ERGA ACADEMY 2018 WORKSHOP

PROTECTING CHILDREN IN AUDIOVISUAL MEDIA SERVICES - THE EFFECTIVENESS OF AGE VERIFICATION AND MEDIA LITERACY (ACTIVITY REPORT)

ERGA
European Regulators Group for Audiovisual Media Services

INTRODUCTION

"We are still at the beginning of an unimaginable shift in how we live. Let's give ourselves a break. If you have a problem with technology, perhaps you're not addicted, just cyber maladapted. And the good news: There are things you can do about that." Mary Aiken – The Cyber Effect

"When we talk about children as "minors" they seem very abstract. So it is good to keep in mind that children are born pretty trusting and willing to rely on parents and school; they believe in fairness and expect systems to be responsive to them; most of all, they want agency to express themselves and to explore. If adults block and restrict them, they will become distrustful of adults. We should take all this into account when building systems to protect them." Sonia Livingstone – Parenting for a Digital Future

Age verification and media literacy are two topics that currently lie at the heart of the debate on how to create an effective framework for the protection of minors in the digital environment. The protection of minors, in turn, has always been at the core of the mission of media regulators.

The newly revised Audiovisual Media Services Directive (AVMSD) is yet more proof of this, with these two concepts playing a prominent role in its text. Furthermore, the fact that they are together in the directive furthermore reinforces the idea that their impact on the protection of minors can be strongest if applied in combination.

On the one hand, technical protection creates a barrier on access to content potentially harmful to children, while on the other an educational approach helps the children develop media literacy skills necessary to navigate the new media environment safely. In other words these are two distinct approaches working toward the same goal. There are great hopes as to the potential of these approaches, but work must be done to understand the full possibilities and their practical impact to realistically assess this potential and, even more importantly, to be able to fulfil it. For this reason ERGA has chosen to concentrate on the effectiveness of both age verification schemes and media literacy in the second edition of the workshop on the theme of protection of minors.

This report is a structured summary of this workshop entitled *Protecting Children in Audiovisual Media Services - The effectiveness of age verification and media literacy* held in Brussels on 3rd October 2018.

Organised by ERGA and hosted by the European Commission, the workshop has gathered both representatives of the national audiovisual media regulatory authorities active in the field of protection of minors, and a wide range of carefully selected **external** personalities to contribute to the lively debate:

- **Rachel O'Connell – Trust Elevate**
- **Max Beverton – Sky**
- **Sonia Livingstone – London School of Economics and Political Science**
- **Mary Aiken – Geary Institute for Public Policy, University College Dublin**
- **Eva Lievens – Ghent University**
- **James Steyer – Common Sense Media**
- **Dan Mount – Ofcom**
- **Ciarán Kissane – Broadcast Authority of Ireland**

The workshop was moderated by Lubos Kuklis, chairman of ERGA, who opened it by confirming the **long-term commitment of ERGA to the theme of protection of minors** as one of the core activities of the regulatory authorities. He emphasised all the previous work of ERGA on this topic, including a separate subgroup in 2016. ERGA is therefore looking to continue this workshop series into the future as a discussion forum on carefully selected topics.

The selected themes for this year's edition were already part of the broad range of measures discussed in the first edition of the workshop in 2017 (see report). But their importance, reinforced by the revised AVMSD, gave strong arguments for examining them in more depth.

The workshop was thus divided into **two thematic sections:**

- **Effectiveness of age verification mechanisms and the potential use of the eIDs**

  The first session focused on the effectiveness of age verification mechanisms and the potential use of the electronic identification systems (eIDs) for the protection of minors. Age verification mechanisms are the bedrock of the measures taken for the protection of minors (especially in the case of video on-demand (VOD) and video-sharing platforms (VSP) services) and will be at the forefront of the implementation of the AVMSD. Firstly, their real-life effectiveness was discussed. We then looked at the planned initiatives of the European Commission and various member states in the area of eIDs and their potential use for trusted age verification, based on the opportunities provided when the eIDAS regulation came into force.

- Possible impacts of the audiovisual content consumption on minors and the effectiveness of media literacy policies

The first objective of this session was to have a unique overview of the current knowledge about the impact of online audiovisual content consumption on minors with the help of strong and diverse academic voices. Secondly, we tried to connect this state of knowledge with the media literacy measures and specific activities of the National Regulatory Authorities (NRAs). At the same time a best practice example from outside of Europe was used to provide a different angle in the debate. This discussion was framed in the context of the new media literacy article in the AVMSD and its implementation by the NRAs.

The chronological order of the presentations and debate is, however, not necessarily reflected in this report as its aim is to bring deeper insights from the presentations and debates that transpired at the event by following and connecting the ideas which developed in various sessions. This approach should ideally capture most of the value created by gathering stakeholders from the relevant sectors.

The report is thus divided into **five sections** that follow the topics addressed by the attendees:

1. Age verification mechanisms and eIDs
2. General Data Protection Regulation (GDPR)
3. Media literacy
4. Content rating and oversight
5. Children's media consumption – national case studies

LIST OF CONTENS

EFFECTIVENESS OF AGE VERIFICATION MECHANISMS AND THE POTENTIAL USE OF THE EIDS

1 EFFECTIVENESS OF AGE VERIFICATION MECHANISMS AND THE POTENTIAL USE OF THE EIDS

1.1 Age verification mechanisms

Firstly, we focused on the age verification mechanisms that are currently available or under development. At the workshop, there were speakers from **Ghent University, Trust Elevate** and **Sky**.

Eva Lievens - Ghent University

Ms Lievens is an Assistant Professor of Law & Technology at the Law Faculty of Ghent University. A recurrent focus in her research relates to the protection of minors in digital media, human/children's rights and alternative regulatory instruments, such as self- and co-regulation. Eva is a member of the Flemish Regulator for the Media and the Belgian Film Evaluation Committee. She has also been a member of various working groups advising the Federal and Flemish government (for instance concerning the right to reply in the digital media environment, cyberbullying and the adoption of a labelling and classification system for audiovisual content).

Eva Lievens from **Ghent University** talked about age verification in recent legislative initiatives in an attempt to address certain questions related to these initiatives. In today's world, we may want to look at people's age for variety of reasons, e.g. when checking if a person is over a certain age and is therefore authorised to travel for a reduced price. However, the workshop was aimed at mechanisms that help prevent individuals under a certain age (often children) from accessing or obtaining content, goods or services that are considered age-inappropriate.

Ms Lievens mentioned **several examples of websites that use some kind of age verification**, for example a gambling website Unibet which, in Belgium, uses the national registry number which includes the date of birth. She also mentioned that there are often age affirmation pages (e.g. on Facebook) which are aimed at confirming that a person is over a certain age. The self-reported age, however, is not checked. She referred to the recent Council of Europe Recommendation on Guidelines to respect, protect and fulfil the rights of the child in the digital environment[1], which recommends that states should require the use of effective systems of age verification to ensure children are protected from products, services and content in the

1 https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights- of-the-child-in-th/16808d881a

digital environment which are legally restricted with reference to specific ages, while at the same time using methods that are consistent with the principles of data minimisation. She stressed that the UN Convention on the Rights of the Child is very important in this regard. A child's freedom might be at stake if they are over-restricted, but their well-being may be at stake if allowed to roam the internet with too few restrictions.

Ms Lievens then talked about **Article 6a of the new AVMSD** which lists possible measures to ensure that audiovisual media services that may impair the physical, mental or moral development of minors are only made available in such a way as to ensure that minors will not normally hear or see them. This article also mentions that the most harmful content, such as gratuitous violence and pornography, shall be subject to the strictest measures. She raised the question of whether age verification can be classed as one of the ***"strictest measures"*** to ensure that children will not see or hear such content. She mentioned that age verification is also present in Article 28a of the new AVMSD, which sets down provisions for VSPs for the first time.

According to Ms Lievens, it is important to note that age verification ***should not lead to excessive data processing (article 6a of AVMSD)***; usually the only attribute that needs to be known is whether a certain individual is under a certain age, therefore not the exact date of birth, or even exact age is needed. In her opinion, an important part added to the new Articles 6a and 28a AVMSD states that personal data that might have been obtained through age verification procedures shall not be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising.

Article 6a (2) - AVMSD

"2. Personal data of minors collected or otherwise generated by media service providers pursuant to paragraph 1 shall not be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising."

Article 28a (3) (f) - AVMSD

"(f) establishing and operating age verification systems for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors;"

Rachel O'Connell - The Trust Elevate

Dr O'Connell is a founder & CEO of Trust Elevate, which developed an age-checking service providing reliable consent directly from consumers verified against authoritative data sources, enabling businesses to comply with GDPR, AVMSD, and related legislation. She is one of the prominent authorities on electronic identification and age verification and is the author of a technical standard entitled PAS 1296 Age Checking code of practice. She was also instrumental in operationally building the business of the start-up social networking platform, Bebo, which was acquired by AOL in 2008 for $850M. In 2000, Rachel set up the Cyberspace Research Unit, at the University of Central Lancashire and secured funding from the European Commission to establish and operate the first UK Internet Safety Centre (2000- 2006).

Rachel O'Connell from **Trust Elevate** started her presentation with the notion of trust being a fundamental building block of the data economy. In her opinion, GDPR changed the parameters of the digital economy. She also pointed to the UK Digital Economy Act 2018 that introduced a new requirement in law for commercial providers to establish robust age verification controls for online pornographic content in the UK. It established a new regulatory framework backed by civil sanctions to monitor, notify and enforce compliance with the law. The British Board of Film Classification (BBFC) will soon begin its role of Age verification Regulator under the Digital Economy Act 2017, ensuring that all online commercial pornographic services have effective age verification controls in place to prevent access by persons under the age of 18, and do not carry any extreme pornography as defined under the Criminal Justice and Immigration Act 2008.

Typically, **traditional age verification methods** oblige each business to conduct a level of due diligence to collect a customer's personally identifiable information, and cross-check it against identity databases to establish age. Businesses must then store verified personally identifiable information which, not only carries privacy concerns but also poses a significant security risk, as this data is attractive to hackers. The adult entertainment sector therefore said they do not want to deploy the traditional approach to age verification (possessing all the data about a person and storing it). They argued that it is natural that people do not want their information to be known, especially when it comes to certain businesses.

Recent technology and policy innovations in the electronic identity sector mean that it is now possible for age check services to check a single attribute of an individual's identity (i.e. age-related eligibility). Age-related eligibility checks pose a question "Is this person over 18 years of age?", which elicits a yes/no response. That is, a customer's current age determines which services he/she is or is not eligible to access and it might relate to a single value

(e.g. over 18) or an age range (e.g. between 13 and 17). Determining eligibility is therefore privacy-enhancing as it reduces the amount of personal data a relying party retains. The term "age checking" is used throughout the PAS 1296 Age Checking code of practice, published by the British Standards Institution in March 2018, to differentiate between traditional methods of age verification and those currently available on the market. "Age check services" is an umbrella term that includes both age check providers and age check exchanges that enable a range of business sectors to meet evolving legal, self and co-regulatory requirements to establish an internet user's age-related eligibility to access content and services online. Age check services can meet the needs of a range of age-rated services that might require either a specific age or the age band into which a customer fits, which might be over 18, or under 13 years of age for instance. An age check elicits a yes/no response to a query such as whether this person is over 18 years of age or under 13 years of age. As mentioned previously, adult entertainment businesses wanted a new approach. An example is the **"Verify once – use many times" approach** which provides reliable age-checks and consent directly from consumers who are verified against authoritative data sources, enabling businesses to comply with GDPR, AVMSD and related legislation.

Platforms that enable **federated attribute management** handle the use of attributes, such as age, across security domains (e.g. between internet users and organizations), in accordance with a set of rules defined in a trust framework, a legal document that deals with issues such as interoperability, liability, security, privacy and trust. A federated model also enables an internet user's age to be checked once, with the response tokenised and reused as per a set of business rules, which can significantly reduce costs to businesses.

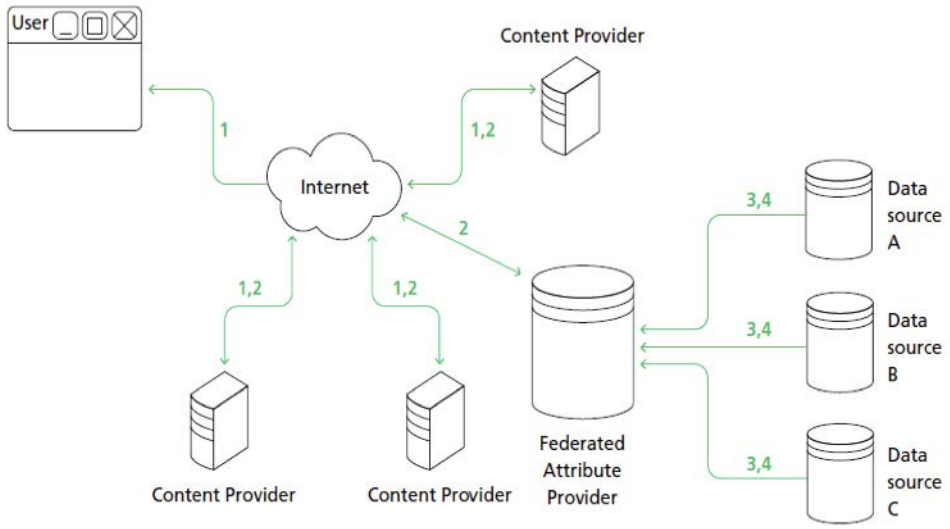


Diagram of a federated attribute management by Rachel O'Connell

Dr O'Connell also talked about the **Publicly Available Specification (PAS) 1296, Online Age Checking**. It gives recommendations for a framework regarding the provision and use of online age check services. This includes, for example, checking the age-related eligibility of those accessing online content, using online services and enabling access to online age-gated material and services. The PAS gives recommendations for processes that can be applied when providing and using age check services to protect consumers and online merchants or to assist an organization that wishes to enable enhanced e-safeguarding.

When creating an **age check service**, the following **elements** should be ensured: data protection principles, trust capability statements (the age check service should categorize its authoritativeness as a source of age-related data) and conformity assessment (the age check service should record any standards to which it conforms). It is also important to take into account questions of audits (the contract between a reliant party and an age check service should stipulate whether or not a third party assessor audits the service), intelligent monitoring (the reliant party should stipulate in a service level agreement or equivalent, the point at which to respond to activity flagged by the monitoring system as possibly suspicious and the extent and timing of that response), and customer support (the reliant party should establish the processes in place for handling customer queries and complaints with an age check service).

Dr O'Connell described **vectors of trust** communicated with the age-related eligibility token, namely:
A vector of trust is designed to be used in the context of an identity and authentication transaction, providing information about the context of a federated credential and consists of the following dimensions:

- The **Identity Proving** dimension defines, overall, how strongly the set of identity attributes have been verified and vetted. In other words, this dimension describes how likely it is that a given digital identity transaction corresponds to a particular (real-world) identity subject.
- The **Primary Credential Usage** dimension defines how strongly the primary credential can be verified by the Identity Provider. In other words, how easily that credential could be forged or stolen.
- The **Primary Credential Management** dimension conveys information about the expected life-cycle of the primary credential in use, including its binding, rotation, and revocation. In other words, the use and strength of policies, practices, and security controls used in managing the credential at the IdP and its binding to the intended individual.
- The **Assertion Presentation Dimension** defines how well the given digital identity can be communicated across the network without information leaking to unintended parties, and without forgery. In other words, this aspect describes how likely it is that a given digital identity was actually asserted by a given identity provider for a given transaction.

In a white paper[2] produced by a cross-industry think tank exploring the issue of Article 8 of the GDPR, the industry recognised that the need for a widely recognised, effective and reliable method of parental verification which can be applied globally. Such a method should be supported by regulators and developed together with the industry.

To align with the GDPR's principle of accountability, data controllers may only appoint data processors which provide sufficient guarantees to implement appropriate technical and organisational measures to ensure processing meets the requirements of the GDPR. Processors are required to process personal data in accordance with the controller's instructions and must obtain explicit and informed consent to process data. In other words, data processors must also obtain consent to process the data of children and young people. In effect, data controllers must have a contractual relationship with data processors. Dr O'Connell presented the TrustElevate Trust framework that will include the contractual relationships between all parties and will govern how the Federation operates. A federated model works on the premise of "verify once, use many times", which drives down the cost to business of conducting Verified Parental Consent and age checks.

Dr O'Connell added that GDPR and AVMSD will precipitate a paradigm shift in digital parenting by ensuring the facilitation, via digital platforms, of higher levels of parental engagement in decision making situations concerning who has access to a child's data and the nature of the content to which age-checked children are exposed. GDPR and AVMSD also foster dialogue about the nature, scale, extent and operationalisation of the legal Duty of Care that digital platforms have toward children and young people in technical and policy terms. When companies go through the process of age-verification, it can make it easier for everybody, both parents and children. It is important to give children the ability to make the choices themselves. Respect for the rights of children is the central underpinning to both the GDPR and AVMSD, which aims to give users greater control of their personal data and enable companies to serve age-appropriate content in accordance with safer-by-design principles. The VERIPASS app was described as an example of a tool to facilitate said control.

VERIPASS app by TrustElevate

Trust Elevate is the first company globally that verifies an assertion of parental responsibility for a child and age-checks that child. Trust Elevate is a B2B2C proposition that enables a company to obtain consent from the parent or guardian of a child who wishes to access a platform or app to either grant or withhold permission for their child's access to the site, and both the data controller and processors to process their child's data. The Parent has a permission dashboard within the app and can thus give consent or revoke it at any time. The whole system is intuitive and easy to use. Once providers know the age bracket of the child and who has the parental responsibility for the child, they can exercise a duty of care towards the well-being of that child and create communities built on trust, and for example, serve age-appropriate content.

2 *https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf*

Max Beverton – Sky

Mr Beverton is Head of Digital Policy at Sky and responsible for public policy issues and government relations across all of Sky's TV channels, content, communications services and social initiatives. He looks after Sky's advertising business' relationships with the government, regulators and political stakeholders. He is also Sky's Director on the Broadcast Committee of Advertising Practice (BCAP) – the industry co-regulator for broadcast advertising. Prior to joining Sky in 2015 he spent six years at the industry regulator Ofcom working developing regulatory policy and strategy for the communications sector.

Max Beverton from **Sky** said that, although the regulation of VSPs in the revised AVMSD is an important first step towards a more level playing field, there is a long way to go to achieve a functioning regulatory model for online harm. Due to new technological developments like Artificial intelligence and machine learning, the question of ethics has now resurfaced. He believes that the most important thing a regulatory framework provides is the mechanism and incentive to ensure online platforms companies comply with the rules. In his opinion, tech companies and platforms should have regulated responsibility for their conduct and for the way they manage what is shared on their various platforms.

As Mr Beverton pointed out, Sky is not only a broadcaster but also an internet service provider. If a website does not comply with the legal requirements for age verification of online pornography, under UK law after April 2019 they can issue an ISP block which means that the website in question will not be available to users. Sky cares about regulation because they want to do the right thing for their customers and to create value for their customers. That is why they created the **Sky Kids app** which parents can set up to provide children with a safe space to enjoy video content and games. They also launched partnership with Common Sense Media in order to provide parents with an easy-to-understand language when it comes to content rating.

In his opinion, people can use TV as a sort of babysitter but cannot use an iPad as a babysitter as they never know where children are going to click on the screen, which presents a problem for our society. Mr Beverton said that **self-regulation will not work with just voluntary codes, there has to be enforcement.** Regulation is about enforcement and sanctions and bringing people into the sector.

Sky Kids app

An app developed with specific controls for parents such as a bedtime setting which puts time limits on how long a child can watch content on the service. The app was designed with children and parents to make it user-friendly for young children, but also allow parents careful control over how their children use the service. The content available on the Sky Kids app is only content from Sky's on demand catalogue that is suitable for children. Parents can choose age ranges to provide a different experience for different ages of children using the app.

When it comes to platforms, Sky does not want deregulation for its own services but a level playing field. As was already stated, their opinion is that some kind of formal regulation is needed. They want a principle-based system that makes platforms accountable. The regulatory authorities need to look at the processes behind the systems, so as to understand how those systems work. There is information asymmetry because regulatory authorities do not have all the information behind algorithms used by platforms. In his opinion, **principle-based regulation** works well because it encourages the companies to adhere to the principles of conduct set by the regulator rather than trying to regulate every single bit of content on the web. In order to make age verification effective, transparent technology needs to be in place.

1.2 Use of eIDss

Andrea Servida – European Commission

Mr Servida joined the European Commission in 1993 and has been the Head of Unit on "eGovernment and Trust" at Directorate-General for Communications Networks, Content and Technology since 2006. He leads the team in charge of the European eGovernment Action Plan 2016-2020 as well as rolling out of the eIDAS Regulation on electronic identification and trust services for electronic transactions in the Internal Market.

Andrea Servida from the **European Commission** talked about the potential use of electronic identification systems (eIDs) in age verification. The eIDAS Regulation[3] provides for cross-border mutual recognition of secure and trustworthy electronic identification means for online access to public services. Being a regulation, it applies directly across the whole EU and thus creates a level playing field of rules, which boosts trust and supports businesses. eIDs provide a high level of security experienced in a way that is convenient to the user. For users, a system should be easy to use. Therefore, a truly useful age-verification system should be seamless and cross-bordersystem of security experienced in a way that is convenient to the user.

For the purpose of electronic identification, the aim of eIDs is that the service provider only receives the data necessary for the individual transactions, for example the age, but not the birthdate or gender. 25 EU states already have an identification system in place, and Germany, Italy, Spain, Luxembourg, Estonia, and Croatia have already notified the European Commission of their schemes under the eIDAS. In addition to these states, Belgium and Portugal are now completing the peer-review of their schemes and the UK has just issued a pre-notification regarding their scheme.

eIDAS plays a role in many areas. The vision of the European Commission is that **eID should speak for us** and not about us. eIDAS gives the opportunity to citizens to control and selectively disclose identity data when accessing online services across borders and also to limit the collection of their identity data to those strictly needed for a transaction, while always ensuring full accountability of the service provider. It allows for the implementation of the data minimisation principle – only collecting the information necessary for a transaction.

3 Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Authentication to validate the age of the person can be performed at various **stages**:

- during the process of user registration on the content provider platform;
- as an additional verification procedure for users already registered;
- in cases where the access to the content does not require registration – no information on the identity of the user but only to assert above the minimum age of use.

Mr Servida said that media providers want to have legal certainty and that for now there is a **disparity between the media providers and platforms**. It is important to know the awareness of the user. In his opinion, platforms have to be more transparent about their business model and regulation should be more vocal about promoting privacy by design. The problem is not the technology that adheres to the rules but the technology that does not want to adhere. Tech companies have no incentive to comply with rules.

According to Mr Servida **providers have a social and ethical responsibility toward the user**. The eIDAS pushes providers to be clear about the purpose of using personal information. There has to be an assertion with the identification of the profile, to know who is behind the profile when a need arises. Our identity is our data and we should have control of it, Mr Servida said. He then presented the SaferChat pilot of the STORK (Secure Identity Across Borders Linked) project, which is designed to ensure that only teenagers of a certain age can access chat rooms included in online courses.

SaferChat pilot in STORK project

This pilot was part of the STORK project that makes it possible for millions of EU citizens, resident in a Member State other than their own, to access online public services wherever they are located. The SaferChat pilot involved pupils and teachers in Austria and Iceland and used eID to verify the age of the users. This verification was intended to ensure that only teenagers between 14 and 18 could access the chat rooms included in online courses. The purposes of the pilot were to test the STORK enabled infrastructure to offer real life services to real life users and to test the possibilities offered by a cross-border interoperability platform with a great potential of development in the future.

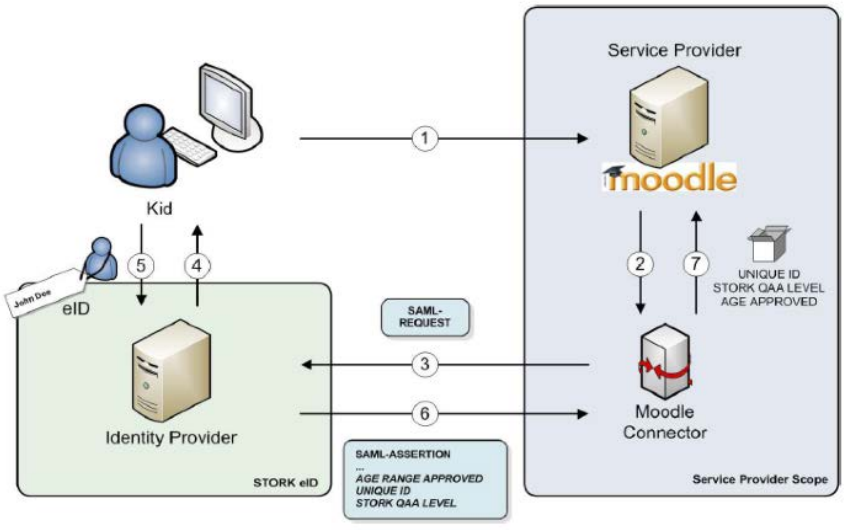


Diagram of the operation of the STORK project

GDPR

2 GDPR

When it comes to the protection of minors, **Ms Lievens** highlighted that the **GDPR includes a recital about specific protection for the personal data of children.** The GDPR does not explicitly require age verification of data subjects but age verification is relevant to Article 8 of the GDPR (consent in relation to information society services offered to a child). According to the Article 29 Working Party,[4] relying on the consent of an underage child will entail that the processing of his or her personal data is unlawful. Processing of personal data should comply with the principles laid down in the GDPR (data minimisation, purpose limitation, fairness, lawful grounds, etc.). Age verification should not lead to excessive data processing; usually the only attribute that needs to be known is whether a certain individual is under a certain age (not exact date of birth, nor even exact age is needed).

Recital 38 of GDPR

"Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child."

In the GDPR, there are critical **opportunities regarding safeguards in connection with the processing data of children**. When processing their data, the rights of the child should always be taken into account, for instance through carrying out data protection impact assessments. Since the providers know so much about what people do online, they could theoretically deduct their age as well, for example by using profiling. The question is whether this is desirable. All these fields are becoming very interlinked but Ms Lievens highlighted the advantages of closer cooperation between media regulators and data protection authorities when it comes to the mechanisms and tools used for processing information about children.

Ms Lievens added that a lot of focus was on the ages at which theyr parental consent is required. Since the entry in force of the GDPR, however, many companies decided not to opt for consent as a main ground for collecting and processing data, but have chosen the grounds of contract and/or legitimate interest. This is something people should be aware of and data protection authorities will need to assess whether this is a valid choice. Certain policies appear to attempt to circumvent consent. At the same time, scholars also argue that

4 Article 29 Working Party was an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor, and the European Commission. On 25th May 2018 it was succeeded by The European Data Protection Board.

consent is often an illusion.

Ms Lievens then concentrated on the principle of privacy by design and by default. The main element of it is that more responsibility is put on the data processor and not the data subject. The simplified version is that all data principles are built into the technology. She also said that there is still a long journey ahead as **user-friendly privacy by design** takes a lot of effort from many players. However, it is something that should go ahead as it might be one of the best ways to safeguard privacy.

Article 8 of GDPR:

"1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child."

Dr O'Connell said that it is hard for companies to grasp everything from an operational perspective. Having an **iterative process** teaches people to think about privacy by design, so companies need to design their products with that in mind. One legitimate reason for such an approach is the balance between the business and the data subject.

Mr Beverton also mentioned the current paradoxical situation where everybody knows about the GDPR but not much about what it actually entails. According to him, the important thing is that companies now think about ethical principles. He also stressed that it is much easier to conduct business when there are **clear principles** in place.

James Steyer – Common Sense Media

James Steyer is one of the most respected experts and entrepreneurs on issues related to children's media and education in the United States. He is the founder and CEO of Common Sense, the leading non-partisan organisation dedicated to improving media and technology choices for kids and families. He is also the founder and chairman of the Center for the Next Generation. Steyer is also an internationally known author, having written the widely acclaimed book Talking Back to Facebook in 2012, as well as another highly successful book, The Other Parent: The Inside Story of the Media's Effect on Our Children. Steyer is an award-winning faculty member at Stanford University, where he has taught for 26 years.

James Steyer from **Common Sense Media** entered the debate by saying that the industry is very resistant and that it is important to look at individual companies. When the Children's Online Privacy Protection Act was first introduced in the US, the big companies were strongly resistant to it. He was pleased when the GDPR was passed because it also significantly changed the situation in the USA. A similar, but less expansive, law has actually been passed in California for data protection. He believes that in general, people from the tech industry resist everything but that this dynamic was altered by the GDPR. He stressed that the regulators cannot count on people from the tech industry to think about the well-being of children so, in his opinion, the EU **needs to step up the pressure.**

Dr O'Connell added that the GDPR already has an effect, for example when it comes to online advertising in making companies think about data protection. There is no reason for the processes to be so difficult. She believes that companies interpreting the GDPR take it further because they still aim at collecting as much personal data from the users as possible. She thinks that we are only at the beginning and a lot of disputes will probably be battled in courts. According to her, the GDPR passes responsibility on to the data processors responsible with fines and reputational damage possibly changing the status quo.

MEDIA LITERACY

3 MEDIA LITERACY

The second part of the workshop focussed on media literacy and how audiovisual and social media impact the lives of children. James Steyer from **Common Sense Media** took the stage alongside renowned academic experts in this field, **Sonia Livingstone** and **Mary Aiken**, to inform this discussion.

Sonia Livingstone – London School of Economics and Political Science
Professor of Social Psychology in the Department of Media and Communications at LSE, she has published twenty books on media audiences, media literacy and media regulation, with a particular focus on the opportunities and risks of digital media use in the everyday lives of children and young people. Sonia has advised the UK government, European Commission, European Parliament, Council of Europe and other national and international organisations on children's rights, risks and safety in the digital age. She is currently writing her book, Parenting for a Digital Future – see www.parenting.digital and www.sonialivingstone.net

Sonia Livingstone from **the London School of Economics** started the session and spoke about potential harm to minors and media literacy from the perspective of a researcher. Her main area of expertise is content consumption at home and at school. She stressed the importance of noticing the number of influences to children and parents, not only from the media. In her opinion *"when we talk about children as "minors" they seem very abstract. So it is good to keep in mind that children are born pretty trusting and willing to rely on parents and school; they believe in fairness and expect systems to be responsive to them; most of all, they want agency to express themselves and to explore. If adults block and restrict them, they will become distrustful of adults. We should take all this into account when building systems to protect them."* Children have the right to provision and participation in the digital environment as well as protection, and balancing these rights in a proportionate and evidence-based manner is crucial. At present, the media are only partially supportive of children's rights and yet teach them many things, some pleasurable, some informative.

Professor Livingstone posed the question, **what is the evidence for harm and can media literacy be a solution to it?** She stressed that the body of research is multi-disciplinary and multi-method, yet contested and so further research is needed. The question of harm is one of the hardest to research (more so than media literacy). The main reason for this is that researchers cannot ask children detailed questions or expose them to harmful content for ethical reasons (especially in the case of research at scale). She stressed that children

access content across many platforms and also transfer content between them. Sometimes they want to explore, to transgress, and seek access to challenging content. In 2014, EU Kids Online quantified the risks of harm children can encounter online. The network is currently conducting a new pan-European survey.

EU Kids Online Network

EU Kids Online is a multinational research network. It seeks to enhance knowledge of European children's online opportunities, risks and safety. Work on this project began in 2006 and is now collecting new survey data on children's online risks and opportunities. Among the most important findings are the following:

1. *Online risks can be classified in terms of content, contact, conduct and contract*
2. *Some risks are increasing – for instance, exposure to online hate and content about self-harm*

For more information, visit www.eukidsonline.net

According to Professor Livingstone, people often wonder why the statistics regarding the number of children that come across harmful content are quite low, especially in comparison with news headlines, which are often exaggerated. She believes, however, that it is important to note **that some children live overall safer lives, but that some face considerable risk and regulators should decide which risks** are sufficiently concerning to call for measures to protect against them. Professor Livingstone highlighted that only a minority of children say that they have experienced cyberbullying and seen pornography, but they all know that people are bullied and that such content is available online if they wish to watch it. This too is a concern – that they live in a culture in which such risks are becoming normalised. Parents struggle to manage content so they often prefer to restrict the overall amount of time children spend online, meaning that any benefits of media and internet use are also restricted, and that children gain little guidance in finding beneficial content (or avoiding problematic content).

Professor Livingstone explained that harm itself can be divided into several types. Some things affect all children and others affect only some children, necessitating different approaches to regulation. Since there are many causes of harm to children, the media may be part of but rarely the sole cause of an individual child's harm due to the many other problems and potential sources of harm that have to be taken into account. For several weeks before the workshop, Professor Livingstone went to schools and talked about privacy and where the data go. Children knew about the GDPR and they also said that they had e-safety courses at school. She is intrigued how quickly the introduction of the GDPR informed the European

population that something is happening about regulation, that they have a choice. But do they? Too often, children feel they must "just say yes" or "lie about your age", anything to make the GDPR-related privacy information on their screen go away. She is worried that the introduction of age verification will be treated in the same way. **The introduction of regulation, if it doesn't present audiences with genuine choices and controls, will fail, and people will instead learn to work around or evade it.** Family members share devices and share their passwords, so it can be hard for the protection of minors' tools to function properly. Parents also do not know whom to turn to when they have a problem. There are also other problems: regulatory (Which authority should I turn to?) and educational (Where does media literacy fit in the school curriculum?). It does worry her that media literacy is thought of as a solution mainly when other forms of regulation have failed.

Professor Livingstone noted that the **European Audiovisual Observatory conducted a study** about media literacy in all 28 EU countries[5] and found out that it is often patchy, uneven, and ineffective. She thinks that there are real limits to what any of the policies can do. Furthermore, children have to be taught about what is going on behind the scenes, about algorithms, etc. At the same time the task of increasing media literacy has to be defined by what can be taught by real teachers, about systems that are changing. Professor Livingstone finished her presentation by highlighting the publication of a new recommendation by the Council of Europe titled *Guidelines to respect, protect and fulfil the rights of the child in the digital environment*[6] which offers member states a comprehensive approach to children's rights – including protection of minors - in relation to all media and online technologies.

EAO Media literacy mapping study results

- 939 MIL stakeholders identified (over two thirds with no statutory responsibility in MIL)
- 189 MIL networks identified
- More than a half of the projects focus either on "resources" or "end user engagement"
- Most prominent media literacy skills were "critical thinking" and "media use"
- Vast majority of the projects only of national importance (409) and only 43 European
- Most common target group remains "teens and older students", with "older people" in only 7 % of the projects (for the top projects)

5 Mapping of media literacy practices and actions in EU-28, European Audiovisual Observatory, Strasbourg, 2016, available online at https://rm.coe.int/media-literacy-mapping-report-en-final-pdf/1680783500.

6 Guidelines to respect, protect and fulfil the rights of the child in the digital environment, Council of Europe, Strasbourg, 2018, available online at https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a.

Mary Aiken – Cyberpsychologist

Dr Aiken is an Adjunct Associate Professor at the Geary Institute for Public Policy, University College Dublin and author of the book "The Cyber Effect," which was selected by the Times as a 2016 book of the year in the Thought Category, and 'best science pick' by Nature the International Journal of Science. She specialises in the impact of technology on human behaviour, and has written extensively on issues relating to the intersection between humankind and technology, or as she describes it "where humans and technology collide." Mary is an Academic Advisor (Psychology) to Europol's European Cyber Crime Centre (EC3), member of the EC3 Academic Advisory Board and member of the INTERPOL Specialists Group on Crimes against Children.

Mary Aiken is a cyberpsychologist whose main area of expertise is forensic cyberpsychology - the study of criminal, deviant and abnormal behaviour online. **Cyberpsychology, as she explained at the beginning of her presentation** is the study of the impact of technology on human behaviour, she quoted Norman (2008) who said "Cyberpsychology is the new psychology.[7]" She pointed out that what happens in the real world impacts cyberspace and vice versa. She argued that it is important to understand that human behaviour can change in technology mediated environments and once this premise is understood, it must be factored in when it comes to research, policy and regulatory initiatives.

Dr Aiken argued that there is now a paradigm shift in how we should conceptualise our relationship within the cyber ecosystem. In 2016 NATO declared cyberspace as a "domain of operations," noting that the battles of the future will take place on land, sea, air and on computer networks. Dr Aiken pointed out that this is one of the first official acknowledgements of cyberspace as a place, as an environment. She said that it is important to note that there is a time distortion effect in this space, she added that we should draw on the field of environmental psychology and apply learnings to the cyber environment in a developmental context.[8] She stated that she was very concerned about the Deep Web and Dark Nets especially as teenagers and children can easily find out how to access these domains, which, in real world terms, could be considered as "bad neighbourhoods." There exist many emerging and developing markets, where the majority of the population are not connected to the internet. Arguably when countries without full access to the internet acquire it, cybercrime is likely to increase.[9] However, she noted that future motive to engage in cybercrime may not just centre on profit, the phenomenon of global warming may result in catastrophic environmental and economic outcomes, which in turn may drive the incidence of cybercrime as a survival mechanism. Therefore, arguably we need to consider this potential future evolution not just as a criminal problem, but also as a social problem in terms of raising

7 *Norman, K. (2008) Cyberpsychology: An Introduction to Human-Computer Interaction Cambridge: Cambridge University Press*

8 *Life in Cyberspace https://www.eib.org/en/essays/life-in-cyberspace*

9 *LexisNexis 2018 Cybercrime Report https://www.threatmetrix.com/info/q2-2018-cybercrime-report/*

awareness and staging intervention. Dr Aiken highlighted that the protection of minors online is complex and multi-faceted, and must therefore be considered from different points of view. Interaction with technology is a continuous process from birth to adulthood, therefore we need to consider developmental aspects of the impact of technology on children alongside cyber environmental aspects, particularly as children are now growing up in cyberspace.

Additionally she said that we have to take into account the fact that **children are not one homogeneous group but vary in age range from pre-schoolers to teenagers.** Dr Aiken outlined three hypothetical groupings; Cyber Babies (0-3 years), Cyber Kids (4 to 12 years) and Cyber Teens (13+ years). She made the following points:

- Children now have a wide choice how and what to watch, on a range of platforms, apps and video-on-demand (VoD) services
- There has been a structural shift in the viewing habits of children from less live, scheduled television to more on-demand and online content. YouTube is now used by 45% of 3-4 year olds, 70% of 5-7s & 89% of 12-15-year-olds (Ofcom 2018)[10]
- Parents are concerned: children are consuming increasing amounts of unmoderated, unregulated, and potentially harmful content online

She stated that from a policy perspective we cannot work on the presumption that all parents are capable of guiding and protecting children online, citing an Ofcom (2014) study which found that one in ten parents of children aged 3 - 4 agreed their child knew more about the internet than they did, she argued that the state has a duty of care in this regard. When developing strategies on how to identify threats and risks to children online, her approach is to "start at the apocalypse and work back." When it comes to **Cyber Babies**, she said we should not just make recommendations for screen time for babies, but we must also factor in best practice for parent and caregiver screen time, along with emphasising the importance of eye contact with infants.

Cyber Babies - selected data

- Avoid digital media use in children younger than 18 months - American Academy of Pediatrics guidelines (AAP, 2016)
- Consider parent and caregiver use of devices (Radesky et al., 2014). Note: average phone checking; 200 times a day, and phone touching; 2,617 times a day (Dscout, 2016)
- More than two hours screen time a day could negatively impact children's cognitive development (Walsh et al., 2018)

10 *Ofcom Children and parents: Media use and attitudes report 2018 https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/Children-and-Parents-Media-Use-and-Attitudes-2018.pdf*

Dr Aiken highlighted the latest research which found that more than **two hours screen-time** a day could be detrimental in terms of a child's cognitive development (Walsh et al., 2018).[11] She said that **Cyber Kids** (4 to 12) are a particularly vulnerable age group due to their increasing engagement online, and yet their relative immaturity. Dr Aiken emphasised that she was particularly concerned about children's exposure to legal but age-appropriate content online, such as extreme violence, pornography and self-harm content.[12] She said that there has been a rise in the online sexual coercion and extortion of children. Cybercriminal groups have emerged that have a commercial interest in exploiting children, Europol has reported that children as young as seven are now being targeted.[13] She highlighted the problem of young children being trolled online by graphic and explicit content embedded in their cartoons available on-demand, she referenced research that has described trolling as a "manifestation of everyday sadism.[14]"

Cyber Kids - selected data

- Legal but age-inappropriate extreme content online: Extreme violence, self-harm, pornography and hate speech
- Rise in sextortion (Europol, 2017)
- Grooming & child abuse material (Europol, 2018)
- Child-on-child sexual assaults "peer on peer" abuse 71% increase
- Anxiety and depression in young people have risen 70% in the last 25 years (Royal Society for Public Health, 2017)

She discussed 2017 UK police reports that child-on-child sexual assaults had increased by 71% since 2013, and stated that in her opinion this increase may be related to the widespread availability of pornography online. She said the most important question to be addressed was one of accountability; Who is responsible when children are exposed to distressing and age-inappropriate content online? She said that at the moment there exists a 'diffusion of responsibility' in cyber contexts; device, ISP, social technologies, content generator, search, and so forth. She argued that whenever a young child is exposed to extreme or traumatising content this arguably manifests as a collective responsibility for the abuse of a child.

She said that, while some may consider that a 'hierarchy of harm' could be created in terms of levels of seriousness, Dr Aiken stated that from her perspective she has a zero tolerance

11 *Associations between 24 hour movement behaviours and global cognition in US children: a cross-sectional observational study https://www.thelancet.com/journals/lanchi/article/PIIS2352-4642(18)30278-5/fulltext*

12 *O'Neill et al. (2014): Report of the Internet Content Governance Advisory Group. Department of Communications, Energy and Natural Resources, Ireland*

13 *Europol online sexual coercion and extortion of children https://www.europol.europa.eu/crimeareas-and-trends/crime-areas/child-sexual-exploitation/online-sexual-coercion-and-extortion-of children*

14 *Buckels, E., Trapnell., P & Paulhus., D (2014) Trolls just want to have fun, Personality and Individual Differences, Volume 67, 2014, Pages 97-102, ISSN 0191-8869, https://doi.org/10.1016/j.paid.2014.01.016.*

position regarding the deliberate harm of a child. She maintains that the point at which we as a society start to think that this is acceptable is the point at which we need to think again. In her opinion, we are living in the largest unregulated social experiment of all time. If children can access extreme content online, they can be harmed by it. This is why we need to think about transparency and accountability. She asked; If the algorithms that underlie search lead a child to a self-harm web site - who is responsible? Who is accountable? Dr Aiken said that we cannot wait for longitudinal studies to prove that there is causation or even correlation between children accessing extreme and age inappropriate content and harm. In the absence of evidence, or in terms of ethical restrictions an inability to conduct research in an area, she stated that a mixture of expert opinion and common sense must prevail.

She said that when it comes to **Cyber Teens**, the evidence of harmful effects of social technologies on their well-being is mounting. These effects include sleeplessness, obesity, compulsive use, and vulnerability to advertising. Sleep deprivation increases the likelihood that teens will suffer a myriad of negative consequences, including the inability to concentrate, poor grades, anxiety, depression, and suicidal ideation.[15] The vast majority of teens (90%) believe online harassment is a problem that affects people their age, and 63% say this is a major problem that teachers, social media companies and politicians are failing to address.[16]

Cyber Teens - selected data

- Evidence is mounting regarding harmful effects of social technologies on the well-being of children (Aiken & O' Sullivan, 2018)
- NHS stats: sleep disorder admissions for under-16s almost 10,000 last year (Marsh, 2018)
- Increases in self-harm and eating disorders (Pollack, 2017)
- Cyberbullying: vast majority of teens (90%) believe online harassment is a problem that affects people their age, and 63% say this is a major problem and believe that teachers, social media companies and politicians are failing to address (Pew, 2018)
- Cyber Juvenile Delinquency (Aiken et al. 2016)
- Fake news: teens now questioning the credibility and value of traditional media

According to Dr Aiken it is **important to avoid** conflation – smartphones, social media, the internet, technology, virtual reality are all related, but are different. She points out that technology is not the same thing as the internet; that children can have meaningful engagement with technology at an early age on air gapped devices, that is, devices that are not connected to the Internet.

Dr Aiken ended by proposing several **recommendations**. These included investigating the impact of technology on human behaviour, factoring in cyberspace as an environment,

15 *Aiken&O'Sullivan,2018https://data.oireachtas.ie/ie/oireachtas/committee/dail/32/joint_committee_on_children_and_youth_affairs/submissions/2018/2018-02-13_opening-statement-professor-barry-o- sullivan-mria-and-adj-assoc-professor-mary-aiken_en.pdf*

16 *Pew (2018) A Majority of Teens Have Experienced Some Form of Cyberbullying, available online at http://www.pewinternet.org/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying.*

formulating stages of 'cyber cognitive development' to inform age verification protocols, and consolidating EU-wide initiatives regarding best practice. Additionally, factoring in future evolutions such as Artificial Intelligence and Virtual Reality, creating research protocols for the continuous investigation and modelling of the impact of media on the developing child, developing educational awareness initiatives, and formulating protocols and regulatory tools where appropriate, to hold technology companies accountable.

James Steyer from **Common Sense Media** presented the work carried out in the USA. As a long time educator he believes in the importance of education of children at schools, with a focus on media literacy and the impacts of social media. He thinks that the EU should lead the charge when it comes to regulating platforms because there is no will to do it in the USA. However, if the EU provides the regulation, the USA will follow, as was the case with the GDPR. According to him the biggest companies like Google or Facebook try to avoid regulation but it is important to hold them accountable. Mr Steyer also described all the extensive activities of Common Sense Media in the USA (library of independent age-based and educational ratings, awareness campaigns, etc.). He highlighted all the resources that are freely available.

Common Sense Media

Common Sense Media is the leading non-partisan organisation dedicated to improving media and technology choices for kids and families in the USA. They try to empower parents, teachers, and policymakers by providing unbiased information, trusted advice, and innovative tools to help them harness the power of media and technology as a positive force in all kids' lives. They offer the largest library of independent age-based and educational ratings and reviews for movies, games, apps, TV shows, websites, books, and music in US. Through "Parent Concerns" and "Parent Blog" they help families navigate the problems and possibilities of raising children in the digital age. Through "Common Sense Education" they provide digital literacy and citizenship programs to educators and school communities. They offer a range of free resources include ratings and reviews of digital tools, a comprehensive Digital Citizenship Curriculum, ready-made lesson plans, videos, webinars, and more. At the same time they act as an advocacy group.

CONTENT RATING AND OVERSIGHT

4 CONTENT RATING AND OVERSIGHT

Lubos Kuklis – chair of ERGA

Mr Kuklis studied at the Law Faculty of Comenius University in Bratislava, where he also obtained a PhD in Administrative law. Since 2006 he has been a chief executive at the Council for Broadcasting and Retransmission of Slovakia. He is the Council's representative in European Regulators Group for Audiovisual Media Services (ERGA), where he serves as Chair and has also led ERGA's Subgroup on Protection of Minors that examined systems for the protection of minors in EU media environment.

Lubos Kuklis, the chair of **ERGA**, asked the guests about their opinion on content rating: what is the future of content rating? Professor Livingstone said that parents want it. With content rating in place, parents are able to create their own social norms and decide what programmes their children will watch.

Mr Steyer believes that EU countries should bring Common Sense Media to their countries because they perfected the content rating and it works in the USA. Distribution companies need to make it available and parents will then make their own decisions. He said that the MPAA rating system still exists in the USA but that the public use Common Sense Media as it allows them to learn about the kind of content which is present in the audiovisual works. In a way, it is like nutritional labelling. Cultural sensitivities have to be taken into account but people really want to know the specifics. They are currently working with the British Board of Film Classification (BBFC) to adjust their age rating in the future to fit the sensitivities of people in the UK. In his opinion, YouTube poses a major challenge in many aspects. For example, even ad companies can take serious issue when their ads are placed next to questionable content that appears driven by YouTube's algorithms.

Article 6a (3) - AVMSD

"(3)Member States shall ensure that media service providers provide sufficient information to viewers about content which may impair the physical, mental or moral development of minors. For this purpose, media service providers shall use a system describing the potentially harmful nature of the content of an audiovisual media service.

For the implementation of this paragraph, Member States shall encourage the use of co-regulation as provided for in Article 4a(1)."

Professor Livingstone asked about the regulators' approach in this area. **Mr Kuklis** said that there is a functional age rating system in almost every EU member state, but it is different in each country. In his opinion there are two possible approaches currently being explored in this regard. One could be legal harmonisation and the other is the technical interoperability of existing systems. In this context he highlighted pilot initiatives, for example the project **Miracle.** He believes that it is important to discuss this and look at the possible solutions. It might be possible that content ratings could be the same for all platforms. Even the tech companies said that any solution has to be technical. Dr Aiken remarked in this regard that there is no AI technology that can screen and moderate all user generated video content in real time. Mr Steyer said that it has to exist across all platforms, with the necessity to blend AI with a human perspective. He also said that although it is metadata, people have started to look at it and he believes that there is going to be a solution in the upcoming years.

Marcel Boulogne - European Commission

Mr Boulogne is a long standing policy expert of the European Commission in the audiovisual field. He is the Head of Sector for 'Audiovisual Media Services' (Converging Media and Content) at DG CNECT. For more than 15 years he has been responsible for the Audiovisual Media Services Directive and its various revisions. Before that he was working for the Office of Harmonisation for the Internal Market, now EUIPO.

Marcel Boulogne, head of sector for AVMSD at the **European Commission**, said that long before the revision of the AVMSD, in 2003, the commission called for an independent study on rating practices. On the basis of this study and the experience gathered over the years, taking into account various national sensitivities, the commission did not consider harmonisation of rating practices as a way forward. According to the amended AVMSD, audiovisual media providers will have to describe the harmful nature of the content, for instance by using descriptors and VSPs will have to offer systems to allow users to self-rate the content. There was a pilot project called **You Rate It** based on the principle of one simple tool enabling viewers and uploaders of user-generated video to rate their own content and provide age rating and information 'translated' into the systems used in the different member states. It is based on a simple questionnaire so users can quite easily rate the content. Technical possibilities are included and since there is now an obligation to put it into place, there is pressure to do something concrete. However, the amount of content uploaded to a platform like YouTube every day will make it difficult to rate each and every piece of content.

You Rate It

The "You Rate It" system was created jointly by the British Board of Film Classification (BBFC) and Netherlands Institute for the Classification of Audio-visual Media (NICAM) and serves for rating user-generated content, thus enabling parents and children to make well-informed viewing decisions on VSPs. It is a simple rating tool based on the same principles as for classifying "professional" content. Ratings can be given by the uploader of the video, by the user, or both. National sensitivities are also taken into account. There are 6 different categories of content. The classification shown for the video (in the form of nationally recognizable rating) is based on the geolocation of the viewer. Ratings can be used by websites, apps, parental controls and search engines.

In **Dr Aiken's** opinion, self-rating of content is not the solution to the problem – she explained that sadistic trolls who covertly embed extreme content in children's cartoons will certainly not flag it up. On the other hand, she does not accept the big data argument that there is simply too much content to check everything. She said that we would not accept such an argument from a TV broadcaster or a newspaper publisher, so therefore this argument should not be accepted regarding online media. She said we have to look at these problems and ask if these technology companies are now big enough to fail? She said that we the experts, and the policymakers may be held accountable because we did not act, and that this is "happening on our watch." Dr. Aiken maintained that in terms of age verification and child protection online we need a combination of software and hardware solutions embedded into devices. She said that it was disturbing to think of young children accessing content online unsupervised, and that parents should make every effort to prevent their children from being exposed to a harmful content.

Miracle Project

A project that aims to overcome the fragmentation of existing systems for the protection of minors. The project is built around the idea of sharing data (for example individual classifications), so that there is no need for different systems, as parental software could easily read the metadata and either block or play the video. It can be processed by every media and platform. At the same time this could improve the user experience.

Regarding the scale of some companies, Mr Mount from Ofcom stated that he agrees with the fact that various comments of the type "nothing can be done" do not constitute an excuse. At the same time, the scale of online content is so big that it is hard to check it all. This can be solved by delaying the uploading of the content. It is not as simple as platforms doing more.

Mr Kuklis said that YouTube has a safe mode that does not allow children to watch unrated content. He believes that if something like this was turned on default, it could help.

Mr Steyer said that we will get a blend of a public private solutions in the end. Companies are scared of the EU regulating them. EU can impose the need for it and then force them to figure it out like they did with GDPR which helped everybody. He believes that platform accountability is a huge issue that needs to be addressed. If there is legislation in the EU, the USA will follow. In his opinion, the tech companies will benefit as well. He also stressed that there is a current lack of trust in the industry.

Anna Herold - European Commission

Ms Herold is the Head of Unit of the Audiovisual and Media Policy unit, which oversaw the revision process of the AVMSD and will also follow the transposition process. Besides several positions at the DG CNECT in the audiovisual and telecoms area, she has been also a Member of Cabinet of Günther H. Oettinger

Anna Herold, Head of Unit of the Audiovisual and Media Policy unit at the **European Commission** said that there will soon be legislation in the EU that will go a certain way towards 'platform accountability'. As AVMSD comes into force, VSPs will be required to exercise a duty of care for protecting minors against harmful audiovisual content available on their services. In particular, VSPs will now need to put measures in place to ensure that minors do not normally access such harmful content. Ms Herold stressed that this duty of care is a reflection of the increasing popularity that VSPs are gaining, especially among younger users, as a means to access audiovisual content online. Even though certain big players are already making some progress on this field, the new AVMSD rules will constitute a regulatory backstop and subject their behaviour regarding protection of minors to the scrutiny of the competent national regulator. Ms Herold also wondered about ways to address the potential problem of content moderators who may get exposed to very emotionally challenging content online; as in content regulation, human oversight will remain to be necessary at one point in the control chain.

Dr Aiken said that many experienced police analysts have been disturbed or traumatised by viewing extreme content online, particularly child abuse material. She said that there were increasing reports of young adults being hired by social technology companies (or their agents) in countries such as the Philippines to work all day, viewing the worst excesses of the Internet (from child abuse material to extreme violence). She said she was aware of some conversations regarding harm and potential class/group actions. She stated that in time she believed that the role of content moderator would be considered as a human rights issue, in the same way as human trafficking or forced labour – she argued that doubling moderators was not a solution, as it arguably doubles the harm to those who are being used as human filters. She said that when building and running a social technology platform unintended consequences must be considered and addressed. She predicted that in ten years' time there will be new social tech models, a completely different landscape.

CHILDREN'S MEDIA CONSUMPTION – NATIONAL CASE STUDIES

5 CHILDREN'S MEDIA CONSUMPTION – NATIONAL CASE STUDIES

During the workshop, representatives of **BAI** (Broadcast Authority of Ireland) and **Ofcom** (Broadcast Authority of the UK) presented the results of recent studies conducted in Ireland and the UK.

Ciarán Kissane – BAI

Mr Kissane is a Senior Manager with the Broadcasting Authority of Ireland. One of his areas of responsibility is the operation of the Broadcast Fund which comprises 7% of the TV licence fee (approx. €14m per annum). Ciarán is a graduate of Dublin City University and the Open University. He holds a Doctorate in Education and is an avid scuba diver.

Ciarán Kissane from **BAI** brought to the table his own experiences when raising children. Social media are increasingly becoming a cause of stress for children. The sense of the damage that social media are causing is not new. The Irish government published an action plan in the summer of 2018 which includes 25 specific actions to be progressed over the coming 18 months.[17] One of the real challenges is bringing the public on board with you. In Ireland, the digital age of consent is 16. However, it is undeniable that young children have a familiarity with social media and various devices.

Mr Kissane then presented figures from the Cybersafe Ireland Annual Report 2017[18] focussing on children aged 8 to 13. The figures showed that **most of the children over the age of 10 own a smartphone**. The number of children owning smartphone at the age of 13 reaches 90%. Overall, nearly 75% of these children use social media and messaging apps.

Cybersafe 2017 – Report highlights

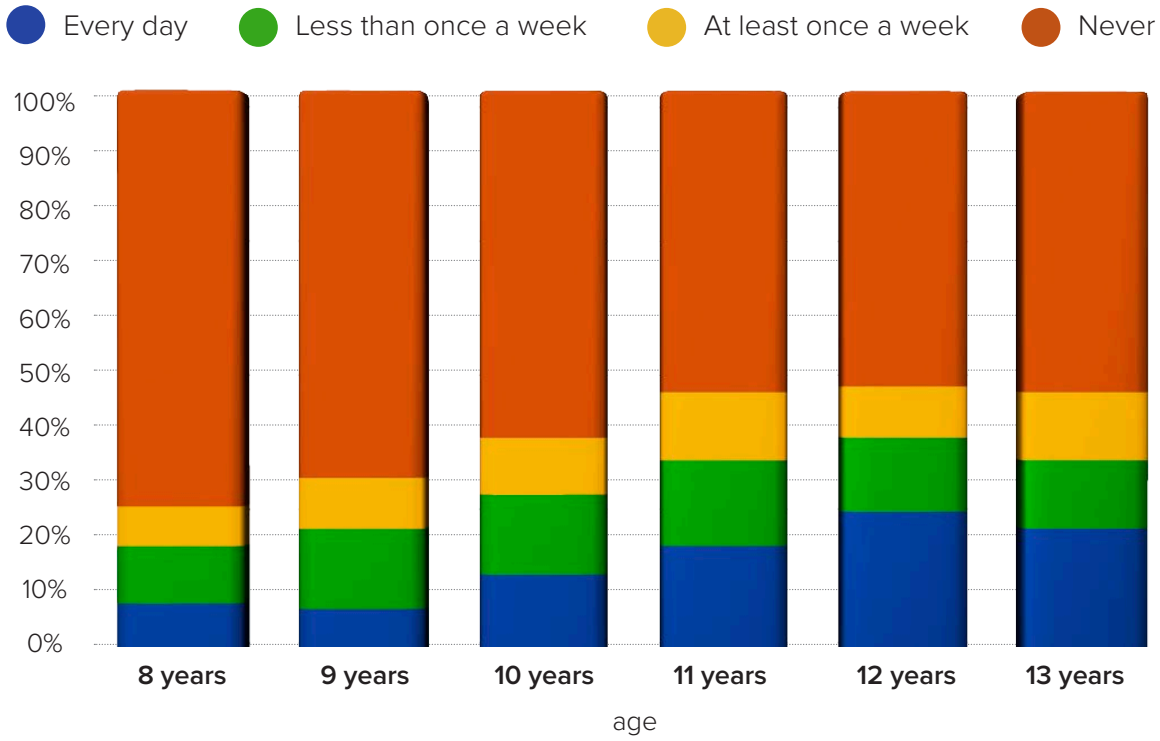
- 68% of 8 – 13-year-olds own their own smartphone
- 70% of 8 - 13-year-olds use social media
- 13% of children spend 4+ hours online including almost 20% of 12-year-olds and 10% of 8-year-olds
- 32% of children talk to strangers online every week (18% every day)
- 30% of children rarely or never talk to their parents about online safety
- Snapchat remains the most popular app for children aged between 8 and 13 with 47% of children on it overall, followed by Instagram (36%) and WhatsApp (33%)
- 33% of children have played over-18 games with significantly more boys (53%) playing them than girls (13%). 41% of 8 & 9-year-old boys have played over-18 games
- The majority of teachers (62%) deal with online safety incidences in the classroom with 35% dealing with between 2 and 5 incidences in the last year

17 *http://www.internetsafety.ie/en/IS/7082532-ONLINE%20SAFETY%20ACTION%20PLAN%202018-2019.pdf/Files/7082532-ONLINE%20SAFETY%20ACTION%20PLAN%202018-2019.pdf*

18 *https://cybersafeireland.org/media/1183/csi_annual_report_2017-final.pdf*

The worrying thing is that **children often talk to strangers online**. The number of children gradually increases with age and almost 50% of children aged 11 and more had talked to strangers at least once, usually once a week or even every day. When it comes to playing games which are rated as unsuitable for children under 18 years of age, more than a half of male children confessed to playing such games.

Children Talking to Strangers Online by Age



Children Talking to Strangers Online by Age, Source Cybersafe Ireland Annual Report 2017, BAI

Dan Mount – Ofcom

Mr Mount is a Senior Associate, Strategy & Policy at Ofcom UK, where he is leading public policy and regulatory development projects of strategic significance to Ofcom and representing Ofcom's position on key policy issues to external industry and public stakeholders. In the past he was the Head of Policy and Public Affairs for an independent consultancy Civic Agenda EU. Before that he served as a Deputy Secretary-General for the Digital Policy Alliance.

Dan Mount from Ofcom presented the results of a study carried out on children's media use and attitudes.[19] **More children than ever are going online**. There is especially an increase in 3-4-year-olds and 5-7-year-olds. In 2005 older children estimated they were spending just over an hour a day online. In 2017 this has increased to nearly three hours a day. Parents estimate that even the youngest children are spending over an hour a day online. More and more children from all age groups now own a tablet. The distribution of ownership of mobile phones has not changed significantly, however the majority of children aged 12-15 now own smartphones which have far greater online functionality than the previous generation of mobile phones. Smartphone ownership rises particularly sharply among children between 9 and 11 years of age.

19 *https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-parents-2017*

Media lives by age: a snapshot

3-4s

1% have their own srnartphone, **21%** have their own tablet
96% watch TV on a TV set, for around **15h a week**
41% watch TV on other devices, mostly on a tablet
40% play games, for nearly **6h a week**
53% go online, for nearly **8h a week**
71% of these mostly use a tablet to go online
48% use YouTube, of which 52% of these say cartoons are their favourite thing to watch, 15% say unboxing videos
0% have a social media profile

5-7s

5% have their own smartphone, **35%** have their own tablet
95% watch TV on a TV set, for around **13½h a week**
49% watch TV on other devices, mostly on a tablet
66% play games, for nearly **7½h a week**
79% go online, for around **9h a week**
63% of these mostly use a tablet to go online
71% use YouTube, of which 30% say cartoons are their favourite thing to watch, 18% say funny videos or pranks
3% have a social media profile
The **TV set** is the device they say they would miss the most

8-11s

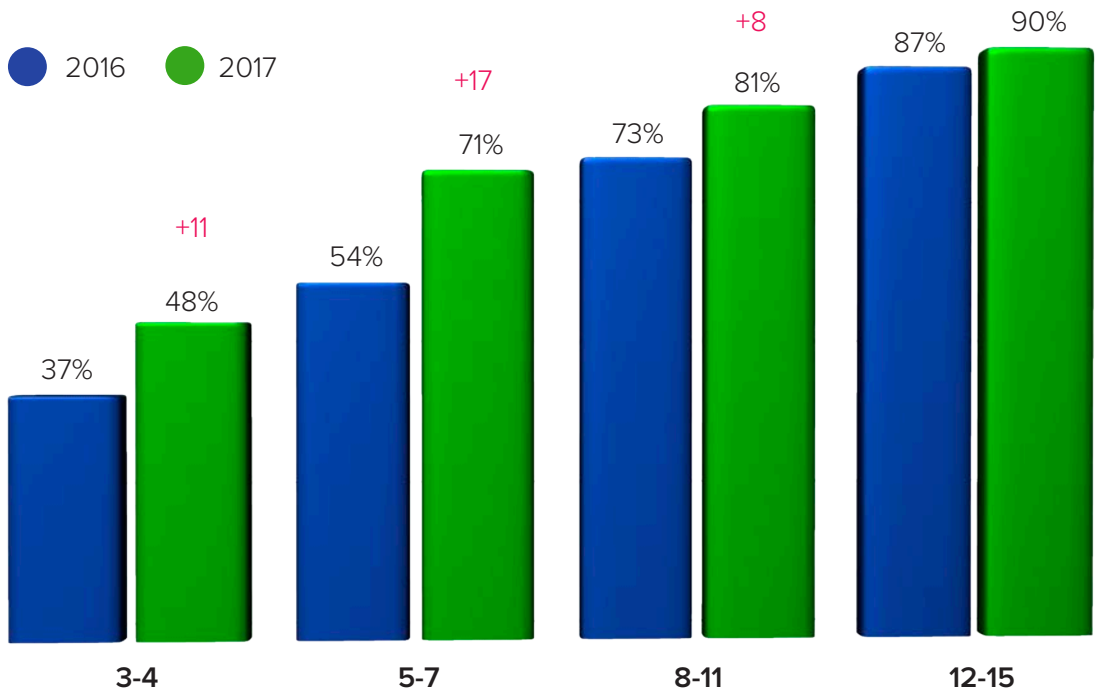
39% have their own smanphone, **52%** have their own tablet
95% watch TV on a TV, set, for nearly **14h a week**
55% watch TV on other devices, mostly on a tablet
81% play games, for around **10h a week**
94% go online, for nearly **13½h a week**
46% of these mostly use a tablet to go online, **22%** a mobile
81% use YouTube, of which 23% say funny videos or pranks are their favourite thing to watch, 18% say music videos
23% have a social media profile
The TV so or **tablet** are the devices they would miss the most

12-15s

83% have their own smartphone, **55%** have their own tablet
91% watch TV on a TV set, for nearly **10½h a week**
68% watch TV other devices, mostly a tablet or mobile
77% play games, for around **12h a week**
99% go online, for nearly **21h a week**
49% of these mostly use a tablet to go online, **26%** mostly use a mobile
90% use YouTube, of whitch 26% say music videos are their favourite thing to watch, 23% say funny videos or pranks
74% have a social media profile
Their **mobile phone** are the device they would miss the most

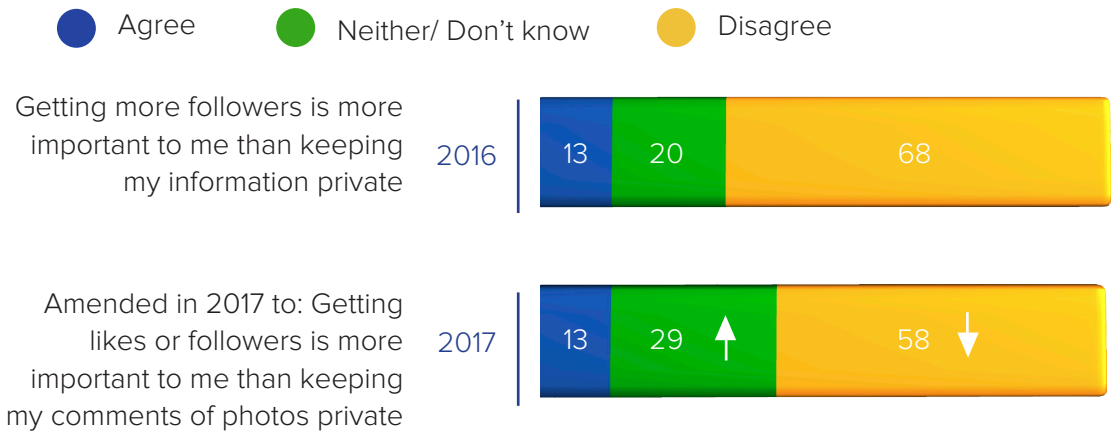
Media lives by age, Children and Parents: Media Use and Attitudes Report 2017, OFCOM

There has been a **significant increase in the number of children using YouTube**, particularly among children between 3 and 11 years of age. 48% of children aged 3-4 use only the YouTube Kids app. 87% of children aged between 12 and 15 years have a social media profile. Fewer say that Facebook is their main site, while the numbers who say Snapchat have increased. At the same time most parents are not aware of the minimum age requirements for different social media services, particularly in the case of newer platforms like Snapchat.



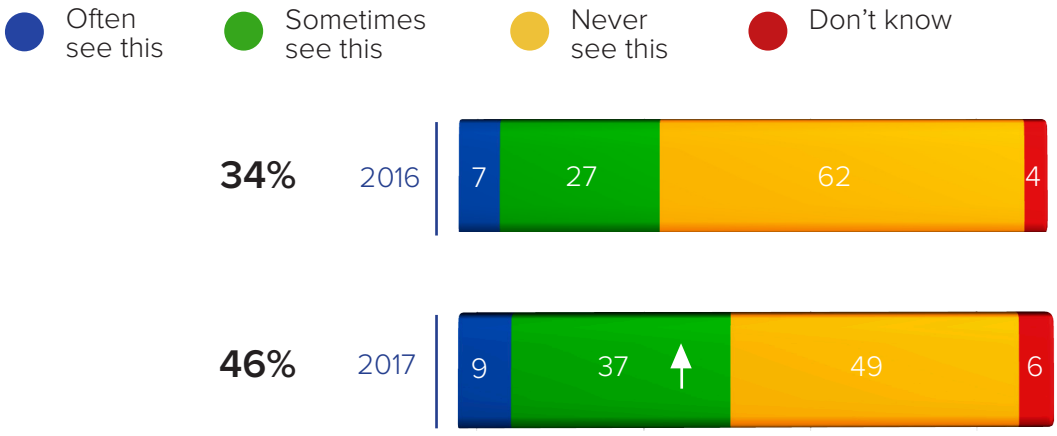
Growth in the number of children using YouTube, Children and Parents: Media Use and Attitudes Report 2017, OFCOM

Some social media services like Snapchat have a kind of **social pressure** built in which prompts children to send daily pictures (Snaps) and highlights lopsided interactions or competition of attention between friends. While the number of children who experience targeted, ongoing bullying is relatively small, the number who feel under pressure to be popular (and to look or act a certain way to ensure that) is much higher. Three quarters of 12- to 15-year-olds who use social media say there is a pressure to look popular and 13% of them feel this all the time. Eight out of 10 children say people act unkindly to each other on social media and one in ten feels this all the time. This suggests that while many children seem to be effectively navigating the social media landscape without high levels of distress, a small proportion of children are having a consistently tough time online.



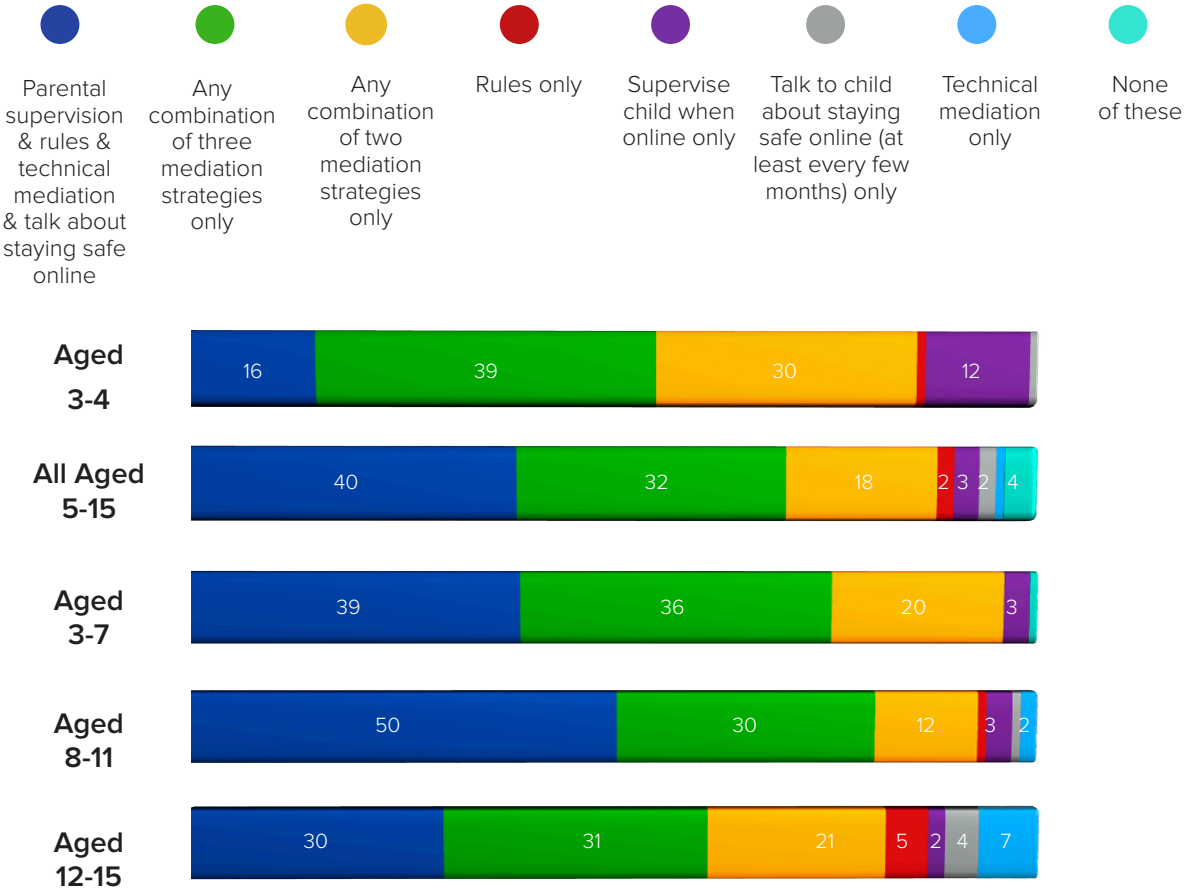
Value of privacy for children, Children and Parents: Media Use and Attitudes Report 2017, OFCOM

The number of children aged between 12 and 15 years that report being **bullied online** (12%) is the same as those that say they have been bullied face to face. However, it is possible that this number is not accurate due to the fact that children put so much importance on being seen to be popular on social media, leading to a tendency to dismiss even quite nasty behaviour as 'banter'. Nearly half of 12- to 15-year-olds have seen hate speech in the last year with some taking action against it, although most are likely to ignore such content. Almost all children participating in Ofcom's research say they have been given information about how to stay safe online. This information came mostly from parents and teachers. 27% children said they find it hard to control their screen time and 72% think there should be rules about what people can say online so that people cannot say hurtful things about others.



How often did 12-15-year-olds see hate speech in the last year?, Children and Parents: Media Use and Attitudes Report 2017, OFCOM

Parents use several approaches to keep children safe online. These approaches include technical mediation, speaking with the child about staying safe online and supervising the child when online. The number of parents using content filters and being aware of them is increasing. However, fewer parents are aware of or use technical controls on phones and tablets (for example to stop apps being downloaded, stop in-app purchases, etc.). Most parents who use network level filters find them useful and feel that they block the right amount of content and that their children cannot get around them. Parents who were aware of the technical tools but did not use them usually said that they do not use these tools because they prefer to talk to their child and use other methods of mediation as they trust their child to be responsible. Some parents also said that their child is always supervised when online.



Combinations of online mediation strategies used by parents of 5-15s whose child goes online: 2017, Children and Parents: Media Use and Attitudes Report 2017, OFCOM

CONCLUDING WORDS

Giuseppe Abbamonte – European Commission

Mr Abbamonte was appointed Director of Media Policy at the Directorate-General for Communications Networks, Content and Technology in January 2014. The Directorate is, amongst many other things, responsible for the European regulatory framework on audiovisual media. In his former positions, he was the head of the electronic communications policy unit and then of the cybersecurity and on-line privacy unit. He also has extensive experience in complex merger cases and in consumer law. He is the author of several publications mainly in English law magazines.

To conclude the workshop, attendees were addressed by **Giuseppe Abbamonte**, Director of Media Policy at the **European Commission**. Mr Abbamonte explained that the issue of internet platforms' responsibility was cross-cutting and relevant in many fields, ranging from copyright to the protection of users, notably children. He noted that the AVMSD aimed to specify the duty of care of the platforms, and that many systems to prevent children from watching harmful content had already been put in place. Mr Abbamonte stressed that the revised directive encouraged the protection of minors on VSPs to be tackled through co-regulation. He also highlighted the importance of media literacy, particularly in the context of the fight against disinformation, on which a code of practice had recently been agreed by online platforms and the advertising industry. The code contained important commitments which aimed in particular to disrupt the revenues of the purveyors of disinformation. He also pointed to the "Better Internet for Kids" strategy, which aimed to create a safe online environment for children. Finally, Mr Abbamonte stressed the reinforced role of ERGA under the revised AVMSD, particularly in providing technical expertise to the commission and ensuring consistent implementation of the directive.

WHAT'S NEXT

Protecting children in the media environment is one of the most important tasks for all ERGA members. However, this environment is changing so rapidly that, to be able to fulfil it effectively, regulators need up-to-date information on the functionality of the environment itself and the latest research on its impact on children. This was the idea behind organising an event where ERGA members could debate the latest developments with distinguished experts in the field. And now, after two successful editions, ERGA is considering **organising the next one in 2019.**


ERGA
European Regulators Group for Audiovisual
Media Services