Report on the proceedings of the

Safer Internet Forum 2017

23 November 2017 Brussels, Belgium

(including annexes on the preceding European Youth Panel and Teacher Panel)



Further information from the Forum, including the full agenda, conference brochure with speaker biographies, and presentations can be found at www.betterinternetforkids.eu/sif2017.

Contents

Introduction	3
Welcome and high-level opening by the European Commission	4
The Alliance to better protect minors online	6
Children and robotic toys	12
Parallel session A1: Should age determine how we experience the internet? Tensions between protection and participation	18
Parallel session A2: Child sexual abuse images – the tip of the iceberg?	22
Building resilience with vulnerable groups	24
Close of Safer Internet Forum 2017	27
Annex I: European Youth Panel	28
Annex II: Teacher Panel	30

Introduction

The 14th edition of the Safer Internet Forum (SIF) took place in Brussels, Belgium on 23 November 2017 with a theme of "From children's tech to resilient youth – how to foster wellbeing online". More than 230 stakeholders in the field of child online safety from some 39 countries worldwide were in attendance to discuss the latest trends, risks and solutions related to youth online safety and empowerment.

On the previous day, 15 youth panellists from 13 European countries also met in Brussels at the European Youth Panel (YEP), an annual event which precedes SIF. The young people were selected from their national youth panels to represent their peers, share their ideas and work collaboratively on a new youth-led campaign. They also actively participated in SIF on the following day, launching their #TogetherForRespect initiative and accompanying video, and contributing to high-level panel discussions.

In parallel with the Youth Panel, a Teacher Panel also met, bringing together seven teachers from the eSafety group of the eTwinning network to discuss some of the challenges facing children and young people when they go online, and to share best practices from different schools and countries. The teachers also participated in SIF the following day.

Participants at the Safer Internet Forum therefore included young people, parents, teachers and educators, industry and government policy makers, technological and awareness-raising experts, and political, educational and social leaders from Europe and beyond.

In line with the Forum theme of fostering wellbeing online, the event included a number of diverse presentations and discussions, ranging from the challenges of the emergence of the internet of toys on children and young people; how we can balance the need for some managed risk to develop resilience against the concerns about exposure to inappropriate or harmful content, contact or conduct online; the scale of the challenge being faced in tackling child sexual abuse material (CSAM) online; and particular considerations for supporting vulnerable groups online. Additionally, a session hosted by the self-regulatory *Alliance to better protect minors online* allowed participants to hear about some of the approaches industry are taking to keeping their users safe on their services and platforms, with the youth panellists equally responding with their views as key benefactors of such initiatives.

The Safer Internet Forum is organised and funded by the European Commission with the assistance of the Insafe-INHOPE network of Safer Internet Centres (SICs) in Europe, under the Connecting Europe Facility (CEF) programme as part of the <u>European Strategy for a Better Internet for Children</u>. The strategy supports projects and events to help create a safer and more positive online environment for children and young people, as well as to promote industry self-regulation and international co-operation.

Find out more at www.betterinternetforkids.eu.

Welcome and high-level opening by the European Commission

Opening address: Claire Bury, Deputy-Director General, DG CONNECT

Participants were welcomed to the 14th annual edition of the Safer Internet Forum (SIF) by the Deputy-Director General of the European Commission's DG CONNECT. In her opening address, **Claire Bury** referred to the current state of play with regards to digital policies addressing our society, from the youngest to the most experienced internet users. She went on to refer to the new <u>Commissioner for Digital Economy and Society, Mariya Gabriel</u>, as being a good digital role-model to drive forward this agenda, having an interest in the social aspects of digital policy, concerned about how technology impacts people's lives, and being keen to work collaboratively to make the internet a better place.



Claire Bury, Deputy-Director General, DG CONNECT, European Commission, welcomed participants to the 2017 edition of the Safer Internet Forum.

This support coming from the Commissioner can act as an incentive for various ongoing legislative frameworks and reforms (such as data protection and audiovisual media services) and, at the same time, highlight the work undertaken by Insafe and INHOPE, and Safer Internet Centres across Europe, under the Better Internet for Kids (BIK) programme of work. Claire Bury went on to illustrate how, in the past year, the Insafe network has been keeping pace with the latest developments and trends in the online world such as fake news, the Blue Whale Challenge (BWC), data protection and youth participation. Working in synergy with the awareness raising and helpline services provided by Insafe, the INHOPE network of internet hotlines received 9.3 million reports on child sexual abuse material (CSAM) globally and, thanks to the hotline's work, 70 per cent of the content was subsequently removed within three working days.

Turning to the work of the *Alliance to better protect minors online*, Claire Bury described how, on the occasion of Safer Internet Day 2017, the European Commission had brought together media and ICT companies, and civil society organisations, to tackle risks online such as harmful content, contact and behaviour. The *Alliance* has embarked on a series of actions since, most recently involved in an ongoing <u>public consultation on fake news and online disinformation</u> (open until February 2018), and in an exercise to build a <u>High-Level</u>

Group on Fake News which will hold its inaugural meeting in January 2018.

Claire Bury concluded her welcome address by reflecting on the fact that, as children and young people are increasingly likely to consume more media content than traditional broadcasting, joint initiatives to enhance media literacy and critical thinking require attention. Against this background, she announced that the European Commission will launch a campaign around cyber culture on the next edition of <u>Safer Internet Day</u>, taking place on Tuesday, 6 February 2018.

The Alliance to better protect minors online

Chair: Claire Bury, Deputy-Director General, DG CONNECT

Panellists: Industry and civil society representatives from the *Alliance* and youth panellists

Following on from the welcome address, the first session of Safer Internet Forum 2017 placed a focus on the work of the *Alliance to better protect minors online*, with various stakeholders taking to the stage including industry representatives from Google and Telia, COFACE Families Europe (a pluralistic network of civil society associations representing the interests of all families) and two youth panellists.



Remit and membership of the Alliance to better protect minors online.

In chairing this session, **Claire Bury** began by outlining the remit and membership of the *Alliance*. She went on to ask the industry representatives to elaborate on the *Alliance's* objectives and processes, giving concrete examples where possible.

Marco Pancini (Google) referred to recent Google developments in terms of better protecting minors online, such as a new tool for cyber-content to offer parents and carers the opportunity to interact with their children in a safe online experience. More specifically, this tool - currently being piloted in the US and Ireland - will facilitate a shared account for parents and their children, aiming to allow parents to introduce kids to online experiences with both full control and shared responsibility. He went on to emphasise that this tool has been developed by Google engineers (who themselves are parents), back to back with a Google outreach programme with child associations and organisations around the world from which they collect feedback.

On a similar note, **Anna Augustson** (Telia) referred to recent developments at Telia working with youth panellists (in Finland and Denmark), local NGOs and schools in co-created workshops, emphasising that the most surprising insight has been that children are already well aware of who needs to be concerned in better internet initiatives. Social activities

offered by Telia include teaching kids how to code and talking about safety online. There has been an enormous interest from NGOs to participate in such activities.

Liz Gosme (COFACE Families Europe) explained that COFACE functions in a pluralistic way, contributing to the work of the *Alliance* with the views of families, consumers and users as shapers of the internet. In this context, Liz Gosme referred to COFACE's position on several European legislative reforms, from the Audiovisual Media Service Directive (AVMSD) to the General Data Protection Regulation (GDPR) and gave some innovative suggestions for improvements online, such as creating special types of accounts for children under 16 where data is not processed.



Youth panellists addressed the SIF audience as part of a session updating on the work of the Alliance to better protect minors online.

The two youth panellists, **Olivia** and **Henkka** (from Denmark and Finland respectively), commented that young people use technology all the time and, particularly, social media which requires a forward-thinking approach in terms of what is being put online. Generally speaking, youth experiment a lot (online) and make mistakes; they should therefore have the opportunity to acknowledge and repair their mistakes by having more control over their data. In this respect especially, Olivia and Henkka advocated for tech companies to be more transparent and honest. Marco Pancini responded, explaining that Google is certainly trying to empower users, while also seeking to make Terms and Conditions as open and accessible as possible (these approaches can be seen in the <u>new Google Privacy Policy</u> and <u>Privacy Centre</u>). Google welcomes feedback on these initiatives.

Following further discussion on how the *Alliance* can work together for a better internet, Claire Bury then invited Olivia and Henkka to share information on the work they had been doing as members of the European Youth Panel. The two youth panellists gave an overview of the new BIK Youth programme which they had been collaborating on along with their fellow youth panellists through a series of webinars. This preparatory work had culminated in a face-to-face meeting with their peers on the day prior to SIF, during which they planned, scripted and filmed a video for their new "Together For Respect" campaign to help build an online world free from bullying, racism and intolerance.



The European Youth Panel launched a new youth-led campaign at Safer Internet Forum 2017 - #TogetherForRespect.

The campaign message calls upon young people (and others) to go beyond just telling their story in terms of cyberbullying, racism or intolerance, but also to explain how they counteracted this, their hopes for the future, being the better person, and standing up also for other people who are active in this sphere and who may be subjected to bullying or harassment as a result. The campaign strategy aims to spread the message using a chain approach, as exemplified in the different roles of the youth panellists in "telling the story" in their video and through a direct call to action. Through this campaign, the youth panellists wanted to explain how cyberbullying goes beyond nationality, age or gender yet, at the same time, we all need to stand together to counteract it, hence #TogetherForRespect. The main distinctive note of this campaign, and the reason why the youth panellists believe it can make a difference, is because it is something (and someone) young people can relate to, being co-created by youth.

In concluding their presentation, Olivia and Henkka revealed that the youth panellists have set themselves a target for disseminating their campaign in the coming months, culminating in the milestone of Safer Internet Day (SID), taking place on Tuesday, 6 February 2018, especially as the youth campaign aligns perfectly with the SID 2018 theme of "Create, connect and share respect: A better internet starts with you". Following SIF, the youth panellists have agreed to take the campaign back to their national youth panels, their schools and their peers, in order to spread the message and share positive stories to stand Together For Respect.

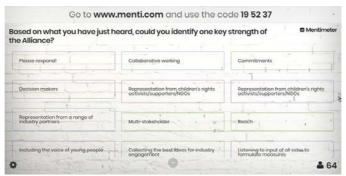
The panel discussion continued, touching upon data protection issues to which *Alliance* members referenced the alignment of its work with the forthcoming General Data Protection Regulation (GDPR), entering into force across Europe in May 2018. A point was raised on membership affiliation to the *Alliance*, to which the EC responded that it is ready to engage with other companies and organisations active in the field upon contact. Youth panellists from the audience also raised the issue of online hate speech, asking how it is being addressed by *Alliance* members. In response, Marco Pancini (Google) referred to the

<u>YouTube Creators for Change</u> programme which seeks to promote positive online messages and combat hate through inclusivity.

The second part of this session was given over to an interactive exercise during which SIF participants were asked to address three key questions as follows:

- 1. Based on what you have just heard, could you identify one key strength of the *Alliance*?
- 2. What is missing? What needs to be included that isn't currently there?
- 3. Are there particular activity lines/support mechanisms which could leverage/strengthen the work of the *Alliance*? This could be an awareness-raising or training activity, a cross-European youth programme, a European policy initiative, and so forth. It is important that the work of the *Alliance* makes an actual difference so what else can and should be done?

Table discussions then ensued, with a table facilitator appointed to keep discussions on track and draw out the key points. Participants were able to submit their responses using an interactive tool which helped to visualise ideas on screen for all participants to see.



An interactive tool allowed for suggestions from the SIF audience to be visualised on screen.

On the point of question 1, **Based on what you have just heard, could you identify one key strength of the Alliance?**, responses included the following:

- Share experience/exchange thoughts and ideas with big companies that have big influence and institutions such as European Commission.
- Have the tools and connections to make changes.
- The *Alliance* has the ability to put pressure on the BIG companies: a fear of being fined will make them more proactive in building tools to keep children safe.
- Wide-reaching change rather than just regional.
- Industry have the chance to share knowledge and experience, instead of working competitively.
- · Common sense and information.
- Knowledge sharing.
- · Cooperation.
- Stronger connections between civil society, regulators and industry.

On the point of question 2, **What is missing? What needs to be included that isn't currently there?**, responses included the following:

- More youth voice, from different backgrounds.
- Clarification of working methods and goals.
- More transparency about the purpose and possibilities of the network.
- Need to consider what added value the Alliance brings.
- Reaching out to websites and web-based services that aren't already involved in child protection, therefore not always preaching to the converted.
- Share results more often.
- Including the voice of adults as well as children (specifically people in further education who have grown up with the internet but are no longer classed as young people).
- Understandable terms of service.
- Comparable data between Alliance members.
- Communicating about what they are doing who is the audience?
- More transparency and progress steps.
- New values.
- Having a specific agenda which leads to a practical solution, not just general issues.
- Involvement of political leaders.
- Young people and users are missing.
- Who will carry out the independent evaluation?
- There are too many coalitions with the same partners.

On the point of question 3, *Are there particular activity lines support mechanisms which could leverage/strengthen the work of the Alliance?*, responses included the following:

- Research.
- More experts.
- An annual campaign.
- Working more closely with government to implement initiatives.
- More teenagers to make resources to promote the existence and work of the *Alliance*.
- Open to contributions from people that are not "in it" but have good ideas about what they should do, something like an "online suggestions box".
- Talk with younger users not at them!
- Creating something for start-ups so they know of the *Alliance* before they start developing platforms and services.
- Common marking.
- Common awareness-raising campaigns.
- Financial support for research and the work of NGOs.
- Guidance on how to translate top-level work into more practical applications in individual countries.
- Communicate areas that the Alliance is working on.
- Consider forming country sub groups.
- An overview of how the *Alliance* comes together with other networks that is, not overlapping or overlaying existing networks, but bringing something more to the table.
- An annual report to give more accountability.

- Closer collaboration with law enforcement.
- Clear labels for advertisements.

To supplement the screen-based responses, a small amount of feedback time allowed for verbal comments from the audience. Comments mirrored those on screen, identifying strengths included the diversity of stakeholders involved in the *Alliance*, and the opportunity to push forward with good practices. Missing aspects included transparency and accountability, and the need to review and reflect on the *Alliance's* developments. As for possible new activity lines, mechanisms, financial support, regulation for young users and pace of change (membership) were the main points raised by the audience. All of the points raised will be taken back to a meeting of the *Alliance* for further discussion.

Children and robotic toys

Keynote speaker: Jochen Peter, University of Amsterdam

Chair: Patrick Geary, UNICEF

Panellists:

Victoria Nash, Oxford Internet Institute

- Catherine Van Reeth, Toy Industries of Europe
- David Martin, BEUC

We are told to expect fundamental changes in human life that will not only apply to adults but, thanks to the emergence of an "internet of toys", to children and young people too. As more and more aspects of our lives are transformed into computerised data, consideration needs to be given to how we protect young people and provide them with opportunities to grow up in a safe and secure digital world.

In his keynote presentation, **Jochen Peter** considered the robotification of childhood by looking at how the interaction between children and connected toys can have an impact on their development, health and wellbeing. He began his keynote by highlighting some of the developments in how we view robots in our daily lives. Once seen as dull, dirty and dangerous, industrial and a threat to labour in factory environments, they have evolved into a tool that we consider to be sophisticated, supportive and social, and something that we can interact with in our homes and in our leisure time. While toys have long been fashioned as robots, we have seen more sophistication in recent years, no longer just taking the shape and form of the classic science fiction robot, but now coming to life in walking, talking and thinking toys.



Jochen Peter delivered the keynote presentation at Safer Internet Forum 2017 on the robotification of childhood.

Jochen Peter went on to explain some of the technological changes behind "robotification", which can be summarised as follows:

- Exponential increases in computing power.
- Mobile connectivity.
- Datafication and networked information.

- Miniaturisation of sensors, microphones, and cameras.
- (Robot) cloud computing.
- Progress in artificial intelligence and machine learning.

Shifting the discussion towards social robots, Jochen Peter gave an example of a conversation with Siri; amusing as a conversation with a digital assistant might be, it shows the depth of maturity behind the AI (artificial intelligence) and algorithms which drive it. A social robot can be defined as "An artificial, embodied device that can sense its (social) environment and purposefully and autonomously interact with (agents in) that environment following social rules attached to its role." Social robots may be especially appealing to children as they early adopters of new technologies and are often targeted also as users of new technologies. In addition, children typically have an emerging but scattered field of diverging interests. As a result, however, children are probably more susceptible to the effects of interacting with robots.

Typical features of child-robot interaction include:

- Mobility.
- Interactivity/Reciprocity.
- "Naturalisation" (speech, gestures, and vision rather than text).
- Adjustability of interaction.
- Personalisation.
- (Dis-)Embodiment.

while processes reflect:

- Anthropomorphism (displaying human characteristics or behaviour).
- Social presence.
- Involvement.
- Perceived similarity.

Jochen Peter went on to highlight some potential consequences for the cognitive development of children stemming from their interaction with robots, both positive and negative. Positive outcomes include improved learning which is personalised to the child, continuously updated and facilitates self-learning. Less positive outcomes stem from "educational bubbles", similar to "filter bubbles on the internet where content is restricted. In such instances, there is a risk of fragmentation in the child's knowledge and delivery of an abundance of facts, while the teaching style is based purely on algorithmic learning.

Similar concerns also apply to identity development of the child. Research-based studies have shown that robots can become an "extension of self" in addition to, and beyond, human to human contact. The positive side to this is that robots may allow older children and teens to expand and improve their identity search and/or definition throughout their adolescence. In terms of contraction of self, robots raise privacy issues, and there is a risk that they may be used as surveillance machines: technically, robots can record anything anyone says in its proximity, raising significant safety concerns for both parents and children.

When it comes to relational aspects, relationships with robots might not always reflect real relationships in real life. On the one hand this might lead to children getting isolated from society, finding comfort in an algorithm that soothes and comforts him or her. On the other hand, however, it could also mean that robots can provide a retreat for kids and teens, able to "discuss" things that are difficult to bring up in conversation with parents and peers. Our relationship with robots will always be a servant/master relationship, but robots can increasingly "pretend to feel" and therefore children might fall in the trap of considering this relationship authentic and mutual.

In conclusion, Jochen stated that robots have more to offer than traditional toys but they also present massive risks for the youngest users.

Following on from the keynote presentation, **Patrick Geary** (UNICEF) introduced the panel discussion by mentioning UNICEF's work on children's rights. As recreation is becoming more digitised and offers increasingly interactive experiences, presenting many benefits for health and education as well as protecting young people from violence, it is crucial to stress the importance of children's right to privacy both online and off.

In addressing the panellists, Patrick Geary posed the questions: What about decisional rights of children? What happens when robots influence children's decision-making skills?



A panel discussion considered some of the emerging issues relating to the internet of toys.

Victoria Nash (Oxford Internet Institute) commenced her presentation with a recommendation for both content and screen limitation, highlighting the fact that the screens with which children now interact on a daily basis could potentially be used by malevolent individuals. However, there has been a marked shift in concerns in recent times; according to Victoria Nash, the time has now come to stop focusing exclusively on screens and "screentime" but to consider also smart toys. She went on to make the point that the markets for smart/connected toys and Internet of Things (IoT)/smart devices in the home are expanding rapidly; some statistics estimate that the market share for this type of device is set to treble soon.

While it is still too soon to have clear evidence of any harms to children or families, there is evidence of pathways to risk around issues associated with some of these devices: for

example, some connected toys have been found to have significant security flaws and some have even proved to be "hackable". A particular concern was raised regarding voice-recognition enabled toys/dolls, as well as toys connected with video and online games.

Through her work, Victoria Nash regularly looks for evidence of risk and harm, as well as pathways to risk. Some of the pathways to risk identified to date include:

- A lack of transparent information for parents about how these devices can be used and what data they store/transmit. Online safety advice largely assumes that children are only connected to the internet via phones, tablets, PCs and similar, but guidance needs to be updated for this new genre of connectivity.
- Storage of data (speech/conversation) and data breaches: how and where is data stored? To give an example, there is evidence of growing identity theft relating to minors in the US.
- How the toy interacts with children: for example, via an app and the toy itself. In many cases, it has been seen that the manufacturer has been unable to respond to concerns raised by connected toys in a timely manner.
- Information given to both parents and children is first and foremost about hygiene and electrical safety. However, there needs to be a hierarchy to the guidance: more emphasis needs to be placed on online safety, and on safely configuring the toy.

Looking to the future, Victoria Nash foresees a risk of transforming parenting into a form of surveillance (one such example was given of a sensor for monitoring children's heartrate and other biological parameters). In this context, many companies might benefit from the data collected through these toys and devices, but we are moving towards constructing what we might call an "algorithmic child": one who leaves a dangerous trace online from the earliest of ages, which not only leads to online concerns but also ethical consequences.

David Martin (BEUC) began his presentation by introducing BEUC's mission of representing consumers' rights and testing products for customers. He went on to provide some examples of significant failings in relation to connected toys, taking into account aspects such as privacy, consumer rights, security, and children rights (research done by Forbrukerradet), to name but a few - more examples can be found using the #Toyfail hashtag. Findings relating to the reviewed products included:

- Terms and conditions are not transparent.
- Insecure products (no password).
- No control over what the toy may tell the child.
- Hidden marketing.

David Martin elaborated on a particular example relating to GPS watches for children, which indeed have now been banned by the German telecoms authority due to spying concerns. It had been proved that the watches can be easily hacked, they may reveal the children's location to malevolent individuals and are generally not secure. He went on to describe a genre of product termed "AI (artificial intelligence) babysitters". These products have raised numerous privacy and child psychology concerns. As a tool, they are supposed to sing songs, teach children basic things and, above all, monitor the child. This basically means that the

child has an online trace from day one without the tool having any clear terms and conditions concerning what happens with this data, where it is stored, and so on.

In conclusion, David Martin outlined how it is BEUC's aim to ensure that products are not made available on the market without prior and thorough testing. Some recommendations for the future include:

- Safety by design.
- A new approach to safety, with recognition that it is not safe for children and young people to use these products.
- Don't rely only on algorithms much unsafe content can make it past filters.
- Children should not be under constant surveillance or be subject to manipulation from connected products.
- Above all, we need to think of alternative business models for the future.

Catherine Van Reeth (Toy Industries of Europe (TIE)) took to the floor next, reminding everyone of the very first examples of toy robots which date from the 1950s, so illustrating how far we have come in a relatively short space of time. She stressed that *play* is at the heart of everything the industry does and that the safety of their users is crucial. As both the UN and UNICEF recognise, play is a fundamental need for children and there are recognised benefits of children having a balanced "play diet". As a trade association, TIE has an awareness-raising role in terms of what technology can offer to young users, while minimising the risks.

According to TIE, new technologies can enhance play and as far as connected toys are concerned - in their experience - "safety settings" might actually deter kids from using them because they find it limiting and less exciting. Industry must however conduct thorough risk assessments when bringing new connected toys to market. In terms of privacy, for example, data protection legislation is already in place, but the incoming General Data Protection Regulation (GDPR) will bring about many changes, particularly when it comes to consent. For instance, if the user is under 14, parental consent will be requested to be able to use the toy. Another mandate is privacy by default and by design.

One main concern of industry is to empower parents to become involved in connected play by knowing how to change factory settings and passwords, and by choosing the right privacy settings on the toy they have just purchased. Catherine Van Reeth stressed that hacking is a criminal activity and it is impossible to fully design against criminal intent. However, while more and more kids are requesting interactive toys, the industry tries to create safe toys which are respectful of physical safety and for which parents need to give consent before their children can use them.

Discussion continued with questions and comments from the floor. For example, Sophie, a youth panellist from the UK raised a common concern of youth of parents posting images of their kids, possessing little understanding of what data harvesting is. She reflected that more needs be done to improve the digital literacy skills of adults too. Another participant raised a concern that kids are taking AI (artificial intelligence) for granted and do not possess sufficient critical thinking skills to question the potential impact of their interactions. Other

comments related to GDPR and data collection, and the fact that more needs to be done to make Terms and Conditions clearer, and to provide end users with more choice.

The session ended with Jochen Peter stating that the internet is still a relatively new phenomenon and data can be considered the "gold rush". For this very reason, these concerns should be put at the centre of our research and interests, while children should be more empowered with what they do both online and offline.

Parallel session A1:

Should age determine how we experience the internet? Tensions between protection and participation

Chair: Simone van der Hof, Leiden University

Panellists:

- Mark Cole, University of Luxembourg
- Abhilash Nair, Aston University
- Emil Valdelin, Facebook
- Anne Mette Thorhauge, Media Council for Children and Young People
- Silvia Costa, MEP

In a rapidly evolving digital landscape, the protection of users, and particularly younger users, is paramount. How can we balance the need for some managed risk to develop resilience against the concerns about exposure to inappropriate or harmful content/contact/conduct? In this session, a panel of experts considered whether we are moving towards an internet which is fragmented across age groups, looking at issues surrounding emerging legislation and technical solutions being proposed to protect children and young people online.

Chair of the session, **Simone van def Hof** (Leiden University) introduced the topic, giving examples of how age classification has already been used for a long while in areas such as film and TV, allowing parents to select what type of content they permit their children to see. She spoke about how the internet is characterised by an exploding amount of data, including that which is potentially harmful or simply not appropriate – or designed for – children and young people. But, while much of the internet's content is designed for adults, it is undoubtedly attractive to younger users. We must also consider, however, that parental limitations to certain content, tools and services might also be harmful to fundamental rights, such as freedom of expression and similar. Simone van def Hof then posed two questions of the panellists:

- 1. Should we verify age to control/differentiate the kind of content/applications that children and young people can access online?
- 2. Can this approach be effective? If so, how?

Mark Cole (University of Luxembourg) raised the question of what is the role currently played by "age" in EU regulatory frameworks, and how prominently age features in recent EU safer/better internet policy frameworks/initiatives. In this regard, he outlined the provisions of the new Audiovisual Media Services Directive (AVMSD) where Article 27, for example, calls for the identification of TV programmes (symbols, sounds) before the programme starts for national television, while Article 12 covers on-demand services. Provisions are also made for advertisements and distinguishing the content's level of "harm" for minors. Mark Cole also referenced the incoming General Data Protection Regulation (GDPR) where, for certain services, parental permission is mandatory for children to access them. The limit is 16, but Member States are currently debating the differences in

age depending on the children level of maturity, education and so on, while any data pertaining to children is basically regarded as sensitive data. There is currently much debate about how this will be enforced, while the Regulation also promotes the use of Codes of Conduct.

Abhilash Nair (Aston University) looked at how regulation can work from a technical standpoint. Age verification has existed in the physical world for a long time, but the online world is still catching up. There are various models being considered – for example, is an age verification regulator needed to deal with setting the rules and with enforcement powers such as the power to issue a financial notice or the power to ask internet service providers (ISPs) to block content and/or access. On this point, he gave the example of the Digital Economy Act in the UK which is introducing a new requirement for pornographic websites to verify the age of visitors. The age verification regulator is expected to be the British Board of Film Classification (BBFC) and will have the power to fine websites up to £250,000 or 5 per cent of their turnover for non-compliance.

Business models for age verification also need to be looked at in depth – as is typical of the web, "free" services still incur a cost to someone, in some form. There is also the question of identification or definition of content – how do we define and identify "harmful" content, and how do we associate this with age. On this point, Abhilash Nair reiterated the issue of rights of the individual when it comes to potentially restricting access to content and services.

Next, Emil Valdelin (Facebook) provide an insight into how Facebook differentiates the user experience for younger Facebook users as compared to adults. A number of features have been designed specifically for a younger audience, such as stricter privacy settings defined by default upon sign up, limiting the scope for the user to modify these and automatically setting profiles to private. More generally, the platform has developed a variety of tools to analyse online behaviour and flag issues of concern, while the community standards enforce strict rules especially in areas such as harmful content and advertising. Linked to this, Facebook provide easy-to-use reporting tools, with many reports being reviewed by humans, while photo DNA technology is used to detect and track images depicting child exploitation. On the point of young people under the age of 13 registering on the platform, Facebook recognises that this is possible in practice. As such, systems are in place for when underage accounts are reported, incorporating various measures and revision processes.

In relation to the requirements of the GDPR, Emil Valdelin explained that Facebook are actively working on compliance strategies. An extensive team has been created to work on the necessary measures, consulting with experts and relevant stakeholders in "design jams" on the topic including issues relating to differentiation by country and the critical aspect of not collecting superfluous data.

Anne Mette Thorhauge (Media Council for Children and Young People) broadened the debate by stating that there are other approaches beyond age verification for addressing this issue. As such, she urged us to take step back and ask ourselves what do we mean by the concept of age verification and what are the problems we are trying to solve? In doing so, we must consider various issues including the fact that not all content is designed for

children and that, even when given the option, children may not be able to make informed decisions about the use of their data.

Anne Mette Thorhauge went on to identify potential issues with age verification measures:

- Children are citizens and age verification might violate their democratic citizen rights, such as right of participation.
- Access to diverse materials, in media, in particular aimed at promoting wellbeing.
- Children have the right of participation beyond the right to protection (although it is a fine balancing act) and the internet is a platform for participation, not only for content distribution.

She referred to the UN Convention on the Rights of the Child (UNCRC) in particular, citing:

Article 13

The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.

and

Article 17

States Parties recognize the important function performed by the mass media and shall ensure that the child has access to information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health.

Silvia Costa MEP provided an overview of Initiatives, approaches and key issues, stating that this is a cross-cutting issue, transversal with all EU policy. As such, we need to go beyond fragmentation and create a real agenda for minors. She referred to various initiatives in this field such as the 2012 EU Framework of Law for Children's Rights (ongoing), the European Parliament Intergroup on Child Rights, and the 2011 report on Children in the Digital World (which also addressed some of the grey areas). She also touched upon various Directives, such as those for child abuse and privacy, and the Single Market Strategy. In terms of European Parliament progress on these issues, we are seeing the development of Codes of Conduct for audio-visual distribution, to be adopted by all, and emerging regulation on online platforms specifically. However, in summing up, Silvia Costa acknowledged that the issue of liability still presents some challenges, as does the balance between protection and freedom in the online world.

Discussion continued with questions and comments from the floor, including issues around user-generated harmful content on social media platforms, and how to tackle the sheer volume of content. On these points, Emil Valdelin responded by stating that Facebook is increasing the number of human reviewers alongside AI (artificial intelligence) review of content. The human perspective is especially important where context has a bearing on whether content would be termed harmful or not. A further comment queried the perceived lack of consciousness of young people with regards to giving informed consent, but argued that many adults may also not be fully informed too.

In summary, the panellists concluded that any form of regulation by age would need to be based on clear definitions, objective criteria, and high-quality research, while also recognising the need to be sensitive to child rights.

Parallel session A2: Child sexual abuse images – the tip of the iceberg?

Chair: Arda Gerkens, INHOPE

Panellists:

- Fred Langford, IWF
- Hedwig de Jager, INTERPOL
- Oscar Pettersson, NetClean
- Ernesto Caffo, SOS Il Telefono Azzurro Onlus

Combatting online child sexual abuse material (CSAM) is an ongoing battle with increasing numbers of invested stakeholders collaborating to do everything possible to keep the internet free of such content. This panel discussion, chaired by **Arda Gerkens** (President of INHOPE, the International Association of Internet Hotlines) discussed approaches, bringing in different perspectives from some of the actors who have taken up the fight. The key message that resonated strongly among the panellists was collaboration.



A panel discussion considered collaborative approaches to combatting child sexual abuse material online.

Oscar Pettersson (Netclean) stated, "We want to highlight the importance of three main areas; technology, knowledge and the importance of collaboration, and that every image counts to be able to detect material and rescue children."

Hedwig de Jager (INTERPOL) seconded Oscar Pettersson's comment and added, "We work with INHOPE via the ICCAM system and receive reports from hotlines. Sometimes the material is known, sometimes the material is new. We need to find new material as offenders keep developing and advancing (technologically) and we have to stay on top on this to prevent an increase in offences." INHOPE's ICCAM system allows for sharing of reports on a secure platform across hotlines, as well as providing information to INTERPOL on the reported CSAM.

Fred Langford (Internet Watch Foundation (IWF)) highlighted the importance of proactive search to find new and previously seen material, "There are an increasing number of people coming online and although we haven't achieved global penetration, we are getting better at finding CSAM."

In addressing the urgent need to unearth previously unseen content, a comment from the audience suggested carrying out proactive searches by non-profit organisations and private companies to assist law enforcement. On this point, Hedwig de Jager cautioned, "Who would provide the appropriate permissions for these bodies to carry out this task? Additionally, we should also be careful while asking stakeholders other than law enforcement to engage in this activity. All organisations should be screened and also monitored regularly."

To conclude the session, all panellists were asked for their priority area of focus: the IWF highlighted the importance of finding content and cleaning the internet of this material, while NetClean's focus was on strengthening and improving collaboration and processes among stakeholders, as well as facilitating detection and reporting of CSAM for the business sector. **Professor Ernesto Caffo** (Telefono Azzurro) stated that research on a global level is vital in order to spread awareness on different levels and to find new solutions to the problems, also by encouraging children to play an active role. Hedwig de Jager said that identifying victims was critical, in addition to removing content from the internet.

While each of the panellists had a different focus area, all agreed that the ultimate goal was to combat online CSAM together.

Building resilience with vulnerable groups

Chair: Anna Rywczyńska, NASK/Safer Internet Centre Poland

Panellists:

- Nadia Kutscher, University of Cologne
- Alyssa M. Alcorn, University College London
- Beckie J. Brown, Film-maker and vlogger

Respondent: Niels-Christian Bilenberg, Centre for Digital Youth Care

This final plenary session discussed the impact (both positive and negative) of technology on a number of emerging target groups, often considered to be "vulnerable". Speakers outlined the challenges for each group and considered how technology can be both a facilitator and an inhibitor.

The panel was chaired by **Anna Rywczyńska** (NASK/Safer Internet Centre Poland) who kicked-off the session by asking the audience to define the terminology "vulnerable group"; it was soon apparent that definitions are widespread and can apply to numerous and varied groups. Against this background, speakers focused on three specific groups: migrants, young people with autism spectrum disorder (ASD), while the final speaker focused on her challenges with <u>trichotillomania</u>, a hair-pulling disorder.

Nadia Kutscher (University of Cologne), outlined that children and young people from migrant backgrounds often come to (or already live in) Europe with particular sets of sociocultural experiences and expectations. While technology is often thought to be a facilitator to connect and participate, online risks and opportunities can differ greatly across contexts. Furthermore, empirical findings and research shows a vital function of digital media in general, because:

- It is important for orientation on the way to Europe.
- It is a central function for appropriation and being acquainted with the society/culture of the receiving country.
- "The internet is like food" social media plays a key role in maintaining contact with family and peers, and for accessing general information.

To exemplify these points, Nadia Kutscher showed the mobile phone home screen of a migrant that mainly showed apps concerning languages, local newspapers and for prayer. However, alongside the many positive aspects, digital media also brings various challenges for migrants, including:

- Infrastructure: It's important to also think about "safe spaces" online in order to ensure that migrants can benefit from privacy and safety too.
- Resources: Migrants spend most of their money on pre-paid phone cards.
- Integration: Alongside having access to technology, migrants also need to receive a good digital education.

Next up was **Alyssa M. Alcorn** (University College London) with a focus on autism spectrum disorder (ASD). The autism spectrum summarises two core domains in DSM-5 behaviour diagnostic process:

- Restricted and repetitive behaviour ("the need for sameness").
- Difficulty with social and communicative behaviours.
- Frequent co-occurrence with intellectual disability, language issues and similar.

Technology and the internet offer endless opportunities for young people when learning, communicating and playing. However, alongside these benefits there are many risks that young people with ASD may be more vulnerable to, such as:

- The internet can give young people with autism opportunities for socialising and special interests that they may not have offline.
- Social challenges, such as a difficulty with understanding others' intentions, can leave this group vulnerable to "friends" with bad intensions.
- Online challenges are often connected to core characteristics of autism: concrete, specific guidance could improve individuals' online experiences, but the underlying challenges remain.

In conclusion, Alyssa M. Alcorn pointed to Childnet's <u>STAR SEN toolkit</u> as a best practice example supporting children and young people with ASD to stay safe in today's digital world.

Niels-Christian Bilenberg (Danish Centre for Digital Youth Care) acted as respondent to the first two presentations, sharing some of his experiences with providing direct counselling to vulnerable children and young people, both online and offline. From this, he concluded that digital media is extremely resourceful and provides positive opportunities for vulnerable groups. However, we need read between the lines as, in many situations, vulnerable groups have difficulties understanding the broader context (for example, online behaviour versus offline behaviour).

A key challenge is how do we keep the internet open for positive opportunities, while at the same time keeping vulnerable children particularly safe? In this regard, the idea of a "social media mentor" was mentioned, allowing someone to connect to the social media profile of a vulnerable child or young person in order to support when help is needed. Equally, however, this could be in conflict with a young person's right to privacy online. The anonymity offered by being online can however be helpful, especially with reference to enabling vulnerable children and young people to open up and talk about their problems and issues.

Linked to this final point, **Beckie J. Brown** (filmmaker and vlogger) shared her story with the audience. Being a YouTuber for 11 years, Beckie started posting content mainly related to her hair-pulling disorder, trichotillomania. Over the years, the online world has helped her to cope with the various struggles presented by her disorder, as she so eloquently stated: *"The online world is a lifeline for those who have no support offline."*

_

¹ The Diagnostic and Statistical Manual of Mental Disorders – 5th edition



Beckie J. Brown spoke about how being online helped her to address some of her vulnerabilities as a young person.

On the flipside however, Beckie J. Brown also addressed the risks of posting content online during periods when she was feeling particularly unwell and vulnerable, and the negative feedback she received as a result: "It's very hard to deal with it [the criticism] on a daily basis, regardless of how famous you are." Reflecting back on that experience now, however, she went on to say: "I opened up and did not hide, which gives me the possibility to collaborate with many great organisations in the field of mental health issues, helping many other people in similar situations."

Nowadays, her YouTube channels count over 49 million views, while she has 33.4k followers on Instagram.

Close of Safer Internet Forum 2017

Closing remarks: Gail Kent, Director, DG CONNECT

In her closing remarks, **Gail Kent**, Director of the European Commission's DG CONNECT summarised that the 2017 edition of the Safer Internet Forum had covered a very wide range of topics, all focusing on the common aim of promoting wellbeing online for Europe's children and young people.

She especially praised the contributions of the youth panellists, and urged all SIF participants to support the youth-led <u>#TogetherForRespect</u> campaign when back in their own settings and countries.

She also reminded participants that although good progress has been made, we must not be complacent – we must continue promoting all the good knowledge and resources we collectively have, and keep the focus for a better internet high in public consciousness. Echoing Claire Bury's comments from the opening session, Gail Kent again stated that the EC will continue to support this line of work, with a further campaign of action launching on Safer Internet Day, taking place on Tuesday, 6 February 2018.



Annex I: European Youth Panel

Coming from 13 European countries (Austria, Belgium, Denmark, Finland, Germany, Hungary, Latvia, Lithuania, Luxembourg, Norway, Poland, Romania, United Kingdom), 15 youth panellists travelled to Brussels for the European Youth Panel (YEP) 2017 edition, organised back to back with the Safer Internet Forum (SIF). The youth panellists had already been working together since September in online capacity-building sessions as part of the BIK Youth programme, and had already agreed upon a principle and youth participation scenario for a better internet for children and young people. Their principle, an "Online world free from bullying, racism and intolerance", identified a series of gaps which could be tackled through a youth participation scenario to be developed in hands-on activities at YEP. The youth panellists envisaged a peer-to-peer digital campaign, where young people addressed their peers through a video encouraging them to stand "Together for respect" and a corresponding hashtag #TogetherForRespect.

The face-to-face YEP activities started on the morning of 22 November 2017 at the Google offices in Brussels. Youth panellists worked together in different teams (supported by a privacy expert, a representative of the Austrian Safer Internet Centre and BIK Coordination Team representatives), agreeing upon a campaign strategy, logo, communication plan, scripting, filming and editing. The youth panellists considered it to be extremely important that this campaign reflected their diverse European backgrounds, and they were also keen to have the script in several European languages to help maximise the outreach at national level. Wrapping up the morning session, youth panellists also had the chance to take a tour of the Google office and discuss their plans with the Google Public Policy Director who was keen to see their youth participation scenario coming together at the Safer Internet Forum the next day.

YEP activities then continued into the afternoon back at the <u>European Schoolnet</u> offices, working in the <u>Future Classroom Lab</u>. There, the youth panellists finalised their communications strategy, filmed their launch video and teaser, and started to edit it for their <u>youth participation scenario "Together for respect"</u>. In the afternoon, youth panellists also agreed upon the information to be shared in the Youth corner (a space in the exhibition area at the Safer Internet Forum) and discussed points to be raised by their two youth representatives in the policy setting of a high-level panel discussion the following day.

During their time together, the youth panellists also discussed current topical issues, such as fake news, and agreed upon different approaches on how they encountered fake news and the fact that many of their peers may use unreliable sources for news, not distinguishing clearly between information and misinformation. When debating digital policy aspects, youth panellists identified a series of elements which are somehow missing or which would benefit from improvement in the online services they are using, including:

- To have more options to control your data (including the right to be forgotten).
- To have the right to erase pictures of children that have been posted by parents.
- To have more control (as users) over the business models that companies use for our data.
- To have a different response from companies (perhaps some special services).

To step up to regain trust from users.

This short video captures the essence of YEP:



Youth panellists from across Europe worked collaboratively to develop their campaign.

The following day, the youth panellists joined the annual, international Safer Internet Forum (SIF), where their "Together for Respect" campaign was launched during a high-level opening session with the European Commission and leading ICT and media company members of the EC-facilitated, self-regulated *Alliance to better protect minors online* – see the main SIF report above for further information.



The European Youth Panel 2017.

For further information, see the additional <u>youth testimonials from YEP</u> or visit the new <u>BIK</u> Youth minisite on the Better Internet for Kids portal.

Annex II: Teacher Panel

Seven teachers from the eSafety group of the eTwinning network² were selected to form a Teacher Panel which met on Wednesday, 22 November 2017, ahead of the Safer Internet Forum 2017³. The teachers came from Greece, Italy, Poland, Romania, Serbia, Spain and Ukraine and spent a day discussing a number of different issues relating to online safety.

The panel had three main objectives:

- 1. To discuss some of the challenges facing children and young people when they go online.
- 2. To provide a better understanding of the Safer Internet Forum and its intended outcomes for participants.
- 3. To share best practices from different schools and countries.

The session began with some ice-breaking activities including a quiz to see how many logos of popular apps and social networking sites the teachers were able to identify. This activity illustrated how quickly technology moves, as well as the vast array of different apps and platforms that are available and being used by young people.

A discussion took place about what online safety meant to the participants, with the key issues shown in the word cloud below.

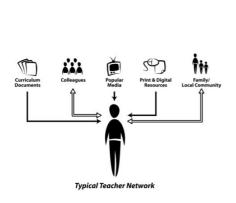


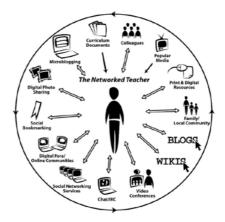
Teachers acknowledged that they do use technology to support teaching and learning in their classrooms, but that this was not widespread. A useful comparison was made between a typical teacher and a networked teacher, as shown in the illustration below⁴.

³ www.betterinternetforkids.eu/sif

² www.etwinning.net

⁴ Diagram based on research by Dr Alec Couros, available under Creative Commons. See https://dmlcentral.net/professor-alec-couros-the-connected-teacher/.





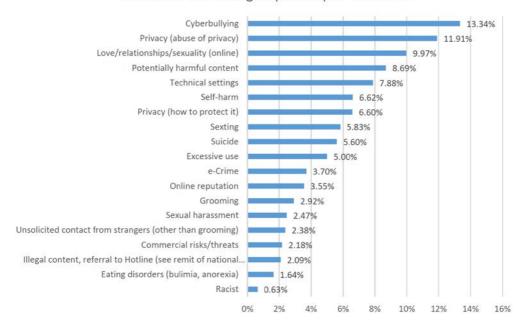
Trends in online safety

A brief overview was shared about some of the latest trends and developments in online safety. It was agreed that it was necessary to move away from some of the more traditional online safety messages (don't talk to strangers online or don't give out any personal information) and to think about some of the other challenges too. A quote from Tristan Harris was shared:

"Technology steers what 2 billion people are thinking and believing every day. It's possibly the largest source of influence over 2 billion people's thoughts that has ever been created. Religions and governments don't have that much influence over people's daily thoughts."

Information about the Better Internet for Kids (BIK) portal (www.betterinternetforkids.eu) was shared with the teachers, along with an overview of the BIK Guide to online services and the Resource gallery. A summary of the Insafe helpline network was also shared which gives a good indication of the issues affecting children and young people across Europe.





Some key issues were identified as follows:

- Young people are getting online at an earlier age with many parents using technology as a substitute for human interaction.
- Some young people are put under a lot of pressure to look or behave a certain way when they are online. They are also finding it difficult to cope with the endless stream of messages, push notifications and the pressure to take the perfect selfie.
- Some recent research is suggesting that perhaps it is parents (as much as young people) who are using technology too much⁵.
- Many schools are confident that they are teaching online safety but whether what is being taught actually helps to keep children and young people safer when they go online is more difficult to define.

Some discussion took place about the prevalence of inappropriate content that is available online, particularly in light of the recent challenges with content on YouTube⁶.

It was agreed that an important strategy for schools in dealing with online issues is to focus on **behaviour rather than technology**. A useful approach is to make use of opportunities that present themselves through stories in the media which allow a conversation to take place between teachers and pupils - and parents and children - about an online-related issue.

Detailed discussion then took place on several specific issues:

Cyberbullying

A detailed discussion took place about cyberbullying and the boundary between "banter" and bullying with participants looking at some content and determining which it was. An activity from Childnet (part of the UK Safer Internet Centre) was used⁷ to help strengthen understanding of the issues.

Sexting

Participants took part in an activity whereby they considered a number of different sexting case studies and assessed them according to a typology created by David Finkelhor and Janis Wolak⁸. It was acknowledged that sexting is a particularly difficult area for schools to address and, of course for children and young people themselves.

Teachers were referred to a range of useful resources including the website of the <u>ENABLE</u> (<u>European Network Against Bullying in Learning and Leisure Environments</u>) project, the <u>Web We Want project</u> and the <u>minisite of the Positive Online Content Campaign</u>.

⁵ http://www.bbc.co.uk/news/education-39666863

⁶ http://www.bbc.co.uk/news/blogs-trending-39381889

⁷ http://www.childnet.com/resources/pshetoolkit

⁸ http://scholars.unh.edu/ccrc/48/

General Data Protection Regulation

Some discussion took place around the upcoming General Data Protection Regulation (GDPR). Schools and teachers generally feel ill-equipped to deal with the new legislation and a brief overview was shared of some of the key points that schools will need to address.

- The GDPR represents are EU-imposed rules which cannot be interpreted by member states within their own countries. These are baseline rules which will apply from May 2018. This is a hard deadline with no leeway. From 25 May 2018, the rules will apply in their entirety although several Data Protection Authorities (DPAs) have indicated that they will show some leniency initially as they recognise that many organisations are not ready and able to comply.
- The law says that any information which relates to or identifies an identifiable individual is personal data. This could include a name, address or email address, for example. It is important to recognise that an email address is personal data even if it is an anonymised address. It may not be possible to determine the name of an individual from an email address but if that email address is an identifier which singles out an individual from all other individuals then it is classed as personal data.
- Privacy notices will need to be updated because GDPR prescribes *for* organisations to include additional elements that were not needed before. *For example, they need to state the legal grounds for processing personal data and explicitly mention the legal grounds for consent.*
- There is a requirement to keep a record of processing activities and this is likely to be the biggest challenge. There needs to be a clear definition on what happens to data, how long it is kept, where it is kept, and so on. The DPA can ask for this information and so it needs to be ready and to hand. For example, for HR purposes, schools may have information such as name, marital status (for tax purposes), date of birth, starting date at the organisation, and so on. The GDPR will not state how this should be done or what format the information should be kept in, but it will state categories of data. Any process involving personal data must be recorded.
- USB sticks and tablets and phones all need to be encrypted. It will be important to have good technical security measures in place. Essentially information should be encrypted and behind a firewall. A major breach point is mobile phones as many schools allow staff members to have work emails sent to their phones. There will likely be a lot of personal information shared through emails, either sent to a mailbox or accessible through an email server and this can easily be lost or stolen. If an employee is accessing work emails through a phone, then the phone should have a PIN and should be encrypted. Data should be able to be wiped remotely through a mobile device management system. There is some uncertainty about iPhones and Android devices concerning exactly when data is encrypted.
- Data Protection Officer (DPO) in some countries this is new and refers to the
 individual who will be responsible for pointing out any issues that an organisation
 has with regards to data protection. All government organisations must have a Data
 Protection Officer. They need to have expert knowledge of data protection law and
 some experience in this field.

Some tricks and tips regarding data use and storage were shared as follows:



More at www.esafetylabel.eu

Following on from the one-day panel activity, the teachers took part in the Safer Internet Forum on the following day where they were able to discuss their work with other SIF participants.



The Teacher Panel 2017.