solutions for the sale of goods (typically alcohol, cigarettes and medication) and gambling

²¹ <http://www.sip-bench.eu/sipbench.php?page=results2007&lang=en>

²² http://cyber.law.harvard.edu/newsroom/ISTTF_techsubmissions

-
- 2) access to online content services depicting sexually explicit images and videos and violence, and
 - 3) for access to social networking sites requiring users to be of a certain age.

When Age Verification Solutions are being discussed the focus is first and foremost on their effectiveness, meaning their ability to protect minors by preventing access to harmful content and services aimed at an adult audience. Effectiveness is not the only concern, however. The cost involved, both in economic and in social terms, is also an important issue. While some methods might be highly effective they can not be viewed in isolation from alternative methods of protecting minors in the online environment and issues related to data protection and privacy.

3.2. Methods, implementation and national policies on age verification

Various methods for age verification purposes are being used by online services and third party technology providers. This section gives an overview of some of the methods used. Each method is briefly described and the different sections also include a reference to the positive, as well as the negative, aspects of each method - as viewed by the different stakeholders. The use of individual methods is illustrated with reference to existing services, and existing national policies on age verification.

As a general observation, most Member States have not introduced legal requirements on the use of Age Verification Solutions for the protection of minors in the online environment. Only Germany²³, UK and France appear to have legal requirements in place, requiring providers of specific online services and ISPs (France) to verify the age of users. In the UK, legal requirements apply only to online gambling²⁴ and in France certain general obligations apply to Internet Service Providers²⁵. The most extensive legal framework is found in Germany. The German model does not only require the use of age verification technologies by providers of specific exclusive services (adult content), it also prescribes a pre-approval mechanism by the state, of age verification technologies and providers, as described in more detail below. In the United States, the Federal Trade Commission has endorsed the use of adult age-verification tools that rely upon information about U.S. adults contained in databases of government and commercial institutions, in cases where online content that is likely to appeal to minors is unavoidable²⁶."

²³ § 4JMSV and §§ 184, 184c of the Criminal Code

²⁴ <http://www.gamblingcommission.gov.uk/Client/index.asp>

²⁵ Article 227-24 de la Loi 5 mars 2007

²⁶ See Self-Regulation in the Alcohol Industry, Report of the Federal Trade Commission, June 2008, at pp. 21-22, available at: <http://www.ftc.gov/os/2008/06/080626alcoholreport.pdf>. The age verification solution referred to in this case is that of Aristotle International's "Integrity" system. See description of that system at the Internet Safety Technical Task Force website, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Aristotle ISTTFTAB_submission.pdf.

The FTC Report notes that "adult age-verification tools, such as the one used by Anheuser-Busch to verify the [legal drinking age] status of visitors to the BudTV website, rely upon information about U.S.

When Age Verification Solutions are used despite the absence of any legal requirements is can be attributed to the general usefulness of these solutions as viewed by organisations involved in the protection of minors and requirements from consumer groups towards online service providers to provide at least some type of minimum guarantees.

Often, providers of online services apply several age verification methods in parallel. For example, some Social Network providers use self certification in combination with semantic analysis. Others use a combination of physical identity methods, as well as hardware and software based authentication methods for further authentication.

i. **Self Certification**

Self certification simply means that users are asked about their age, often when entering a site that contains adult content or when subscribing to social network services. Self certification is distinctly different from age verification solutions however in so far, as self certification relies solely on the information provided by the individuals themselves, and does not involve the use of other means to verify the correctness of the information provided.

When self certification is included in this overview the main reason is that self certification appears to be the most commonly used “method” by online providers of adult content services and social networking sites, not least because of the low costs involved.

Since self certification is so obviously flawed for purposes of age verification there are services using additional measures to prevent users from lying about their age. Cookies for example, which will prevent users from re-registering on a site with a different age, or walled gardens where children registering as adults to access adult content will lose access to their favourite programs from the same provider only available to minors. Other means consist of email verification, enforcing Age Limits and privacy settings.

Fig3.1: Negative and positive aspect of self certification

+	-
<ul style="list-style-type: none">• Easy to use• No additional costs for providers and end users	<ul style="list-style-type: none">• Relies on the honesty of individual users• Does not provide any guarantee for the correctness of the information provided.

A recent study on the effectiveness of self certification measures on Social Network Sites showed that nearly a quarter of children between the ages of eight and 12 are evading the age restriction imposed by social networking sites Facebook, Bebo and MysSpace.²⁷

adults contained in databases of government and commercial information, and have long been in use.” See <http://www.ftc.gov/os/2008/06/08o626alcoholreport.pdf> at n. 108.

²⁷ <http://www.guardian.co.uk/technology/2008/aug/07/socialnetworking.facebook>

ii. Credit and debit cards

Credit Cards and similar payments cards (debit cards and pre paid card) used for online transactions were not initially developed to verify the age of the card holder. And issuers of these types of cards, like VISA, do not take any responsibility to ensure that the customers are of the correct age. This responsibility lies entirely with the service provider²⁸.

Credit card checks can only be used as an age indicator for persons 18 and above. Moreover, credit cards, debit cards and pre paid cards are increasingly issued to minors as young as 13 years old.

Minors can also have access to credit cards issued to their parents.

A credit card transaction will also charge a transaction cost to the account of the card holder, limiting the use of this method to services that can charge this fee to a customer.

Some companies also issue anonymous cards, for the most part pre-paid ones where information in the card is not validated against an online database.

Fig 3.2: Negative and positive aspect of credit and debit cards

+	-
<ul style="list-style-type: none">• Credit cards are widely used and can be used as an indicator of the age of the cardholder.	<ul style="list-style-type: none">• Credit cards are issued for other purposes than age verification• The method can not verify the age of credit card holders under the age of 18, only that they are above.• Some cards are anonymous Minors can have access to cards without the knowledge of their parents

In Iceland a pilot project on chat rooms, for certain age groups using debit cards in the age verification process, is currently being prepared, in collaboration with the Office of Post and Telecommunications and the Ministry of Financial Affairs²⁹.

iii. Electronic Identity Cards (eID)

EID cards are electronic identity cards containing information about the user imbedded in an electronic chip on the card. EID cards are used for a number of purposes mostly associated with e-government services and were not initially developed for age verification purposes for the protection of minors. EID cards are essential tools for the implementation and use of electronic signatures, and the advance of eGovernment services where identification - for the purpose of border control, tax declaration, hospital services etc. - is essential.

²⁸ As referred to in the COPA case: “The rules of payment card associations in this country (US) prohibit Web sites from claiming that use of payment cards is an effective method of verifying age, and prohibit Web site owners from using credit or debit cards to verify age”.

²⁹http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating sns/results/eukidsonline_a532698.pdf

Since eID cards are issued by governments they offer the advantage of being a more reliable and trustworthy data source than other means of age verification.

One challenge is that eID cards may contain more information on the card than just the age of the cardholder, such as social security numbers and other identifiers for a wide variety of identity management services in the public sector. This raises serious privacy and data protection issues that need to be solved before eID cards can be more widely used for age verification purposes.

To date, the wider use of eID cards is also limited by the low number of countries having implemented them. While this could change as a number of Member States are in the process of implementing national eID schemes³⁰, cross border use of these cards will require a significant harmonisation effort on the EU level³¹.

Fig 3.3: Negative and positive aspect of eID

+	-
<ul style="list-style-type: none">• Using trust worthy data sources• When fully developed and solutions for interoperability between different systems have been solved, eID cards would address many of the flaws and draw backs of other age verification methodologies currently in use in the EU	<ul style="list-style-type: none">• Not developed for age verification purposes• Based on national standards• Varying degree of implementation and use on Member State level• Can result in the migration to other services

The Belgium eID scheme

The Belgium eID Scheme³² was launched as the first in Europe in 2001 and gradually used for a variety of eGovernment services. Embedded with a digital certificate, the purpose of the card issued to age groups 12 and above was to allow Belgian citizens to communicate online, conduct secure transactions with government agencies, and access government applications etc. A separate card was issued to children between the age 6 and 12.

Although not initially used for age verification purposes, the Secretary of State for eGovernment introduced special chat rooms³³ for minors between the age of 12 and 18 with the purpose of preventing abuse of children by adults online. This has not, however, been a

³⁰http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Nachrichten/Pressemitteilungen/2008/07/e_personalausweis.html A national eID Card for people at the age of 16 and older will be available in Germany in 2001

³¹ http://www.eid-stork.eu/index.php?option=com_content&task=view&id=57&Itemid=69
The STORK project is funded the European Commission. It aims at implementing an EU wide interoperable system for recognition of aid and authentication that will enable businesses, citizens and government employees to use their national electronic identities in any Member State

³² <http://eid.belgium.be/fr/>

³³ www.saferchat.be. See also www.chat.be and www.kidcity.be

very successful initiative. Minors have chosen to use other commercially available services where age verification methods are not being used.

Following privacy and data protection concerns raised by a number of stakeholders, the eID Card scheme is currently being revised with the aim of enabling Belgian citizens to identify and authenticate themselves for a wide variety of online services. The updated eID card will also enable the use of digital signatures. As such the eID card is a multipurpose document that can be used for healthcare services, as a driver's licence, for banking, e-commerce and as a tool for age verification. At the Safer Internet Forum the eID card was presented as a key that opens a number of doors.

The new eID card will contain information on identity, signatures keys, accredited certification, information needed for authentication purposes and residential address.

One card will be issued to Belgium citizens age 12 and above, one card will be issued to Belgium citizens age 12 and below and one card will be issued to foreign residents.

The card issued for children under the age of 12 is not obligatory and can not be used as an e-signature.

iv. Semantic analysis

Automated text analysis for age verification purposes is a method employing a search algorithm, using terms commonly used by underage users, to find under aged profiles on social networking sites, which is subsequently deleted. This method is used by My Space³⁴ as one of several safeguards to protecting teens online. The rationale is that people of different ages normally would use different levels of sophistication. The method is used in combination with other data sets available.

Fig 3.4: Negative and positive aspect of SA

+	-
<ul style="list-style-type: none">• The method can be used as a supplement to self certified information about age and provide an additional verification level.	<ul style="list-style-type: none">• Semantic and machine supported analysis still in its infancy• Persons have different levels of maturity• Can at best only identify the age range and not the exact age• Problematic in multilingual environments

³⁴http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating_sns/results/myspaceageverifsection1.pdf

v. Social Security Numbers and similar identifiers

Using social security numbers or similar identifiers managed by the public sector is not commonly used in the EU. While Social security numbers are used by the Public Sector to identify individuals in connection with eGovernment services, the use of social security numbers by private companies and individuals are often highly restricted due to data protection issues. There are numerous accounts of identity theft using social security numbers and similar identifiers such as “person numbers” of individuals issued by the public sector.

Fig 3.5: Negative and positive aspect of Social Security Numbers and similar identifiers

+	-
<ul style="list-style-type: none">• Highly reliable and trust worthy data source	<ul style="list-style-type: none">• Data protection and privacy concerns• Limited use in cross border services

A number of services in **Denmark** have implemented age verification solutions using identity checks against the social security number³⁵.

Outside Europe, an interesting example of the use of the social security number is found in Korea³⁶, where Google Korea asks users of the Google search engine interface to verify their age when adult content search terms are used, triggering users to provide their name and the Korean version of the social security number.

vi. Biometrics

Biometric solutions involve the use of technology that by means of capturing fingerprints, measuring the density of bones, iris scans and other biological differences, is said to be able to determine the age of users, at least within a certain range³⁷. The enabling technology (the scanner) connects to a computer via the USB port or comes built into the device³⁸. Biometric solutions can also involve the use of Webcams for facial recognition.

Fig 3.6: Negative and positive aspect of self certification

+	-
<ul style="list-style-type: none">• Trust worthy and more cumbersome to circumvent	<ul style="list-style-type: none">• Ethically offensive and privacy sensitive• Can not predict the exact age• Relatively costly and Relying on hardware components

³⁵ See for instance www.nogleskapet.dk

³⁶ <http://www.webpronews.com/topnews/2008/03/13/google-korea-starts-checking-ids>

³⁷ Biometrics are increasingly used for identify checks at border controls using biometric data incorporated in passports that are checked for validity against an external data base

³⁸ See as an example <http://www.netcaucus.org/books/childssafety2006/i-mature.pdf> and

A US social networking site targeting girls between the ages of 6 and 15 uses biometric technology to verify the age and identity of users³⁹.

vii. Offline verification, physical and parental control

A number of services are using face to face identification and physical control to verify the age of persons intending to use specific online services, including content delivery on Mobile Platforms. Physical age and identity verification is then supported by the use of traditional ID cards like a passport or a driver's licence. This method is commonly used by mobile operators at the point of sale for mobile devices. Outside the mobile sector, the German system for access to adult content provides another good example of this. In Denmark, a number of services also involve parents and teachers in offline age verification procedures for access to online services.

Fig 3.7: Negative and positive aspect of offline verification, physical and parental control

+	-
<ul style="list-style-type: none">Physical identification is one of the more reliable means of age verification. Strong means of verificationEffective	<ul style="list-style-type: none">CumbersomeUser migration to other platform and service providersThere is always the risk that minors get access to pin codes e.g.Costly

Age Verification for the protection of minors in Germany

The German law on the protection of Minors mandates the use of Age Verification Solutions. According to Article 4 (2) of the Interstate Treaty on the protection of Minors in the Media (JMStV) content proven to seriously impair the development of children, and adolescents is only legal (in “telemedia”) if the provider can assure that the content may only be accessed by adults.

The law makes a distinction between content that is absolutely illegal, content endangering minors and content that is harmful to minors. Content endangering minors includes content for adults only such as pornography and gambling, and providers are obliged to use what is referred to as a strict age verification solution, which intends to ensure that content is not available to minors. What is referred to as, “Basic Age Verification”, is applied to harmful content, like violent games and similar elements in games and chat rooms, as well as communities with a minimum of supervision.

Strict Age Verification implies a one-time physical identification, where the identity is checked against a valid identity card, either at the post office (e.g. PostIdent), at the point of sale in mobile phone shops, or at lottery offices. Other accepted forms of identification that rely on identity checks done in the past, and for purposes other than accessing harmful

³⁹ <http://www.annesdiary.com/>

content, are bank cards with an age criteria (65 million in Germany). The identity check is done in connection with the opening of a bank account, or the entering into of a credit card contract (e.g. Schufa-Q-Bit). A digital identity card with a build in age criteria for age verification purposes will be launched in 2010.

A subsequent authentication process takes place every time the identified person intends to access harmful content. To prevent multiplication of access data and the distribution of access data to third parties this includes the use of Unique Identifiers (copy protected hardware), bank or ID cards with age criteria or SIM cards, and clearly identifiable devices such as PCs or set top boxes, or so called PIN/TAN systems.

Basic Age Verification relies on the control of ID card control numbers, credit card numbers and sometimes web cam checks, intended to verify that the person is above 16 years old. The authentication is simpler than under the Strict Verification Process and uses a one time authentication and a pin code provided by SMS.

Based on the legal requirements of Article 4 (2) of the Interstate Treaty on the protection of Minors in the Media (JMStV), and what is referred to as Common Guidelines developed by Jugendschutz (KJM), Jugendschutz approves solutions and solutions providers in Germany to assure conformity to the legal requirements. To date the KJM has approved 24 providers of Age Verification Solutions⁴⁰.

According to the KJM the approval process is viewed as a seal of approval by industry. It has considerably reduced open access to adult content sites hosted in Germany.

3.3. Media and service specific solutions

i. Age Verification Solutions on Mobile platforms

Mobile operators use a variety of methods to prevent minors from accessing commercial content classified for adults (18 years and above)⁴¹. Physical control at the point of purchase has already been mentioned above, in combination with methods such as credit reference lists (i.e. Experian) and the processing of transactions on credit cards. At the point of sale, face to face control is supported by the use of identity cards, such as driver licenses, national identity cards and passports. Mobile Operators also use parental control mechanisms; In most countries minors are not permitted to sign up for a mobile subscription without parental consent, and many operators offer opt-out solutions where parents can restrict access to specific categories of commercial content services.

⁴⁰ <http://www.kjm-online.de/public/kjm>
⁴¹ http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating sns/results/dt_a532083.pdf

http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating sns/results/mbg_a531686.pdf

http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating sns/results/orang_e_a531653.pdf

Not all mobile operators use the same methods. In some countries operators' credit cards checks are used more extensively. Age Verification is also done against public data. In Denmark for instance, Mobile Operators can check against the Social Security Number provided by the state.

At the Safer Internet Forum Deutsche Telekom presented their approach to Age Verification in the German market, called NetGate. Following a registration process conducted at the Point of Sale, online or via the telephone, age is verified by means of 1) a credit check (Schufa and a method named Qbit) or 2) the T-mobile contract 3) Face-to-face control or 4) by means of the Postal Identification Service. Clearing is done either automatically or manually depending on the method used. Several access technologies, authentication methods and different hardware components are used in the authentication process, as visualized in the figure below:

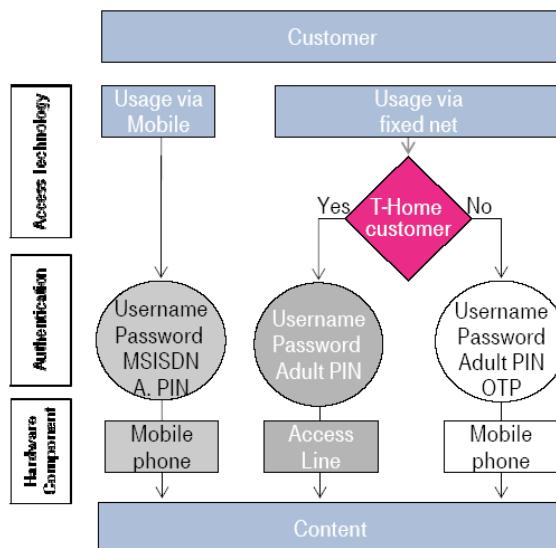


Fig 3.8: T-mobile

The combination of methods like this used in the “closed” mobile phone environment, can make the effectiveness, and reliability of Age Verification more achievable than in the more open environment of the personal computer.

The GSMA European Framework for Safer Mobile Use by Younger Teenagers and Children⁴² commits signatory mobile operators to the use of access controls to ensure that access to adult content can be restricted via mobile services.

There has also been a specific effort by providers of online content to design mobile-friendly versions of their sites to ensure that children are protected⁴³.

⁴² http://www.gsmworld.com/gsmeurope/safer_mobile/index.shtml

⁴³ In the contract with Vodafone, MySpace and YouTube are required to check all videos before they are made available to mobile browsers.

ii. Video on demand

Some providers of video on demand services have implemented Age Verification Solutions as a control mechanism to ensure that audiovisual content with a certain age bracket, following age rating requirements by industry or the public sector, is not accessible to minors⁴⁴. If effective, the combination of rating and age verification solutions would be the equivalent of physical access control to the cinema to watch a film.

iii. Social Networking Sites

In addition to Self Certification, used by most Social Networking sites as the only means of gathering information about the age of their users, some are experimenting with automated semantic analysis tools. Moreover, many of these sites rely on community self regulation mechanisms such as members reporting abuse, as a measure to keep adults from soliciting children. Recently, one of the more popular sites has asked users to provide one-time proof of identity such as drivers licence, passport or ID cards⁴⁵.

To increase efforts to protect minors online, MySpace and Facebook announced in 2008 a joint statement with 49 state Attorney Generals, where they agreed to form the Internet Safety technology Task Force to evaluate if an effective age verification technology exists or could be developed. At the Safer Internet Forum, My Space said that they had conducted extensive research and review of numerous identity verification solutions on the market and concluded that none of them are effective for social networking where adults and minors can congregate and interact.

The most popular Social Network Services (measures against the number of users) based in the US⁴⁶ set a minimum age limit of 13 and 14 for users to register. Recent studies show however that a large portion of children under the age of 12 falsely register with a higher age.

3.4. Stakeholders view –from the online consultation and the Safer Internet Forum

Based on the replies to the online consultation, and the views presented at the Safer Internet Forum, most stakeholders seem to agree that there is no existing approach to Age Verification that is as effective as one could ideally hope for, a view shared by those Age Verification Solution providers and services present at the Safer Internet Forum.

Each individual method carries its own flaws⁴⁷, as does any combination of methods used. And while additional security may be obtained by requiring physical identification procedures

⁴⁴ The BBFC Online scheme uses technology provided by NetIDME

<https://www.netidme.com/welcome.aspx> , see also the solutions provided by www.verify-U.de

⁴⁵ <http://blog.secondlife.com/2007/05/04/age-and-indentity-verification-in-second-life/>

⁴⁶ http://en.wikipedia.org/wiki/List_of_social_networking_websites

⁴⁷ The effectiveness of payment cards and Data Verification Services was under scrutiny in the so called COPA case in the US which concerned the constitutionality of the Child Protection Act. In the case,

like the ones used in Germany, these measures must be balanced against other interests and challenges posed by the cross border nature of the internet, lack of standards and the many different approaches that are taken in different Member States.

Even the German model, using face to face identity control, log in authentication and a walled garden approach, or the British model, restricting access to online gambling sites, (overall seen as the most effective in preventing access to sites using these technologies), have weaknesses that call for the use of additional, and non technical protection measures. In the cases of Germany and the UK, it is recognised that the global effectiveness of these solutions are largely undermined by the availability of sites offering similar services from other jurisdictions where age verification methods are not being used.

Cross border issues also arise from the use of typically national data sources that might not be accessible for Age Verification purposes for services located in other territories.

From a security point of view, as presented by Jeff Schmidt at the Safer Internet Forum, the use of Age verification Solutions for the purpose of the protection of minors must also be viewed from a risk management perspective. Not only are there initial problems with the identification and authentication methods used, such as the lack of secure and reliable data sources, it also creates the illusion of a safe zone which is not actually safe from determined and highly motivated predators. From his point of view, using Age Verification Solutions with the aim of creating more security is a bad trade-off that creates many new risks and opportunities for unintended consequences.

Given these flaws, many, including the Byron report and industry, have pointed to the risk of focusing too much on the use of Age Verification Solutions, to the detriment of the role of parental control and education. One of the lessons learned by Vodafone in their attempt to implement Age Verification Solutions is, that Age Verification Solutions must be delivered in tandem with an education and awareness programme.

Data protection and privacy is also of great concern. At the Safer Internet Forum concerns were raised by a number of participants on the use of national identifiers and other similar methods for data collection in connection with age verification as it risks undermining generally accepted norms on privacy.

Even if Age Verification Solutions are not considered a silver bullet, they are still used and viewed by many as necessary for the protection of minors. Accepting that there is no system that is 100 percent foolproof Age Verification Solutions can be made reasonably effective. There is already market acceptance for the use of Age Verification Solutions, even if they are

which rendered the Act unconstitutional and facially violative of the US constitution, none of these methods were seen as effective as a defence and minors access thereto.

not 100 percent efficient – as pointed out by John Phillips from the Age Verification Solution Provider Aristotle⁴⁸

At the Safer Internet Forum Jugendschutz emphasized that age restricted access regimes to internet services is both desirable and feasible, and that age verification will be an element that will have to be considered by providers of online services promoting content or services harmful to minors in the future.

John Carr from the Children's Charities Coalition on Internet Safety drew parallels to the sale of physical goods, where, according to UK laws (and the laws in many other countries) companies selling knives, alcohol, lottery tickets, scratch cards, fireworks, betting etc., must control that these age restricted goods and services are not sold to minors. In principle, these requirements apply equally to the sale of harmful goods and services in shops as they do to online retailing, but few countries have yet to require the use of online Age verification Solutions. His prediction is that in the next 10 years this will change and that Age Verification Solutions will be mandated as they have for online gambling in the UK. John Carr was also optimistic about solving data protection and privacy issues since technological solutions exist that can verify age without having to create databases with personal data - that can be accessed online.

Several recommendations were given for the future of Age Verification Solutions for the protection of minors, and the roles of the different stakeholders involved:

- Authorities should continue to monitor the development of Age Verification Solutions, disseminate good practices and work with industry to develop ways for parental control software to automatically communicate with websites to prevent children from signing up to sites using false information about their age⁴⁹.
- Age Verification Solutions must be technology neutral and not discriminate against different access technologies. Age Verification Rules should also be persistent with other media.
- Legal requirements and other means of government intervention must be based on transparency, stability and predictability, and sound co-regulatory measures, or alternatively left to industry by means of self-regulatory initiatives. One risk of overregulation is that users migrate to services located in other and less regulated jurisdictions.
- The effectiveness of Age Verification Solutions can only be achieved if they are universally accepted, inclusive, secure and relatively inexpensive.

⁴⁸ <http://integrity.aristotle.com/>

⁴⁹ The Byron report

- Age Verification Solutions cannot be readily relied upon in the absence of an Industry Wide Standard, for which further research and analysis is required.

3.5. Age Verification Solution Providers and services

In the EU, Age Verification Solutions appear to be more widely used in countries that have introduced legal requirements relevant to their use such as Germany and the UK. In Belgium and Denmark, where the use of age verification solutions is not required by law, the availability of trustworthy and accessible data for identity and age verification purposes seems to have been a determining factor.

The table below provides an overview of Age Verification Solution providers, organised at the country level. Some of these solutions providers are also service providers of online services targeting minors. In the case of Germany where online providers of content harmful to minors are subject to a pre-screening, service providers use any of the available methods for physical identity control in combination with technologies for authentication control.

This overview is non-exhaustive. There may be other Solution and Service Providers in the EU and EEA Member States than those that are listed here. It should, however, give a reasonable overview of the different methods applied and the domains in which they are used for the protection of minors.

Table 3.1: Denmark

Denmark			
Name	Description	Method	URL
Uni-Login	Identity management system used by all primary and secondary schools in Denmark and financed by the Ministry of Education. Provides log-in and authentication services for a broad range of IT services/application in the educational sector	User identity administration localised to individual schools using the Danish Social Security Number as a unique identifier on which individual login IDs and a password is created	http://support.emu.dk/ni-login/index.html
Priway	Conditional and context based age and identity verification	Combining several methods	www.priway.com
Nøgleskapet	PIN code login via online services supporting the use of this particular solution or via Nøgleskapet. When accessing a site using the PIN code, user name, social security number and other relevant identifiers confirmed. Parents can issue certificates to minors.	Digital signature validated against the Social Security number.	www.nogleskapet.dk

Netamina/Net-safe	Single login	Net-safe one stop shop registration using Infocards under the “CardSpace ⁵⁰ ” functionality in Microsoft Windows Vista	https://www.net-safe.info/about/#what
WAYF	Provider identification solution for minors using UNI-login (see above).	Transfer to the WAYF site when login on to dedicated online services. Generates a pseudonym and age bracket identification. A label is then issued for identification on online services towards users. other	https://www.wayf.dk
Certified Kid	Issues a open source based certificate for use in chat rooms	On site physical verification in schools subject to confirmation by teachers and parents	www.certifiedkid.com .
Lenio	Certificate only revealing the age of the user under full anonymity	Validated against the social security number	
Integrity		It works by verifying standard issue driver license or other government-issued ID of citizens of 157 nations.	http://integrity.aristotle.com/

Table 3.2: Germany

Germany⁵¹			
Name	Description	Method⁵²	URL
Verify-U	Age verification for videos on demand, trailers and similar audiovisual content	Software	www.verify-u.de
Goavs	Adult content		www.goavs.de
Coolspot AG	Adult content	Hardware+ pin code	www.x-check.de
Videoload	The Movie platform of Deutsche Telecom		www.videoload.de
Gamesload	Games		www.gamesload.de
Zentraler Kreditkarten ausschuss (ZKA)	German Central Credit Card Committee	Debit-Chipkarte	http://www.zentraler-kreditausschuss.de/
Arcor Online GmbH	Video on demand provider	Hardware based authentication	http://www.arcor.de/
T-Online International	Telecommunication and provider of Video on	Hardware based authentication	

⁵⁰ <http://www.microsoft.com/windows/products/winfamily/cardspace/default.mspx>

⁵¹ A more detailed description of the individual solutions referred above for Germany can be found at http://www.kjm-online.de/public/kjm/index.php?show_1=91,85,56

⁵² The method of physical verification is only referred to when the post office identification method is not used

Cross Media Rating and Classification and Age Verification Solutions

– Safer Internet Forum 2008

AG	demand solutions		
Vodafone D2	Telecom and mobile provider	Identity check when contract is signed + pin code for authentication purposed	http://www.vodafone.de/
Full Motion Entertainment GmbH	See http://www.kjm-online.de/public/kjm/index.php?show_i=91,85,56	Challenge Response procedure with hardware key in form of a VideoDVD and pin	http://www.kjm-online.de/public/kjm/index.php?show_i=91,85,56
RST Datentechnik/F.I.S.	Web application developer	CD rom and pin	http://www.dlscripts.net/
Hanse Net	Video on demand	Smart Card	http://www.hansenet.de/index.html
Giesecke & Devrient GmbH	Provider of smart card and security solutions	Internet smartcard for Authentication	http://www.gi-de.com/
insic GmbH	Online Gambling	Personal ID hardware component	https://www.insic.de/cgi-bin/WebObjects/Insic.woa/wa?dispatched=121930635451&locale=de
Fun communications GmbH	Provider of proof of age, payment, eTicketing eSignature and authentication with smart cards	Physical control point in Banks + smart card based authentication	http://www.fun.de/
SCHUFA Holding AG	Identity Service Provider	Credit checks	http://www.schufa.de/de/home/
Media transfer AG	Provides internet security technologies and services	Authentication using a system called mtg	http://www.mtg.de/servlet?do=home&lang=engl
Premiere AG	Video on demand and adult content	Smart card pin code	http://info.premiere.de/inhalt/de/index.jsp
Erotic media AG	Adult content	Pin code	http://www.kjm-online.de/public/kjm/index.php?show_i=91,85,56
Integrity		It works by verifying standard issue driver license or other government-issued ID of citizens of 157 nations.	http://integrity.aristotle.com/

Table 3.3: UK

UK			
Name	Description	Method	URL
NetIDMe	Verifies identity for sign up to a number of online services, including social networking sites. Also used - the identity of others.	According to the website NetIDMe uses a number of methods,	https://www.netidme.com/contentPages/about.aspx
Annesdiary		Biometrics, USB fingerprint reader	www.annesdiary.com
GB Group	Using ID3Check international ID verification and URU third party technologies.	One stop check against a number of sources (Passports, utility bills, payment cards, etc)	http://www.gb.co.uk/
192 Business	Solutions for online gaming providers	Age verification against Voter databases, credit references, passports, travel visas, national identity cards and voiceprint	http://www.192business.com/our-solutions/verification/age
Integrity		It works by verifying standard issue driver license or other government-issued ID of citizens of 157 nations.	http://integrity.aristotle.com/

Table 3.4: Belgium

Belgium			
Name	Description	Method	URL
Safechat	Closed Chat rooms for minors	eID	www.Safechat.be

4. Conclusions

A significant number of stakeholders gave their input to the online consultation and provided valuable input at the Safer Internet Forum on the issues of pan-European Cross Media Rating and Classification and Age Verification Solutions.

Industry and consumer organisations do not believe that a pan-European Cross Media Rating and Classification policy is either feasible, or instrumental for the protection of minors from harmful content for traditional offline media distribution platforms. Users are accustomed to existing national solutions and efforts to introduce a new system will only create confusion and not the clarity sought after by the approach.

PEGI, the cross border solution for games has been a success, even if improvements may still be achievable. There are also national and industry driven initiatives for rating and labelling of web pages and video on demand that are promising, including machine readable techniques. Some Member States are also considering implementing Cross Media Solutions based on the model of Kijkwijzer.

The Commission is, however, not pursuing a top down approach, but will continue to act as a facilitator and encourage the uptake of solutions for the protection of minors within the EU.

A number of Age Verification Solutions are available for the protection of minors within the EU, some of which were presented at the Safer Internet Forum. In some Member States there are legal requirements for their use. There is an overall consensus, however, that existing technologies are not sufficiently effective and should not be used to replace educational efforts, parental control and other means of protecting minors online. Despite the shortcomings, there is a certain market acceptance for their use. Concerns were also raised about the false sense of security that might be provided and the adverse effects on safety this might have. Privacy and data protection were also raised as important issues. Additional research is needed, and a standard for Age Verification can be pursued.

Annex 1

Resources and research projects

- Belgium Conseil de la Consommation (2008): Recommendations on the use of bank and similar payment cards by minors in the online environment:
http://mineco.fgov.be/internet_observatory/pdf/advice_fr_001.pdf
http://mineco.fgov.be/protection_consumer/councils/consumption/pdf_avis_2008/393.pdf
- Evaluation of the German youth media protection law by Hans-Bredow-Institute (German):
<http://hans-bredow-institut.de/forschung/recht/jugendmedienschutz.htm>
- Microsoft Windows Card Space
<http://www.microsoft.com/windows/products/winfamily/cardspace/default.mspx>
- IBM Identity Mixer Technology <http://www.zurich.ibm.com/security/idemix/>
- The Stork Project on eID schemes; http://www.eid-stork.eu/index.php?option=com_content&task=view&id=57&Itemid=69
- On the implementation of eID in Germany, press release;
http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Nachrichten/Pressemitteilungen/2008/07/e_personalausweis.html
- The Byron Report:
<http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf>
- Literature review of available research across the EU by Prof. Sonia Livingstone, London School of Economics: www.eukudsonline.net
- Internet Safety Technical Task Force Berkman Centre For Internet & Society
<http://cyber.law.harvard.edu/research/isttf/documents>
- The Safer Internet Programme,
http://ec.europa.eu/information_society/activities/sip/programme/index_en.htm
- On Social Networking and Age Verification, Adam Thierer:
<http://www.scribd.com/doc/2887234/Social-Networking-and-Age-Verification-ThiererPFF>
- The Law and Economics of Identity, Claire A. Hil:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=844345
- Good Practice Principles Audiovisual Content
<http://www.audiovisualcontent.org/audiovisualcontent.pdf>
- Final Report of the COPA Commission: <http://www.copacommission.org>

Annex 2

The Public Consultation

1. Public Consultation

This year's Safer Internet Forum 2008 (25-26 September) will be dedicated to age verification, cross media rating and classification and online social networking. The purpose of the public consultation is to gather the knowledge and views of the relevant stakeholders. The consultation is structured around 4 questions covering each of the above topics (Annex I).

2. Practical information

❖ The consultation is being launched in English, with an electronic version of the document. If you have received the document by mail and wish to reply electronically, please go to the website indicated below or send an e-mail to the address given below.

❖ Interested parties are invited to send their comments and replies to the following questionnaires to the Commission **by 31 July 2008 at the latest** using one of the following means of communication:

- Internet: <http://ec.europa.eu/saferinternet>
- E-mail: saferinternetconsultation@ec.europa.eu
- Post:

*European Commission
L-2920 Luxembourg
Directorate-General for Information Society and Media
Unit E-6 Safer Internet and eContent
For the attention of Mr Richard Swetenham*

You can submit your comments and replies to either one of the questionnaires, or to several of them. You can reply in any official language. However if you submit your comments in another language than English, we kindly ask you to submit also a summary in English.

❖ Electronic contributions received in reply to the consultation will be published on the Internet at the above-mentioned address. Publication online will be regarded as acknowledgement of receipt of your contribution by the Commission. For replies sent in paper form, an acknowledgement of receipt will be sent within 15 working days of receipt. If you do not wish your contribution to be made public, please indicate this clearly at the beginning of your reply. In that case, your reply will also not be mentioned in future documents which may refer to this consultation.

❖ If you are replying on behalf of an organisation, please state your name, address and official title in your reply. Any reply on behalf of an organisation which does not state the interests which it represents or the extent to which it is representative of the sector (number of members, size of organisation in relation to the sector to which its members belong) will be regarded as an individual reply and not a collective one.

At the end of the period during which contributions are accepted, after reading and analysing all the replies received, the Commission will prepare a report summarising how the consultation was carried out and the main points emerging. Contributions that you do not wish to be made public will not be mentioned in this document.

Questionnaire 1

Cross media rating and classification

With the current trend towards platform and media convergence, the opportunity and feasibility of cross media rating systems need to be discussed. In its recent Communication on the protection of consumers, in particular minors, in respect of the use of video games⁵³, the Commission welcomes and supports further efforts to achieve a self-regulatory and co-regulatory cross media, pan European age rating system.

One session of the Safer Internet Forum 2008 (25-26 September) will be dedicated to this topic. In order to collect facts and views on this issue, the European Commission launches a public consultation with the following questions:

1. Of which media rating systems are you aware in your country. Has there been an attempt to implement a cross-media rating system? If yes, what are the positive outcomes of it and its success factors? If no, what could be used as a starting point towards a cross media rating system?
2. What are the main obstacles moving towards a pan-European cross media rating system?
3. What role should the different stakeholders play (industry, public bodies, etc.), towards implementing a pan-European cross media rating system?
4. Are you aware of relevant research, pilot projects, or national cross media rating initiatives? If published online, please provide us with the relevant URL.

⁵³ http://ec.europa.eu/avpolicy/reg/minors/video/index_en.htm

Questionnaire 2

Age Verification

Various systems are used by internet, content and service providers, and mobile operators to verify the age of their users, and provide appropriate services linked to that age (e.g. access to adult content, access to social networking communities for adult only or above a certain age like 13).

One session of the Safer Internet Forum 2008 (25-26 September) will be dedicated to this topic. In order to collect facts and views on this issue, the European Commission launches a public consultation with the following questions:

1. Which age verification systems are you aware of? In which domains are they being used?
2. Do you think that these systems are efficient? If yes, please state why. If no, why do you think they are unsatisfactory?
3. Are you aware of legal requirements in your country for providers of online services to verify the age of their visitors/customers?
5. Are you aware of relevant research, pilot projects or national initiatives towards age verification on the internet? If published online, please provide us with the relevant URL.