Report on the proceedings of

Safer Internet Forum 2021

(including an annex on the preceding BIK Youth Panel)

Further information from the Forum, including the full agenda, conference brochure with speaker biographies, presentations and session recordings (where available) can be found at www.betterinternetforkids.eu/sif.

Contents

Introduction

The **Safer Internet Forum (SIF)** is a key annual conference in Europe where policy makers, researchers, law enforcement bodies, youth, parents and carers, teachers, NGOs, industry representatives, experts and other relevant actors come together to discuss the latest trends, opportunities, risks and solutions related to child online safety. This year's edition took place online on 6-7 October 2021 and explored how to make **Europe's *Digital Decade* fit for children and young people**.

In March 2021, the European Commission adopted 2030 Digital Compass: the European way for the Digital Decade to translate the European Union's digital ambitions for 2030 into concrete targets and to ensure that these objectives will be met. The document identifies four 'cardinal points' on digital capacities in infrastructures, education and skills, and on the digital transformation of business and public services. This European way for the digital society is also based on ensuring full respect of EU fundamental rights, and will propose a comprehensive set of digital principles, including protecting and empowering children in the online space. A corresponding consultation exercise has sought to gather the views of European citizens, and particularly those of children and young people, on these digital principles.

Alongside this, the importance of the rights of children and young people have been brought to the fore in recent months with the publication of the EU Strategy on the Rights of the Child, the overarching ambition of which is to build the best possible life for children in the European Union and across the globe, including online. Additionally, the publication of General Comment No. 25 by the United Nations Committee on the Rights of the Child places a specific focus on the rights of young people online. In short, **every child has the right to be respected, protected and fulfilled in the digital environment**.

The European Commission has long been committed to this aim, providing legislative and financial support to Member States to create a safer and better internet for more than 20 years. Central to this effort has been the European Strategy for a Better Internet for Children (commonly known as the BIK Strategy) which has provided a key point of reference for online safety policy making since 2012. Within the contexts outlined above, the time has now come to review and update the BIK Strategy.

The 2021 edition of the Safer Internet Forum therefore showcased key findings from the recent digital principles consultation, amplifying the voices of children and young people to deliver a vision for a #DigitalDecade4YOUth. The event highlighted the priorities that different groups, including parents, carers, and teachers, have identified in order to fulfil children's rights in a digital world, while allowing them to engage, create and contribute within safe, ethical and inclusive online spaces.

Please read on to discover more about the event. Further information, including session recordings and presentations (where available), can be found at www.betterinternetforkids.eu/sif.

Safer Internet Forum (SIF) 2021 was organised by European Schoolnet on behalf of the European Commission in the framework of the EC's Better Internet for Kids initiative with funding provided by the Connecting Europe Facility (CEF) programme.

Safer Internet Forum 2021 – pre-event

To kick off this year's edition of the Safer Internet Forum (SIF), a pre-event took place on the evening of Tuesday, 5 October 2021 to launch of the findings from the #DigitalDecade4YOUth consultation: *How to make Europe's Digital Decade fit for children and young people? A report from the consultation with children and young people*. This was followed by a youth-led discussion with the BIK Youth Panel 2021.

Opening the proceedings, **June Lowery-Kingston, Head of Unit Accessibility, Multilingualism and Safer Internet, DG CONNECT, European Commission** welcomed attendees, and gave particular thanks to the BIK Youth Panellists and those young people (and facilitators) who had been involved in the recent consultation exercises.

Setting the context for the days to follow, June quoted a young person as cited in the consultation report "*Adults – and in particular politicians – do not care about their [children's] experiences in the digital environment*". She countered this by stressing that SIF 2021 would provide a space to listen to youth and to follow up with concrete actions, in turn ensuring that policies and practices have a positive impact on those they are designed to support. She continued by saying that the experts are in fact those who are under 18; we need them and their input to drive the agenda forward, and this has been a guiding principle behind the consultation. Moreover, the European Commission is committed to youth consultation and President von der Leyen – in her 2021 State of the Union address – had recently designated 2022 as the Year of European Youth, thus highlighting the important role and influence of young people.

June went on to state that the consultation will help shape the digital principles announced by the EC during the spring of 2021, which is due to be signed by the end of the year. Equally, the views shared will help to shape the new European Strategy for a Better Internet for Children (BIK Strategy), due in spring 2022.

Valerie Verdoodt, Affiliated Senior Researcher, KU Leuven then took the floor to present the key findings and outcomes from the consultation, again illustrating the importance of child- and youth participation, and the importance of understanding their role in the digital environment. She commented that children and youth across the EU (and beyond) were consulted, and this shows the EC's aspiration to put child participation at the heart of policies. Valerie also explained how the consultation was carried out in two phases, with the first phase with children and young people involving targeted consultations, including with many vulnerable youths. The second phase, ongoing at the time of the Forum, targeted all EU citizens including parents and teachers.

Valerie went on to outline how she supported the development of the consultation methodology, based on a child-rights approach to participation. It therefore followed the United Nations Convention on the Rights of the Child (UNCRC) principles of making efforts to be inclusive, reaching hard-to-reach youth, and enabling proper adult support, among other factors. A further important aspect of the approach was accountability in terms of a commitment to follow-up, therefore making a clear link between the exercise and the ongoing policy work of the EC.

The key findings and outcomes from the consultation report can be summarised as follows:

- The internet plays an important role in all parts of children and young people's lives. Interestingly, they recognised that the online world – much like the offline world – will never be completely safe.
- When asked what they care about the most online, there was a large cluster around gaming, listening to music and watching videos. Another cluster was around communication with friends and family, while a third cluster focused on information gathering and for learning purposes.
- During the pandemic, the internet was the most important link to the outside world for children and young people.
- When asked about the most important online risks, some respondents were concerned with all types of risks. However, the most frequent risks listed by children and young people were violent and harmful content, bullying, unwanted ads, and personal data not being safe.
- A general concern emerging from the findings was the lack of awareness of risk and mitigation measures among children and youth but also parents. Younger children were considered to have particularly low awareness.
- Other specific concerns were cyberbullying, followed by harmful and hateful content. The young respondents felt that if you were different in any way, you were more likely to be targeted. Other frequently mentioned risks included fake news and disinformation, privacy and data protection, lack of inclusion and accessibility, and financial risks in online games.
- With regards to policy recommendations and what needs to be improved, the respondents gave interesting insights such as harmonisation at EU level, improved media literacy, monitoring and enforcement of existing rules, and pressure and incentives for industry to improve. They feel that all relevant actors should take responsibility and work together where possible. They find it unacceptable that industry seem to fear their stakeholders more than keeping their users safe, and ideas were put forward on raising taxes from industry to improve awareness and education in the field.
- Young people see an important role for technology to improve the online environment but, equally, there needs to be more pressure on industry from the EU.

The next part of the session was led by the BIK Youth Panel, where they presented their views on the future of the internet. **Pratchi**, **Jane** and **Mia** explained that this year's BIK Youth Panel comprised 30 youth aged 12-18 from 19 European countries. Collectively, they want the internet to be a better and safer place, while at the same time offering opportunities and benefits. They explained how the Youth Panel first met, online, during September and brainstormed and researched topics that they feel policy makers need to address. They subsequently created a video for each topic, which were shown to participants:

- Why is it important to create a better online school environment?
- Why is our data being collected?
- How do we wish the internet to look in 2031?

The first video was about the online school environment, why schooling needs to adapt when teaching and learning happens online, and why teachers need to be more involved and acquire more digital skills. Digital inclusion is important in terms of education; for example, some students have not been able to take part in schooling, especially during lockdowns, as they don't have the necessary technology and access. This can cause them to drop out of school.

The second video focused on social networks and advertising, including how to act online, and the importance of protecting data. The young people spoke about their concerns over unwanted ads, and the fact that they feel monitored online, especially as geolocation tends to be the default setting on many apps and platforms. Questions like where data goes and who has access to it were raised, and they feel that data policies are too long or too vague. They suggested that policies need to change to help users better understand what they are consenting to, and that open-source methods should be used for tracking of data.

The third video focused on online society and investigated what could happen in the future. There is a lot of great technology, but this also provides cause for worry. The young people were concerned about the increased use of the internet due to the pandemic, and especially the increase in cyberbullying and fake news that came with this. They feel that unless changes are made, the internet could become a place of hatred. They also considered a way forward and felt that, along with industry, we can create an internet based on education and inclusivity. In short, Gen-Z strive for total inclusion; we need to unite to achieve this.

The session then split into breakout rooms, where participants worked with youth panellists to discuss the issues raised. After the breakout rooms, a representative from each room presented the main discussion points:

Angelo from the first breakout room started by saying that the video was created thanks to everyone in the group. He commented that during the pandemic, schooling took place online but internet issues sometimes impacted access. The group also discussed how you need to start by targeting teachers with professional development to improve learning on digital skills.

Dimitris summarised the discussions from breakout room 2 which covered many aspects related to privacy such as not reading what you are giving consent to. The group discussed how big companies do not provide real options for consent at present.

Anisa and **Billie** from the third breakout room shared their discussions, which included issues relating to inclusivity. They also talked about how COVID-19 has highlighted the importance of access to the internet. It is also essential that the internet becomes safer and more inclusive, while issues such as cyberbullying need to be combated collectively by multiple actors. The group also discussed simplification of terms and conditions, and the need for industry to become more child-friendly and transparent. In addition, language and age verification needs to be improved.

Mia summarised the discussion from breakout room 4 by stating that the internet needs to become more accessible, teachers need to be educated, people need to learn how to act online and where their data goes, and policy makers and industry need to make big changes to improve safety online.

Safer Internet Forum 2021: Introduction and welcome address

Karl Hopwood, European Schoolnet officially opened the Safer Internet Forum 2021 and welcomed all participants, remarking that over 670 people from 68 countries, representing a wide range of stakeholders, had registered for this edition. He went on to summarise the various consultation work which had taken place over recent months to guarantee that children and young people are placed at the centre of EU policy making with the aim of ensuring that we collectively promote, protect, respect and fulfil children's rights in the digital world when shaping the online world of the future. He concluded by stating that the opportunities and challenges presented by this will form the focus of discussions at the current Forum.

Karl then introduced a video address from **Thierry Breton, European Commissioner for the Internal Market**. In the address, Commissioner Breton confirmed that a safe, secure and trusted digital space is a cornerstone of European digital society, and this is especially true for children and young people who are increasingly growing up online. Every child has a right to be as respected, protected and empowered online as offline. He reflected that the pandemic has highlighted the digital divide, and that not all children have equal access to the tools that can support them. Digital literacy is key, and the digital transformation is a fundamental objective for Europe to provide everyone with equal opportunities. Keeping children and young people safe online is crucial, as is reducing risk, and tackling illegal content, while also upholding children's rights and ensuring that they receive adequate education. Commissioner Breton also reflected on the recent consultation exercises, and commented that the Safer Internet Forum provided an opportunity to take stock of the feedback received and seek inspiration on what needs to happen next. He therefore called on all participants to contribute, together, to build a digital world that young people deserve.

Keynote session: The Digital Decade we want to see for children and young people – a vision of 2030 online

The recording and selected presentations from this session are available from www.betterinternetforkids.eu/sif.

SAFER INTERNET FORUM Shaping a #DigitalDecade4YOUth

Keynote address

Professor Urs Gasser

Professor of Public Policy, Governance, and Innovative Technology,

Technical University of Munich, Germany

Better Internet for Kids

Professor Urs Gasser, Professor of Public Policy, Governance, and Innovative Technology, Technical University of Munich, Germany, delivered the keynote address of Safer Internet Forum 2021, opening his presentation by stating that he would explore 'bigger picture' issues for building a better internet for youth. He commented that we need to reflect on the past to build new policies and to focus on some persisting policy challenges that need to be addressed.

Professor Gasser stated that technology has dramatically changed over the last decade or so, as have the conditions of access where the lines between online and offline are becoming blurred. This is especially true given the onset of mobile technologies. Access is now ubiquitous, and these technological and behavioural shifts have had a big impact on both young people and adults.

Another trend over the last decade is that the youth spaces have become deeply commercialised; and online and offline starts to interact in this context. Giving the example of purchasing a pair of sneakers, Professor Gasser described how young people move between the two environments to plan, validate, source and complete the transaction. Despite some concerns, important skills are nevertheless developed within these commercial enclosures.

We are increasingly seeing new technologies emerge which support us in our online activities, but these in themselves are often paradoxical. Research suggests that young people, especially, want to reduce their screen time but, conversely, they may end up using more tech in doing so in the form of artificial intelligence (AI) and personal digital assistants. Such technologies are also making their way into classrooms.

The level of awareness of the positive use of technology is growing, but research shows that gaps remain related to age, participation and socio-economic conditions. It's important to be aware of risks and opportunities online, but it's equally vital to identify how we can move beyond awareness alone to a position of empowerment and agency for children and young people. The biggest puzzle here is to understand the intersectionality between the different areas. The complexity of interactions between, for example, technological advancements, changing business models, regulatory interventions and policy decisions are now recognised, but despite this we are still far away from an understanding of how to plan the future of policy.

Based on this, Professor Gasser highlighted three persistent challenges in the policy cycle:

- Evidence and learning policy: We all aspire to be evidence based but, at the same time, there is more work to be done to build robust interfaces between the world of research on one side and policy making at various levels on the other. Research and policy work needs to be synced and we need to know that we are asking the right questions, hence the need for youth involvement. Researchers need to be able to have access to data from industry, and funding for research needs to become easier to access. We also need a longitudinal study with youth to see impact over time – we currently do not have a method and ability to track policy in this way.

- Stakeholders and spheres: Stakeholders need to work together to address several issues such as literacy and privacy, and we need to decide who is responsible for what. We need to ask ourselves how we can work together to ensure that youth also have agency and empowerment, and consider both risks and opportunities. One example of this is connected learning: young people are learning in different ways, in different places, and with different partners in the digital environment compared to the old analogue environment. This presents a tremendous opportunity, and especially so for those young people who previously had no access to traditional learning environments. However, risks and new barriers also emerge in this scenario – we need to understand how youth, parents and caregivers, schools, industry and policy makers can work together to promote digital literacy, and bolster 21st century skills across different spheres, including in the social and personal space.

- From policy to practice: A key challenge is how to move from policy to practice. There is a big knowledge gap to bridge between the private and public sector, and the global south and the global north. Resources need to be assigned to translate policy into practice. Best practice guidance is emerging: for example, UNICEF has developed guidance on AI for children, but it's still difficult to understand what it means in reality. To give one example, the Berkman Klein Centre (BKC) along with the City of Helsinki worked on an AI-based tool for personalised learning. While the concept was great there were also many risks and although legal, technical and social policies were provided, it was very difficult to operationalise the principles (for example, What does it mean to live up to accountability? What is meaningful participation, and what does it look like?).

The final part of Professor Gasser's presentation focused on the importance of youth participation in the future. Previous policy cycles have focused on protection and this needs to continue, as does a focus on provision and access. However, we also need to add and strengthen participation; we must figure out how to equip youth to really participate in shaping the future. How can we create environments for youth to fully participate in society? And how do we involve youth in both policy making and policy implementation?

Youth participation requires investment, and we need to ask youth what they want. Here, Professor Gasser reflected on some research on youth participation in the digital world in which young people were asked what they wanted in return for their involvement in policy exercises and conversations. Four key areas stood out in the responses:

1. Young people want to acquire domain-specific and transferable skills as a result of their involvement.
2. They seek long-term engagement that is also relevant to their long-term goals.
3. Youth have a unique perspective and they expect to be equal partners in the exercises.
4. Course and programme design should be sensitive to these contexts.

Professor Gasser concluded his presentation by reflecting on four possible models for youth participation:

- Youth board: A programme to engage a group of young people who work with senior executives at the highest level of an organisation on strategic initiatives.
- Co-design: A collaborative and creative methodology that brings together youth with experts to learn from and with each other.
- Youth lab: A youth lab is envisioned as a space (whether physical or virtual) within, for instance, an academic institution, company or non-governmental organisation (NGO) that convenes a group of young people with adult stakeholders to create knowledge exchange opportunities.
- Participatory research: A research model that enables young people to participate as co-researchers in every stage of the research process, from conceptualising the themes to defining the methodology and the creation of outputs.

He further challenged all stakeholders to consider what we can do to bolster youth participation at both the policy and implementation level, and to take youth participation seriously moving forward.

Professor Veronica Barassi, Professor in Media and Communication Studies in the School of Humanities and Social Sciences, University of St. Gallen, Switzerland spoke next, opening her presentation by stating that she wanted to focus on how much data we produce on children.

She started with a personal story: during lockdown she found herself emptying out a room in her parents' home and was overwhelmed by all the data traces that she found from her youth. These included messages which were passed under the desk by her peers during classes, old medical reports and bills, and a report card from secondary school where her teacher had commented that she was 'very distracted' and 'lacked academic skills'. Professor Barassi reflected on what would happen if all of this were processed in the same way as modern data. Would she have had access to all of this? Would this be available to future employers, tracked by artificial intelligence (AI), and so on?

Professor Barassi fell pregnant during a time when she was working on research on data and participation, and realised that society did not have a critical understanding of what is happening to family life. She therefore launched her own research, Child Data Citizen Project (2016-2019), to investigate how different parents made sense of the experience, while also looking at her own experiences as a new parent. The study was structured as follows:

- The study was based on families in London and Los Angeles, with children between 0-13 years of age, whose personal information online is ruled by the Children's Online Privacy Protection Act (COPPA) (1998).
- 50 semi-structured interviews were carried out, alongside 9 months of digital ethnography of 8 families 'sharenting practices' on their social media accounts.
- Three years auto-ethnographic research was conducted on the datafication of Professor Barassi's own children, including all instances where she did not have a choice on data taken on her children.
- 'Platform analysis' of 4 social media platforms, 10 health tracking apps (pregnancy and baby apps), 4 home hubs, and 4 educational platforms.
- Analysis included the promotional cultures, business models and data policies of the different platforms, including how they also target children.

The key findings were:

- There is inevitability of datafication of family life. Families increasingly felt pressured, and the amount of data that was asked of them has increased significantly over the last five to six years. The research included people from different backgrounds, for example in terms of ethnicity and income. The findings showed a real issue of inequality when we consider datafication. For example, some men felt that they were well informed on how and why their data was being collected, whereas some women immigrants felt violated by the datafication of everyday life and, for them, everything had happened very suddenly.
- Another finding was the complexity of the environment that we are living in – families do not have the choice anymore and the pandemic has increased this. For example, during the pandemic, Professor Barassi had to create a Google Classroom account for her daughter. Despite trying to have agency and talking to the school about alternatives, ultimately she did not have a choice.
- Thirdly, children are the first generation of citizens which are 'datafied' from before birth. What we are collecting about them today will define them publicly in later life… unless we take action now.

When we talk about the profiling of children, it happens on at least three different levels:

- Data brokers are creating and selling profiles of children on the basis of the data they are collecting. For example, educational data brokers are collecting information on children as young as two. These profiles are very reductionist in nature; children are being profiled on the basis of ethnicity, religion, and whether they are 'awkward' or not. Legislation still does not cover these practices.
- The other issue emerging is the development of AI technologies which are used to profile children in different contexts. In schools, for example, we are not only seeing developments in terms of personalised learning, but the use of facial recognition, for example, to profile children who can be potentially at risk or could be perpetrators of mass shootings as is being see in the United States.

- Big tech companies have access to different types of data such as health data, educational data, and also home life data (such as virtual assistants, Google Home, and Amazon's Alexa), along with everything we publish about ourselves (such as online and on social media). As such, these companies have the opportunity to combine all this data to build a very detailed profile of individuals.

Consequently, all of the types of data outlined above could follow children throughout their lives. However, most of the data sets produced are not accurate and are not a correct representation of the individual. Children are being profiled on the basis of this data regardless, which can lead to bias, error and implications. It is not only personal data, but also highly contextualised data that is connected to the family, which is ultimately very unpredictable, messy, and complex.

We are living at a time where we see a radical transformation and we do not have sufficient regulations to protect children. There is often a lot of focus on consent but sometimes there is not a choice, and we need policies to address what is happening behind the scenes. We also need regulations stating that if a company gathers data from a child from a profile, they should not be able to process this data. There is an urgent need to tackle these issues as we move towards a more AI-driven future.

The third speaker of the keynote session was **Regína Jensdóttir, Head of the Children's Rights Division and CoE Coordinator for the Rights of the Child, Council of Europe**. She began by stating that, from the Council of Europe (COE) perspective, listening to children is the most important action to take when discussing the rights of the child, and this is something the COE consistently tries to inspire when working with Member States. The consultation and participation of children needs to happen at various stages. When dealing with the online domain, we need to try to balance the rights of the child with opportunities and risk, and aim to empower, strengthen and protect them at the same time. We need to build on the standards that we currently have to ensure that they are relevant, that they make sense, and that a balance is being reached through the legal frameworks which exist. We also need to adopt different strategies, with the help of entities such as the European Commission, the United Nations and the COE, to ensure that all of the relevant existing legal instruments are harnessed and put into practice. Equally, we need to look at what already exists in order to address gaps.

Children have been thrust into the online environment over recent years, without being asked; online schooling is an example of this. However, we are living in a digital divide and universal access is key. The platforms need to respect child rights and privacy, and we need to understand how data on children is being used. The vision for 2030 is that children have been listened to by all stakeholders – the EU, the COE, Member States, industry, the educational sector, parents, and so on. The opportunities exist, and methodologies and safeguarding measures are in place, so there is no excuse not to listen.

Regína reflected that the children involved in the Forum have raised concerns about cyberbullying, hateful and harmful content, fake news and disinformation, as well as threats to privacy and data protection. To counter this, they are asking for more awareness – they want themselves, parents, teachers and younger children to all be on board for this digital journey. They also want issues relating to gender, inclusivity and accessibility to be addressed, and assurance that children in vulnerable situations are also included. It's important to understand that online safety is a shared responsibility where industry also needs to be accountable. Member States cannot always address the risks that the private sector is creating, and this can result in perverse consequences.

We need to better train teachers and other professionals, and children want media literacy issues to be properly addressed. Currently, we are not educating children on what they want to be educated on; children need to be able to get answers from the adults that support them, instead of resorting to the internet for their education, for example in the area of sex and relationship education. By 2030, we need proper educational curricula and strategies built on child rights; this is critical for children’s safety, empowerment and wellbeing.

We also need to build on solid human rights legal frameworks and guidance, and ensure that the various standards that exist have been put into practice.

Child impact assessments need to be developed; this is not easy to implement but it is essential to ensure that the impact of new technology will not have an unwanted effect on children.

Children should not be object of legislation and policies, but they need to be involved in an age-appropriate manner, they should be heard and involved, and what they say needs to have an impact. We also need true leaders at State level who believe in children.

Regína concluded by quoting Einstein: “*Don’t listen to the person who has the answers, listen to the person who has the questions*”. Hence, we should be listening to children who are able to ask the right questions and tell us what we need to hear.

The EC consultation – an overview of findings

The recording from this session is available from www.betterinternetforkids.eu/sif.

Sabrina Vorbau, European Schoolnet hosted the first part of this session, focused on the findings from the #DigitalDecade4YOUth consultation, and introduced two representatives of the 2021 BIK Youth Panel. Frida from Finland and Francisco from Portugal explained the work which they have been doing with the BIK Youth Panel in recent months in terms of focusing in on some of the key themes from the consultation.

Frida's group worked on the topic of the importance of a better online school environment which has been particularly pertinent during the pandemic. Undoubtedly, it's been a time difficult for both students and teachers, but it's also provided opportunities. The group's video highlighted a range of issues from the right to access diverse, quality content; being equipped with digital literacy skills, and skilling teachers in this regard also; removing the digital divide; and mental health issues. Frida concluded that change must take place and that youth have a voice that must be heard.

Francisco's group focused on the topic of social networks and advertising and, especially, why our data is being collected. Social media is more and more engrained in our lives – in politics, economics, socialising. Some things are not done in the best way possible, and young people advocate change in this regard. The group's video raised questions over geolocation; the use of data online; the complexity of terms and conditions; and the importance of consent.

June Lowery-Kingston, Head of Unit Accessibility, Multilingualism and Safer Internet, DG CONNECT, European Commission then took the floor to chair two discussion panels – the first dealing with protection and the second dealing with empowerment.

The EC consultation – an overview of findings

Discussing the priorities that children and young people, and parents, carers and teachers, have identified in order to fulfil children's rights in a digital world.

Panel I
Protection

The role that different stakeholders need to play to make the internet a safer space for younger children.

Marta Kuljon
DG JUST

Alexandra Evans
TikTok

Kristina Krulić Kuzman
Centre for Missing and Exploited Children (Croatian SIC)

The first session included representatives from policy, industry and a Safer Internet Centre outlining their key priorities and actions for child protection online.

Marta Kuljon, Policy Assistant, Rights of the Child Team, DG JUST, European Commission stated that protection and empowerment are intrinsically linked. We need to examine the rights of the child online as they also apply offline. This has been highlighted in General Comment No. 25 as issued by the Committee on the Rights of the Child (CRC). She reflected on a comment from youth at the pre-event, that how you behave online depends on the offline environment you grow up in, and the types of relationships you have. She reiterated the point that just as in the offline world, the online world will never be completely safe.

Marta highlighted important factors which she believes contributes to creating a safe online space: knowledge, awareness, and creating space for dialogue and listening to each other, so supporting the arguments for effective child participation. A new EU children's participation platform is currently being developed. It will seek to bring together existing child participation mechanisms, to better learn from each other, to better listen to each other, and define – collectively – what needs to happen online and offline to make both environments safer and more fulfilling for children and young people. In responding to the general demand for more transparency and easier-to-read policies, the EC has published the EU Strategy on the Rights of the Child in child-friendly and accessible versions, created in collaboration with young people.

In conclusion, Marta hopes that such initiatives will help the EC to meet the call to action from children and young people, and ultimately create more accessible and digestible data, policy and legal documents that affect children's life.

Next up was **Alexandra Evans, Head of Child Safety Public Policy for Europe, TikTok** who provided an overview of what the platform is doing to keep its community safe. A key aspect of this is safety by design, which is particularly evident within the direct messaging tools which prevent images from being shared from off-platform, and limits unwanted contacts by only allowing mutual 'friends' to direct message each other. TikTok is committed to considering what it means to be a teen on the platform, and is aware that the need to balance issues of participation, empowerment and protection is critical. TikTok firmly believes that teens have the right to participation in the digital world, and that feeling safe is an essential prerequisite to full participation. Initiatives such as General Comment No. 25 and the UK's Age appropriate design code are welcomed and have given a renewed focus to this important work.

TikTok acknowledges that young users of the platform are still learning and growing, and hence also considers the additional support that will be needed: age appropriateness and a collective understanding of childhood and adolescent development is fundamental here. For under 16s, direct messaging is disabled by default, and for those aged 16-17, the default is off so that a conscious decision must be taken to permit messaging. Under 16s are not able to host livestreams, and users have to be 18 or over to receive virtual gifts on the platform. All accounts are private by default for those under 16, for both new and existing users.

TikTok also seeks to work with families: parents are the first line of defence and so the platform has invested in safety tools which allow parents to be involved. Once again, the balance of protection and empowerment is key here; it is absolutely not a monitoring approach, but aims to support teens in setting parameters for use in dialogue with their parents.

Alexandra concluded by stating that TikTok knows that there is no finish line to this work, but is trying to move forward as fast as it can to enhance its strategies. This includes proactive measures to keep children under the age of 13 off of the platform.

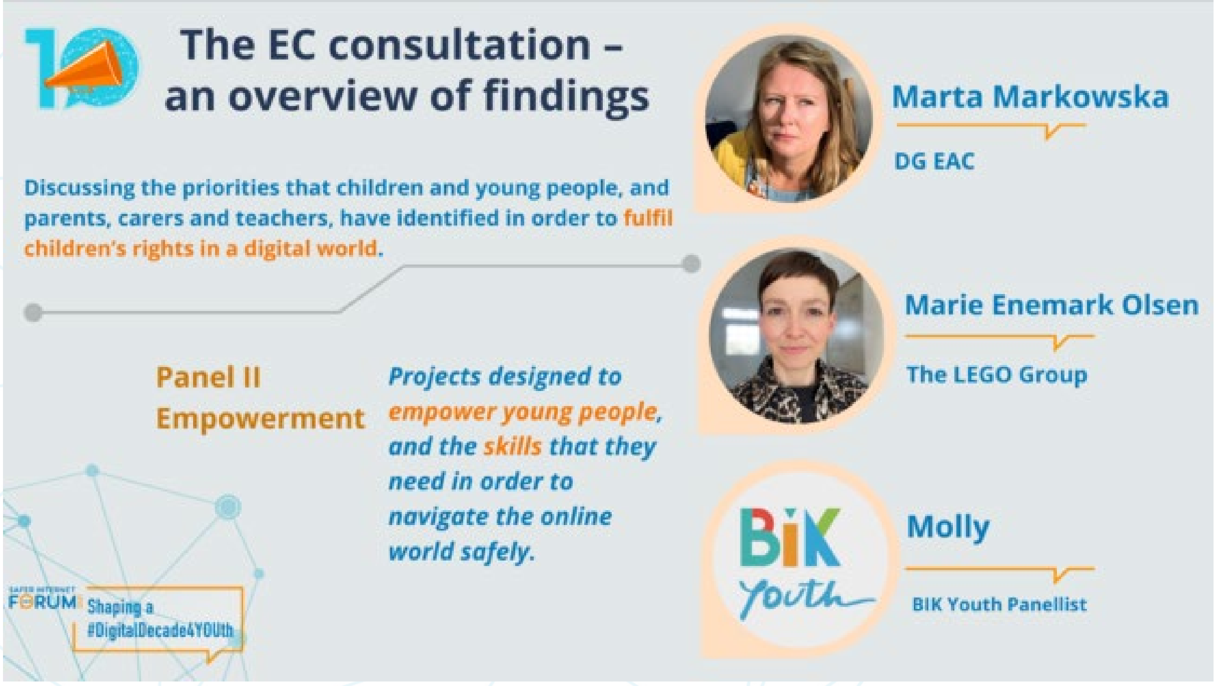
The last speaker of this panel was **Kristina Krulić Kuzman, Psychologist – Head of Expert Team, Center for Missing and Exploited Children, Croatia (Croatian Safer Internet Centre)** who began by giving an overview of the work of the organisation. It was originally established in 2006 with the main purpose of protecting children and youth in the online environment but, since then, its scope has significantly expanded to cover four main pillars of work: online safety; support regarding missing children and the national shelter for child victims of trafficking; provision of social services for children and families; and prevention programmes in fields such as violence and addiction among children and young people.

In the context of the online safety domain, the organisation provides helpline, hotline and awareness-raising services under the umbrella of the Croatian Safer Internet Centre. Through its work, the centre has noticed a growing trend in recent months of the impairment of health of children, often requiring psychological counselling and psychotherapy. Children and young people are presenting with a range of mental health challenges including anxiety, depression, suicidal thoughts, obsessive compulsive disorders, fears and behavioural issues. Clinical needs are therefore increasingly complex, and the level of interventions are more demanding. Unfortunately, the pandemic has made the situation more difficult.

In conclusion, Kristina stressed that the upcoming period will be especially challenging for all professionals involved in prevention and treatment. We need to further invest in awareness raising regarding risky online behaviours, media literacy and online safety. We need to develop more guidelines, more data protection policies, and more child-friendly materials. Furthermore, we need to ensure that new services and new materials for the protection of mental health for children and young people are available.

In bringing this panel to a close, June asked the speakers to summarise their ‘killer idea’ for change in this space:

- Marta would like to focus on making the online world accessible for all children and young people, irrespective of a range of physical and social factors. Aligned with this is ‘mental accessibility’ of adults, for them to be open to new experiences online and interact with their children in discovering these.
- Alexandra would like to focus on the alignment of content and services to truly meet the needs of children and young people, commenting that the balance between empowerment and protection changes depending on the capacity of the individual child. Young people need to be front and centre in the conversations on how to design digital environments which do not infantilise them, but equally we must not expect them to behave like adults.
- Kristina’s wish is for every child to enter the online world with the adequate knowledge and skills about online safety, risky behaviours online, their rights online, and who to contact in case help is needed.



The EC consultation – an overview of findings

Discussing the priorities that children and young people, and parents, carers and teachers, have identified in order to fulfil children's rights in a digital world.

Panel II Empowerment

Projects designed to empower young people, and the skills that they need in order to navigate the online world safely.

Marta Markowska
DG EAC

Marie Enemark Olsen
The LEGO Group

Molly
BIK Youth Panellist

Moving on to focus on empowerment in the second panel, June asked the speakers in this session to similarly provide an overview of their priorities in this space.

Marta Markowska, Policy Officer for Digital Education, DG EAC, European Commission kicked off the session by commenting that discussions over recent days speak volumes about the reality of the digital world and the digital space with live in, but also the challenge areas which need to be bought back into the policy domain. We need to acknowledge the fact that younger people play a pivotal role in shaping and leading our digital societies. It's crucial that we provide education and training, and help them to find their voice to see how best they can make a positive contribution to our societies through digital citizenship and empowerment. We know that opportunities online are limitless, but we also need to be mindful of the challenges and threats they encounter be they tackling disinformation, cyberbullying, or online radicalisation. It is our responsibility as policy makers, educators, parents, and wider society to keep our young people safe and empowered online.

Marta went on to outline some of the aims of the Digital Education Action Plan (DEAP) as adopted by the European Commission in September 2020. This essentially provides an ambitious vision for the roll out of high-quality digital education that is accessible, inclusive, and available to all learners across Europe. One of the priorities focuses on strengthening the digital skills and competences of children and young people, and this is where the empowerment dimension comes in. Digital literacy is key here – helping young people to access, create and share information, alongside supporting them to become both confident and critical users of what they see online will facilitate positive online experiences.

We know there is a clear demand for digital literacy skills. Eurobarometer data from 2020 indicates that 40 per cent of young users think that media and digital literacy is not taught sufficiently in school. The DEAP has a specific action on this, aiming to develop guidelines for teachers and educators on how to promote digital literacy and tackle disinformation. The guidance will be pedagogically sound and practical, and is being shaped by a wide-ranging expert group. The guidelines will be adopted in September 2022 as part of a ‘back to school’ initiative. Similar actions are taking place in various programmes such as Erasmus and eTwinning, so evidencing a bottom-up mobilisation of education and training to promote digital literacy.

Next, **Marie Enemark Olsen, Director, Responsible Child Engagement, The LEGO Group**, provided an overview of the organisation’s actions in this space. The Lego Group’s mission is to inspire and develop the builders of tomorrow and, as such, the company regards children as role models. This is applicable within both online and offline play experiences. Lego acknowledges the potential that technology can have in contributing to children’s rights and wellbeing, but this is only the case if the focus is on children’s needs and interests, and if experiences are designed around this.

Lego works with partners such as UNICEF to advocate for children’s rights in business principles and to develop best practice tools for online safety. A further important partnership is with DQ Institute, a world-leading think tank on digital citizenship and online safety. Together they are working to equip children and families with the knowledge and skills they need to thrive in the online world. As a result, some new interactive skill-building experiences, for both children and their parents, have recently been launched.

In closing, Marie commented that the core concept within The Lego Group is safety by design. However, building safe experiences is not enough – we need to also focus on empowerment such as skill building.

BIK Youth Panellist Mollie then gave her insights on what empowerment of young people online means to her. Children and young people are constantly being told that online is important, but education on this topic is barely provided. They feel disempowered as a result. Peer education programmes might be a good way forward here to empower young users.

Equally, policies need to be improved – children and young people just accept terms and conditions by default, as they are too complex to unpick. In doing so however, they have no comprehension of how their data can and will be used. This is a huge problem. Policies need to be simplified, for the benefit of both the user and platforms (for example, in terms of removing content). This will ultimately give the user more power.

Cyberbullying is a growing issue, causing children and young people to feel very vulnerable. Policies to protect against hate online need to be made stricter, and response times improved for removal of problematic content. Mollie concluded by making a plea that we all work on these issues together.

An additional panellist, **Giuliano De Luca**, spoke from the educator perspective. He began by reminding us that technology and the internet are nothing but tools, and like any tool, they have great potential, but also present some risk. We need to be able to provide correct information to children and young people on how they can use these tools safely and responsibly.

Digital literacy must become a cornerstone of education; there is currently a lack of training. Students – and educators –often just receive a single training lesson, and there is lack of continuity. Digital education needs to become a mandatory subject in every school, and we need to increase the role of digital educators. We also need to create structured and uniform training paths across

Europe, and we need to start to report on the results obtained. This will help to ensure that the correct follow up is provided, and that future resources are directed in the correct way.

Once again, June asked the panellists to wrap up the session with their single wish for the future:

- Marta commented that there is one message for education; we cannot consider it obvious that youth are digitally literate and digital natives from birth. We need to look at critical thinking and what it means to be digitally involved. We have a collective responsibility to provide formal learning, informal learning, parental engagement, and so on. We need to shape the future together, and a large conversation needs to take place.
- Marie stated that we can change the future by designing for child rights. We need to empower and protect, but we also need to think about impact and risks on children. There is collective responsibility. We need to not only provide safe platforms, but also empower and teach children when they are using them.
- Mollie wants a future with less hate. Children and young people often don’t understand the impact of words and the potential consequences, and this comes down to protection and age limits. Online hate and cyberbullying can lead to mental health issues, hence it is critical to address this.
- Giuliano hopes that we will find a way to block access to dangerous content. We will undoubtedly see the impact of young people being able to access harmful content in the coming years. Young people are growing up with a distorted image of society in terms of issues such as respect, gender, and relationships, and this needs to be addressed now.

Deep dive sessions

DD1: Age-appropriate design and the role of age assurance/verification

The recording from this session is available from www.betterinternetforkids.eu/sif.

The first of the Forum's deep dive sessions focused on the importance of age-appropriate design and the role that age verification and age assurance has to play in that.

Deep Dive Session 1

SAFER INTERNET FORUM 2021

Age-appropriate design and the role of age assurance/verification

Speakers:

Professor Simone van der Hof
Academic Director, Professor of Law and Digital Technologies, Leiden University

Almudena Lara
Child Safety Global Lead, Google

Better Internet for Kids

The subject of age-appropriate design and age verification had already been touched upon in earlier SIF 2021 sessions, as well as during the consultation exercises with children, young people and teachers. It is also one of the four pillars of the Better Internet for Kids Strategy. The concept of age-appropriate design includes having appropriate privacy settings that do not put young children at risk and avoids situations in which they would inadvertently agree to privacy setting without understanding the implications. Inappropriate privacy settings may put children or young people at greater risk online, for instance as easier targets for grooming or threats to their online reputation. Therefore, default privacy settings for children should be systematically arranged, privacy-friendly electronic identification methods used when users create profiles and accounts, default age-appropriate designs implemented, and clear warnings about adverse consequences linked to accessing platforms or content should be received by the user. The collaboration between industry and various actors and users is key in order to implement the latter elements in the best possible way. Two speakers were invited to present their know-how, views and experience of age-appropriate design and age verification.

Professor Simone van der Hof is Academic Director, Professor of Law and Digital Technologies, at Leiden University in The Netherlands. She is currently involved in the euCONSENT project (Electronic Identification and Trust Services for Children in Europe) which is an initiative of the Dutch Ministry of the Interior and Kingdom related to behavioural design in games. This comes in addition to her teaching activities on children's rights and digital technologies, and various activities as part of expert groups and committees. Touching upon some of the results of this work during her presentation, Professor van der Hof highlighted the difference between age-appropriate design and age verification; age verification being applicable when there is a legal obligation to shield children and young people from harmful content and practices too mature for their age, whereas age-appropriate design is wider in scope. Indeed, age verification can contribute to age-appropriate design but may not be enough to make a technology or application age appropriate. Additionally, the implementation of age verification must be done in an age-appropriate way and must respect the rights of children and other users.

Professor van der Hof provided some examples of where age verification can be a legal obligation. Firstly, it is worth noting that there is no general legal obligation for digital service providers to verify the age of their users, but that is not to say they do not have a duty of care to provide a secure service, especially for children and young people. However, the law does require the implementation of age verification in certain circumstances, and this can vary from country to country. In general, provisions cover the following:

- Harmful content (for example, violent porn and advertising): Age verification is typically a requirement in the EU for 18+ plus content, but what constitutes 18+ content may differ from country to country, and there are distinct cultural differences also. Video sharing platforms need to comply with the EU's Audiovisual Media Services Directive (AVMSD) and age verification has been listed as one of the appropriate ways of protecting young users against content that is not suited to their age group.

- Harmful services (such as gambling): the minimum age differs from 16 to 21 for countries in EU, and for gambling, for example, age verification is not the only measure that has to be implemented. It comes together with other measures to restrict the targeting of children or young adults with adverts. Some laws also require registration of customers in order to provide support if they subsequently show problematic behavior. Some countries have rules related to which age verification methods need to be used, or an obligation to report which method is used by a company.

- Restricted goods (such as alcohol, tobacco): there are different age limits established across Europe for the consumption and sale of these products, which are also available for sale online. While age verification may be required online, age verification can also take place when the product is delivered to someone's house or location. However, research shows that age verification rules are rarely applied and respected for restricted goods.

Alongside age verification measures, some countries also use age classification to give parents and children the possibility to avoid viewing potentially harmful content. This method also considers the fact that not all children are the same; what might be harmful to one child may be appreciated or enjoyed by others. Parents, therefore, have the opportunity to make their own decisions, preferably in consultation with their own children. In this regard, age classification is often seen as advisory rather than mandatory.

A further tool is parental control systems whereby parents are given the opportunity to set limits on what their children can see, based on individual profiles. This gives parents flexibility in deciding if content or services are appropriate for their children. This also supports the notion that parents are the primary responsible for their children. However, it should be noted that such tools can create a false sense of security as they do not address any and all risks that children can encounter in the digital environment. Professor van der Hof noted that encountering some risk online is not necessarily a bad thing, especially if children have a supportive environment that can help increase their resilience rather than cause harm.

While there is no general obligation for service providers to verify the age of their users, the GDPR (General Data Protection Regulation) changes things somewhat as it aims to provide a high level of protection for all children. While the GDPR does not have an explicit requirement for age verification, there is an implicit requirement to verify the age of data subjects as it aims to provide a high level of data protection for children and anyone under 18. If a data subject says they are under 18, then this can be taken as a given and there is no need to verify age; the data subject can simply be provided with a high level of protection. However, if the data subject says they are over 18, you would need to verify that this person is not actually a child. The high level of protection for children is explicit in some parts of the GDPR and more implicit in others. It is, for instance, explicit in terms of transparency provisions requiring the use of simple language in data privacy statements or in terms of avoiding profiling when not in the best interests of children.

Article 8 of the GDPR on the age of digital consent (and parental consent in cases where children have not yet reached the age of digital consent) is also significant here. The Article only applies when the lawful basis for data processing is consent rather than another legal basis. It is however an important provision; it mentions that if there is no age verification, and that the legal ground for processing data is consent, there can be legal consequences for entities who ask the consent of children too young to legally provide consent in the first place.

The euCONSENT project highlighted the fact that it is very difficult in practice to ensure that a person is truly the legal guardian of a person, and especially to do this in a privacy-friendly way. Hence, the project investigated if parental consent methods could be replaced by age verification, ensuring for instance that the age of the person giving the consent for the child is significantly higher than the child's age to be valid.

Staying in the context of the GDPR, the euCONSENT project also looked at various applications and games to evaluate what was currently implemented for age verification. Most applications and games used self-declaration, that is providing a date of birth to verify age. This is an issue as it is easy to get around such a system by giving a wrong date of birth. Some platforms also used consent as a legal basis. This is also an issue since, if you are under the age of digital consent, there is an incentive to lie about your age to not be excluded. This creates situations in which data processing becomes unlawful as consent cannot be given by a data subject under the age of digital consent.

The conclusion is that from a GDPR point of view, self-declaration is not an adequate age verification method as processing data from children is considered to be high-risk, and responsibility is placed on the child. According to the GDPR, it is the implicit legal obligation and responsibility of digital platforms, not children or parents, to secure their high-risk data processing activities and to protect vulnerable data subjects.

Age verification methods providing a higher assurance than self-declaration methods are therefore required. However, age verification should not lead to the processing of more data than necessary. If an entity collects traditional ID documents to check the age of users than this process leads to the provision of more personal data than just the date of birth, and hence too much data. Equally, it is often only necessary to check the range of age of the user at the time of registration, not their specific date of birth. The provision of traditional ID documents is also not a suitable age verification method; ID documents which are suited to digital identification and to the digital world should be developed.

Age verification methods must be privacy preserving, anonymous, and based on privacy by design and default. For instance, age verification could take place on the device of the user, in which case the platform would get a 'yes or no' type of answer but no data. The drawback of applying this method would be that this requires a database to centralise all of the information from users, which could subsequently be the focus of attacks. Hence, security measures would need to be state of the art.

Aside from being privacy friendly, age verification methods should be age appropriate (child-friendly) by design. Children must understand what is being collected and why, and be able to predict what information will later be visible or not online. For example, users may consent to their city of residence being collected, but not explicitly consent to this data being later automatically displayed on their profile.

Age verification methods should also be proportionate and effective, while not excluding children or invading their privacy. Child impact assessments can be carried out to see how different verification methods affect the rights of children but also to address concerns that children or parents may have, and to implement safeguards. Those types of assessments should not be a one-off exercise but should be conducted at regular intervals, as age verification methods may undergo regular adjustments. Not every child is at the same stage of development or equal in terms of their cognitive or physical situation. Parents may also be in different positions when it comes to supporting their children; for example, they may be tech savvy or not. Parents and children must also be able to get support or be able to report if they encounter issues with an age verification method.

In conclusion, age appropriateness does not simply mean implementing an age verification method. When age verification is legally required or implemented it must be done in a way that is age appropriate and should take into account the specific rights of children, including in terms of data privacy as vulnerable data subjects.

Almudena Lara, global lead in child safety at Google has worked with regulators, civil society and tech companies. She explained that we need to develop, together, age-appropriate solutions allowing the safe participation of children and, in doing so, we need to collectively work with parents, regulators, tech companies and civil society. As a society, we need to explore various scenarios as each situation requires some trade-offs; it's important to find a trade-off with which we are all comfortable. Protecting children and allowing them to actively participate in the online world is sometimes seen as being in conflict, and it is important to find an adequate balance in terms of allowing them to be online but also putting adequate safeguards and limits in place.

In terms of the age verification debate, it is important to consider that part of the solution may be to design experiences which are great for children. To gate children out of adult experiences is needed but as long as there are no children-appropriate solutions which can bring equally high-quality experiences to children, children will try to bypass these systems.

Google has a programme to support children in terms of digital literacy (as well as teachers and parents), and have experiences specifically designed for young children. Supervised experiences have also now launched on YouTube, for example. The experience offers three 'buckets' of content that parents can choose from with protection mechanisms for children, such as chat and content creation functions being switched off to create a safer experience online.

The Family Link platform was designed with the objective of letting parents stay in the loop and set some digital ground rules as their children or teens explore the online world. This can potentially help families build healthier digital habits together.

In terms of what is available to children, there are a set of Google experiences for users under the age of 18. Accounts should only be created from when the child has reached the age of digital consent. There are also special features for children above the age of digital consent but under 18 in the form of a safe search feature, with location and personalised ad features being disabled.

When discussing age assurance methods, a large part of the debate comes down to this question: how do we know if we have a child using certain services? There is currently no perfect one-size-fits-all solution in response to this question and the underlying need, and so companies are collectively discussing and consulting with different types of actors to find an appropriate method to detect if the user is a child.

The current method of identification is as follows; there is an age screen for signing in users where a date of birth is requested and users cannot correct that date later on. If the user enters a date under the age of digital consent; they will be directed to the Family Link app and asked to create a supervised account with parental support. If they are above the age of consent but under 18 years old, they are directed towards the more secure experience for minors for which different settings – including privacy settings – are applied by default.

The roll out of a new system has also started in Europe to assess the type of user. Hence, once users are signed in and use the system, the system will make use of machine learning and algorithms to assess if the user is a child or adult. This is based on information such as the longevity of the account, type of searches made, or category of videos the user has watched. Should a user be put in minor mode, he or she will be notified. However, this type of system is a new territory that needs further exploration from Google and other industry players. In case of system failure, if a user has been misclassified, there are means to report this to Google. Additionally, if a user is put in minor mode, and wants to see 18+ content, they have an opportunity to prove they are an adult user using their traditional ID or credit card.

Almudena concluded her presentation by summarising what makes a good age assurance method:

- Proportionality: The age verification method should be proportionate to the risk children are faced with when using the service or accessing the content.
- Data minimisation and purpose limitation: There is the need to ensure that the system preserves privacy and that it does not collect unnecessary data.
- User friendliness and inclusivity: Experience shows that users abandon a service or will try to circumvent a system that is not user friendly. When it comes to inclusivity, we should consider that age verification methods involving the collection of traditional ID or face

recognition may be less attractive for children from the LGBTQ+ community, for example, who may not want their gender or identity divulged. Hence, a company or platform may need to use a number of different methods in parallel to ensure inclusivity.

- Trust: More transparency regarding how the data is shared, used, collected, stored and deleted is needed. How companies can build the trust necessary to be more transparent, and how society and governments can support this process, should be a key element of focus.
- Collaboration: Cross-industry collaboration is required to find adequate final solutions. A very centralised solution may cause various issues, including in terms of security. However, dealing with many collaborators may challenge the user-friendliness of a method.

DD2: New and emerging tech

The recording and presentation from this session is available from www.betterinternetforkids.eu/sif.

The second Deep Dive session considered some of the new and emerging technologies that we are likely to see over the next decade, and the challenges and risks they bring with them.

Deep Dive Session 2

New and emerging tech

Speaker:

Dr Victoria Baines
Visiting Fellow, Bournemouth University,
United Kingdom

Dr Victoria Baines, Visiting Fellow, Bournemouth University, United Kingdom, is a researcher whose work focuses on online safety policy and the future of cybercrime. During this session, she presented an overview about future scenarios and developments of new technologies, focusing especially on the opportunities and challenges to be expected in the next 10 years.

In 2012, she prepared a special exercise in the framework of Project 2020 which explored future predictable developments of new technologies for 2020. Main concerns at that time were around cybersecurity and criminal misuse. More recently, she has been rerunning that exercise independently with Trend Micro, a cybersecurity company, for 2030. In both cases the so called 'Gartner Hype Cycle for Emerging Technologies' was used; a baseline that helps to identify which year a technology will be ready and when it will become mainstream.

Dr Baines presented the technologies that will be of greatest interest for children's online safety in the coming years: artificial intelligence (AI), which will be plugged into pretty much everything, in both online and offline activities (for example, smart city technologies, Internet of Things, smart technologies, energy distribution); Next-Gen Persuasive Computing, which means the use of machines to affect changes in our perceptions, or behavioural changes; and immersive environments (XR), such as virtual reality (VR) and augmented reality (AR).

By actively interacting with the younger participants present in this session (from the BIK Youth Panel), Dr Baines raised various ethical and legal issues regarding the increasing use of AI on the internet (for example, the creation of images of fake people, and of images depicting child abuse of fake children). One of the main questions is what these fake images and related crimes constitute legally and ethically, and how countries and authorities should punish and prevent the spread of such images or the criminal use of AI. In the next few years, we will see more and more of these images; as these generative adversarial networks get smarter, we will see an enhancement of certain fake images resembling real images.

The term AI is often considered a bit 'loose' due to the fact that the hype around AI has grown enormously of late. In fact, AI is often confused with just machine learning (ML) or automation (such as that used in social media). But what is expected in terms of future AI developments is the growth of algorithms and machines that are truly capable of learning and increasingly replacing humans.

AI concepts are widely applied in everything related to internet safety, and companies increasingly rely on automation for safety issues. Dr Baines affirmed that we can hopefully foresee an increasing use of automation to improve safety issues, especially for children, on the internet. In the cybercrime world, this has already happened to an extent (for example, in spam detection being automated or for identifying online grooming). AI can help when human presence is not enough in order to guarantee a constant high level of safety when using the internet. In particular, AI will bring opportunities for live non-human support to children and young people who need help, when human support cannot be provided.

Another important issue raised by Dr Baines is the need for AI to require larger data sets in the future to be more effective. She highlighted the fact that AI and machines require large data sets to be effective and to learn accurately, but this raises key ethical questions. If we accept that we may need to collect more personal data from children in order to keep them safe, what are the limits to that and who would set them? Authorities should also address the question of who and how should explain AI to the public. For example, is it the role of the education system, data protection authorities, the company using it, or another body entirely?

The session also addressed concerns around the fact that machines may gradually take over many activities that humans have usually performed, as has happened in recent years for data collection and analysis (such as AI collection and analysis of Big Data). Nevertheless, Dr Baines pointed out that, luckily, machines still do not have – and will unlikely ever have – the irreplaceable skills of human intuition and critical thinking, which are often fundamental in tracking down scams or frauds. Even though we are already at a point where many artificial assistants (such as Google or Amazon's Alexa) are providing us with some help and taking over some of our functions, AI still lacks the ability to understand when something is wrong.

The second emerging technology addressed in the session was that of persuasive computing and its relationship with internet safety education programmes. In the next few years, the use of digital technologies to affect perception change and behaviour change will increase. When we develop internet safety programmes, one of the main goals is to prevent adverse experiences for children. In the future, the ability to change this perception of children, and even their behaviour, will be stronger. Equally, the opportunity to change the behaviour of those who may pose a danger or threat to children is also likely to increase. The question that arises from these future developments is whether we need new transparency and accountability measures, and alternative methods, if our education and intervention tools become more persuasive.

The third technology that will see important future developments in this field is extended reality (XR) and immersive environments. Research has shown that what we experience in XR leads to an increased emotional impact, and this can be both positive or negative. Currently much work is being invested in this technology to increase the so-called haptic feedback to people; that is, the impression of feeling physically there when using XR. On the positive side, this can enable people to feel more confident or powerful in the online environment; on the more negative side, it may also lead to people no longer wanting to leave these environments. One of the positive examples where XR has been used is to generate empathy for others (for example, refugees and trafficking victims, or victims of bullying). We must also consider the implications of the extensive use of virtual reality on critical thinking; it’s essential to ensure that future generations maintain the same level of critical thinking ability, also for their own defence.

Dr Baines concluded her intervention by talking briefly about brain-machine interfaces (BMIs). Even though medical uses already exist, mainstream use of bi-directional interfaces that both capture data from the brain and transmit data to it will probably not be mainstreamed in the next decade. While such technology can be used to challenge the thinking of people, and perhaps even persuade them (with some positive uses predicted in, for example, the treatment of severe depression), the potential risk for misuse is immense.

The results of research presented by Dr Baines can be found in the White Paper Project 2030: Scenarios for the Future of Cybersecurity.

The floor was then opened to questions, a selection of which follow:

Molly from Ireland asked if robots could help people who have issues expressing their feeling in schools or other public environments. Dr Baines replied that AI could certainly be used in schools to support pupils with disabilities or who are experiencing particular issues, or used in helpline settings to make up for human absence (for example, outside of operating hours). AI can also be used with people with dementia or Alzheimer's disease to allow them to feel more confident and comfortable in expressing themselves.

Mico from Finland asked if there will be a backlash in the trend enabling more and more digital manipulation. Dr Baines affirmed that tech companies have a responsibility to deal with manipulation of information. However, the more that tech companies use tools to tackle this, the less we’re going to use our critical thinking, which is a negative effect. Dr Baines believes that we need to keep on training people to use and improve their critical thinking to actually tackle issues such as the manipulation of information, the spread of fake news, and so on.

Finally, one participant asked if there will be more plans for AI after 2030. Dr Baines thinks that 2030 will not be an endpoint for AI. That raises important questions about who is going to regulate that, and ethical use of AI.

Dr Baines concluded the session by affirming that even though she has fears about the future development of new technologies, she is hopeful that the same technologies will actually be able to tackle many of the challenges and ultimately provide a better online experience for children and young people.

DD3: Child sexual abuse material (CSAM)

This session, led by INHOPE (The International Association of Internet Hotlines) focused on the ongoing work to eradicate child sexual abuse material (CSAM) online, showcasing the latest technological advances as well as the most up-to-date research.

Deep Dive Session 3

SAFER INTERNET FORUM 2021

Child sexual abuse material (CSAM)

Speakers:

Denton Howard
Executive Director, INHOPE

Cathrin Bauer-Bulst
Head of Unit, Security in the Digital Age, DG HOME, EC

Ruben Roex
Attorney, Timelex

Dave Miles
Head of Safety – Europe, Middle East and Africa, Facebook

Arda Gerkens
CEO, Expertisebureau Online Kindermisbruik (EOKM) (Dutch Safer Internet Centre)

Better Internet for Kids

This session was conducted under Chatham House Rule and hence a session recording is not available. Equally, participants were asked not to reveal the identity nor the affiliation of the speakers in any external communication. For further information, please contact INHOPE direct.

The first speaker of the session was **Cathrin Bauer-Bulst, Head of Unit, Security in the Digital Age, DG HOME, European Commission**. Cathrin set the scene for the session by presenting the problem and the possible solutions to the challenges.

Child sexual abuse has two elements: an online and an offline aspect. Where the abuse takes place offline, in the majority of cases it is committed by someone very close to the child. The online component has two aspects to tackle: 1) the offenders take pictures and/or videos of the abuse and use it to relive the experience and share it with others, and 2) offenders have access to children and high potential to contact new potential victims through the internet. The second is seen in many cases where offenders pretend to be peers of a child and flatter the children to the point that they are coerced into abuse. In both cases, even when the children are rescued, the images continue to circulate on the internet which is very traumatic for the victims.

The focus of the session was specifically on child sexual abuse material (CSAM); that is, images and videos of child sexual abuse available on the internet. The European Commission is making serious steps and investments to ensure that CSAM is detected whenever it is made available online and that the children depicted in this material are rescued. Cathrin presented two ways of identifying this material online: 1) accidental finds by citizens who stumble upon this content and then report it to an INHOPE hotline (which will consequently take action to remove the material from the internet) and 2) systematic proactive detection by internet companies which take a positive approach to keeping their platforms clean and therefore aim to detect whenever CSAM is posted. Cathrin differentiated between material that has already been classified as illegal – known images and videos, and new (or previously unseen) material which can be sorted into the relevant category by use of hash matching technologies.

New material can be detected with tools that incorporate AI (artificial intelligence) and machine learning (ML) which learn from previous classified CSAM examples and identified patterns. These methods appear to result in extremely low error rates. Cathrin flagged that US companies report CSAM to NCMEC (National Center for Missing & Exploited Children), which consequently shares those reports with law enforcement agencies worldwide. She gave an example of her own region – North Rhine-Westphalia – where more than 1,800 suspects have been identified and more than 70 children have been rescued as a result of NCMEC reports. However, only a handful of companies send reports and, last year, 90 per cent of these reports came solely from Facebook. She stated that there is clearly a cost factor for companies when it comes to detecting and reporting CSAM, and equally some companies refrain from doing it because it might draw negative attention to their company. There is also a fear that if a company starts identifying CSAM by building and deploying tools for its detection, that those tools might be used for other purposes. Cathrin pointed out that these concerns must be addressed so that companies can detect and remove CSAM in a swift manner.

Cathrin closed her presentation by stating that the EU has committed to create a clear legal framework to better protect children. This will be done by strengthening companies' roles and creating systems to support victims better, so they do not have to rely on accidental finds of their abuse images online.

Denton Howard, Executive Director of INHOPE continued the session by providing an overview of INHOPE and ICCAM (a secure technology platform that allows INHOPE member hotlines to streamline report processing, increase productivity and efficiency, and minimise the amount of CSAM that analysts are exposed to). He provided a brief non-technical introduction into what automated detection of CSAM online means, and how it can be achieved. He also explained that companies can detect CSAM without actually looking at the content, which is key when it comes to privacy. This is where hashes play a significant role. Denton explained the concepts of hashes, the different types, how they are deployed and the importance of accuracy/quality control with regard to hashes. He concluded by reiterated Cathrin's point that there must be boundaries when using these tools, and that they should be solely used for the detection of CSAM and not for other purposes.

The next speaker, **Ruben Roex, an Attorney at Timelex**, presented automated detection from a legal perspective and highlighted the importance of scoping when one does an analysis of hash sharing with the GDPR (General Data Protection Regulation). He set the scene by making a distinction between the different activities when it comes to CSAM detection online, and explained that there is a difference between automated detection by private sector services versus sharing hashes between different parties. When it comes to automated detection, several legal instruments apply which would not typically apply to sharing hashes (regulated solely by GDPR). He advised that when we talk about sharing hashes, we must presume that the hashes have been created in a compliant manner in the first place (that is, in accordance with GDPR).

Ruben stated that GDPR contains rules on the processing of personal data, and for each processing activity, and that there must be a purpose. Each purpose must have a legal basis (and possibly also an exception). It is important to consider that what GDPR tries to govern and regulate is the processing of personal data. GDPR requires a granular analysis and breaking up of all processing activities to consequently identify the purpose of the processing and a corresponding legal basis for it. The purpose of fighting CSAM online in this case is very broad. The purpose of sharing hashes is the specific activity of detection, as well as notice and takedown (NTD). It is also important to note that a hash value does not qualify as a special category of data. Images and video are considered personal data. Personal data cannot be seen from a hash value.

The legal basis to share hashes under GDPR falls under two articles:

1. Legal obligation (Art. 6.1.c GDPR): applies to tasks carried out in the public interest which must be included in the law.
2. Legitimate interest (Art. 6.1.f GDPR): which defines different possible legal basis and possible scenarios.

A four-step test is required to define the legitimate interest:

1. *What is the interest, what makes it legitimate?*
   Protection of children, fraud prevention, or even general interest can be considered as legitimate.
2. *What is the impact on data subjects?*
   The interests of victims and perpetrators should be taken into consideration while keeping in mind that it is a processing activity of pseudonymised hashes. If the hash value is wrong, the impact on the data subject can be profound, but we have to keep in mind that we are trying to protect children.
3. *What is the provisional balance?*
   There are threats of false positives when comparing hash sets. Data proliferation and retention also plays a role, as well as oversight and security.
4. *Additional safeguards?*
   Many safeguards can be introduced in practice to invoke the legitimate interest. This can be done by data verification by authorised sources, providing only access rather than copies of data, and setting specific governance structures.

In his closing remarks, Ruben emphasised the importance of pseudonymisation and anonymisation when sharing hashes. A hash is highly pseudonymised which is not the same as anonymised. A link can be drawn between the data subject and the hash if one has additional data which can be linked to the hash. For instance, a company can link a particular hash to a particular individual. This additional data must be kept separate by the data controller. The pseudonymisation strengthens the legitimate interest argument.

The next presenter, **Dave Miles, Head of Safety – Europe, Middle East and Africa, Facebook**, presented how detection of CSAM is implemented in practice at Facebook. He emphasised that Facebook has zero tolerance to CSAM on its platform and therefore the company does everything to proactively and aggressively remove it. A huge team of trained specialists review and remove the material. Detection is only one pillar of Facebook's efforts; prevention and response play a large part too, and it provides victim support and reporting options to its users. In 2020, Facebook removed more than 20 million images following on from NCMEC cyber tips; 99 per cent of this material was removed before anyone even reported it.

Facebook conducted an analysis on the material it reported to NCMEC in October 2020. More than 90 per cent was the same or similar, and copies of just six images were continuously being reshared. Facebook is consequently developing new targeted, evidence-based solutions based on the analysis.

Facebook conducts different activities to prevent and support, with one example being a pop-up when someone searches a CSAM-related term which gives information on organisations providing help to offenders. The pop-up also explains the legal consequences for sharing. Currently, Facebook is running a 'Don't share' campaign which has been reducing the rate of harmful content in Latin America, Africa and Asia. Facebook also makes transparency and accountability a priority, to create conditions where everyone has a voice. Facebook's Community Standards show what is not allowed in terms of safety, privacy and dignity. Since 2018, Facebook has published reports which document the changes they have made to child endangerment policies.

Dave also emphasised the value of partnerships for Facebook and the role of their Safety Advisory Board. Facebook is committed to educating people on how to stay safe online and is industry-leading in building best internal systems. Facebook was an early adopter of PhotoDNA and use classifiers to detect new potential CSAM, and especially interactions between adults and children. Facebook has also open sourced its video matching technology. Facebook is part of the Technology Coalition, the WePROTECT Global Alliance, and many others.

As additional presenter, **Annie Mullins, Online Safety Consultant at Yubo**, presented on CSAM detection on this livestreaming platform for generation Z. Yubo is a French company, and is just five years old. It uses the Internet Watch Foundation's (IWF) and NCMEC's filtering hashes to detect any CSAM on the platform. However, Annie pointed out that Yubo is a livestreaming app where children come to meet and talk in small groups, and it is very important to realise that safety on the Yubo platform is different than other platforms. Subsequently, the abuse detection tools are also different. Yubo takes screenshots of the livestreams every 10 seconds to detect nudity (even topless boys are not allowed). Children are often not aware that someone can screenshot them and blackmail them afterwards. This is how Yubo focuses on prevention rather than action.

Yubo also has live intervention on the app, where if the algorithm picks up a nude, a moderator is alerted, and the young person will be informed that they have one minute to rectify the situation otherwise the stream will be closed. Yubo notices that its community responds well to this, and the users tend to 'police' each other: "*don't do that because they will stop the stream*". Other measures include detection and checking of profile pictures of young people, and Yubo uses an API from Google to cross check any Google-removed images. Yubo also tries to pick up on other signals such as the bio or registration age of a user using age verification in collaboration with Yoti. If a user registers as being under 18, then they are kept in that bracket; that is, adults can only socialise with other adults, while kids cans only socialise with other kids. Yubo has an agreement for dual reporting, so it reports to both the French police and NCMEC.

The final presenter of the session was **Arda Gerkens, CEO, Expertisebureau Online Kindermisbruik (EOKM) (Dutch Safer Internet Centre)** who presented on the swift removal of CSAM by enhancing cooperation between local enforcement agencies (LEAs) and industry. EOKM is currently running a research project in collaboration with PricewaterhouseCoopers from April 2021 to June 2022 with the intention of identifying whether it is possible to create a hash database and build a proof of concept. The research looks at six different fields of interest:

1. Technical attributes of existing data sets of CSAM.
2. Data governance, quality control and protection processes.
3. Third-party engagements.
4. System used in CSAM classification.
5. Database-related legislation.
6. CSAM-related legislation.

The technical attributes of existing data sets are the purpose of the data set (investigation, notice and takedown (NTD), ensuring clean service and/or data sharing); the type of sets (illegal and exploitative data); hashing language (SHA-1, SHA-2, MD-5, Photo DNA); and the rate of growth of the data sets.

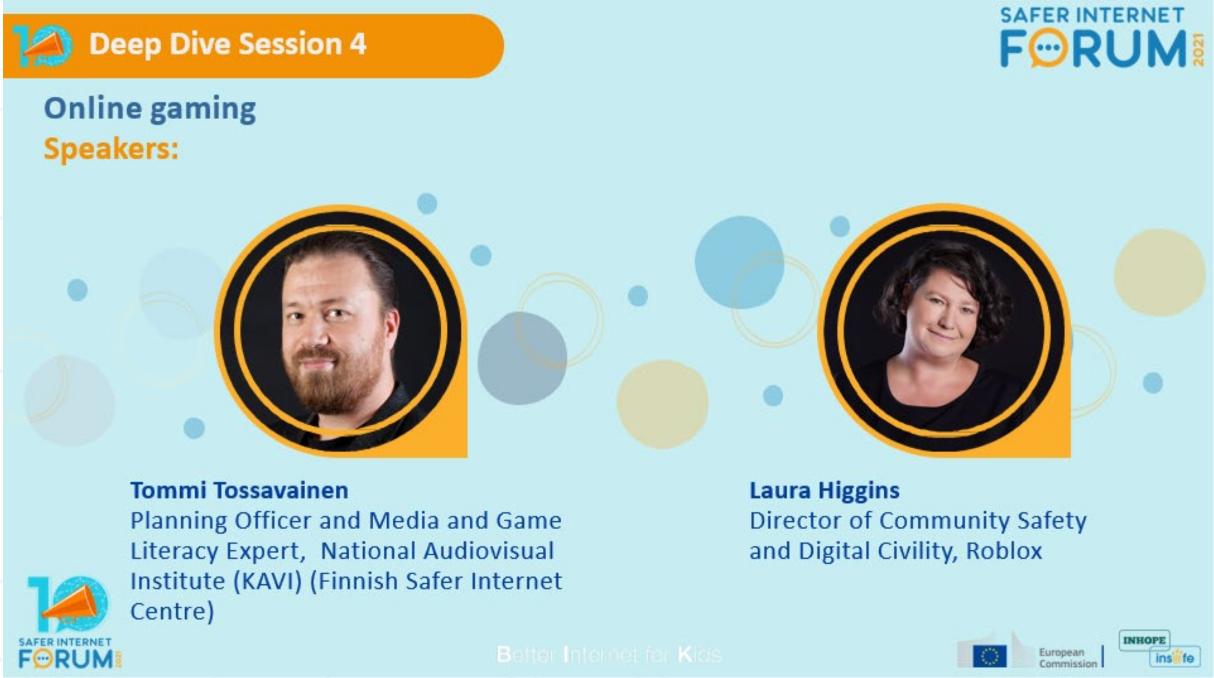
In terms of data governance, quality control and protection of processes, EOKM has concluded that the specific governance processes in place vary greatly and that all participating parties have a data protection policy. These data protection policies largely revolve around access management and there is unfortunately a huge problem with contaminated databases. In terms of third-party engagement, EOKM has concluded that the legal basis for sharing hashes varies greatly by country and this is subject to legal, technical and resource challenges.

The final field of interest that EOKM analyses is the legislation related to each country and each database. The conclusion is that there is no universal definition of CSAM and there are many methodologies used, such as Baseline, COPINE, SAP, Oliver, Sexual Offences Definitive Guideline, Grey Area, US-technology sector system, and so on. The differences in jurisdiction are immense and this also has impact on analysts. Also, GDPR and data sharing regulations pose further challenges to the process. Arda concluded by presenting the HashcheckServer project of EOKM.

DD4: Online gaming

The recording and presentations from this session are available from www.betterinternetforkids.eu/sif.

This deep dive aimed to explore the latest trends, risks and challenges with online gaming, focusing on children and young people.



Deep Dive Session 4

SAFER INTERNET FORUM 2021

Online gaming

Speakers:

Tommi Tossavainen
Planning Officer and Media and Game Literacy Expert, National Audiovisual Institute (KAVI) (Finnish Safer Internet Centre)

Laura Higgins
Director of Community Safety and Digital Civility, Roblox

Better Internet for Kids

Games then and now? Online gaming as a safer internet issue

Tommi Tossavainen, Planning Officer and Media and Game Literacy Expert, National Audiovisual Institute (KAVI), Finland began the session by reflecting on digital progress and evolution. He noted that as society has become digital, so have our lives and this in turn has made them a lot safer. This technological evolution has reached video games too, which first gained popularity and notoriousness in the 1990s. This is also around the time when video games started to become a significant media concern, with games such as Mortal Kombat often being highlighted as extremely violent.

Tommi mentioned the PEGI system: a framework that can help parents get more information on a game, such as the exact type of harmful content and scenes it might include. However, he also pointed to the challenges which emerged as video games moved from a single-player experience to an online shared environment: most problems are encountered in the game culture surrounding the game, rather than the game itself. This is an aspect that concerns Europe at large: in Tommi's words 'Europeans are gamers', with over half of the EU population playing video games. Additionally, half of video game players are women – and research shows that certain video games could act as a path to STEM careers by increasing interest in these subjects. More effort is needed in this direction though and, according to Tommi, one mistake back in the 80s in still causing issues in this area.

He noted that the 1980s marked a fast period of growth for women, with more and more of them choosing to go into computer science degrees. With desktop computers becoming largely accessible to the public (but primarily marketed towards men), this trend decreased. Tommi then highlighted how this issue extended to different sectors and areas in the gaming industry. For example, in game development studios, 80 per cent of employees are still men, meaning that most games designed will be targeting men. Tommi gave the example with Grand Theft Auto, and how female characters, even if they are not the main ones, tend to be overtly-sexualised. This trend is also seeping into other sectors, such as game journalism. At the same time, he shared some success stories from Finland, highlighting what has been done to promote women getting into the game industry and playing games in a safe place. For example, the city of Helsinki is organising gaming activities and safe gaming spaces for girls and minorities, where they can play together without the stress of having to compete with men or external influences. Additionally, some games target minorities specifically, such as the Mimmit Koodaa.fi programme – an initiative in Finland that aims to increase gender equality in the Finnish software industry.

Another issue raised by Tommi was that games often include gambling elements, noting that the line between gambling and games is becoming thinner and more blurred. He cited FIFA as an example of this, stating that what is often not advertised is that the chance of getting the most famous players (such as Ronaldo) is actually less than 1 per cent. In fact, a user would need to buy hundreds of packs to get a chance to play with this character. While this is a trend which is problematic for adults, it also affects children and young people, and more practical solutions to handle this issue are needed. Tommi gave some examples of practical ways to support gaming knowledge, such as game educator handbooks.

Finally, the speaker also noted the importance of screen time and screen time warnings as a means to promote a more balanced view on a typical post-COVID day. While some believe this is a myth from a bygone era, other countries (such as China for instance) still have policies in place to limit screen time.

Creating a safe and civil metaverse – Roblox

In the second part of this deep dive session, **Laura Higgins, Director of Community Safety and Digital Civility at Roblox**, began by introducing Roblox, highlighting that rather than a simple gaming platform or repository, it is a place where people can come together when they cannot be together in real life. In this sense, the idea behind Roblox is to collect different experiences and offer a chance for people to come together with their friends and enjoy independent activities. Importantly, Roblox offers a different experience for everyone, with every bit of it being user-generated connecting millions of people every day. Laura shared that, on average, Roblox welcomes around 43 million daily active users, with more than 8 million active developers and 3,000 moderators working all over the world.

Laura then introduced the Roblox metaverse. Roblox's vision for the metaverse is to create a platform for immersive co-experiences, where people can come together within millions of 3D experiences to learn, work, play, create, and socialise. The Roblox metaverse space is always growing and changing in an organic manner – but it also has rules in order to contribute to building a safer internet space, and protecting children and minors.

Laura also listed some of the ways in which Roblox is ensuring safety: through an automated chat filter, additional privacy restrictions for those under 13, a reporting system for players, and giving users the ability to block other players. Additional resources exist for parents of children under the age of 13: for example, they can make lists with approved content. There are fewer restrictions for teenagers above the age of 13. The platform also includes email and person verification to try to prevent unauthorised purchases. No billing information is stored, and extra attention is paid to working with families to minimise the risk of someone bypassing the system. In addition, Roblox offers tools and knowledge to teachers, parents, and children so they have the necessary skills and understanding to experience games in a positive way. One example of this is the Digital Wellness Lab, a Greek organisation led by a children's hospital.

To understand how teenagers interact online, Roblox conducted a survey during August 2021 in conjunction with three focus groups (19 teenagers interviewed across several days) with the aim of supporting young people to have a safe and fulfilling experience online. The key findings can be summarised as follows:

- The survey respondents highlighted the positive impact of the internet in helping them create strong friendships with others, which 'bring out the best' in them.
- Teenagers who play games are more likely to be confident and have more liberty in expressing themselves freely, as they feel that game communities offer a space for them to be themselves and provides an opportunity to meet like-minded people with similar interests.
- Overall, teenagers are cautious when it comes to unwanted contact, including people who do not appear genuine on the internet.
- Some of the main challenges associated with gaming include setting time limits and finding balance.

Laura concluded by highlighting the role of safety partnerships between organisations, safety centres and players as fundamental towards making regulation and legislation usable. Collaboration is also essential: the Roblox community has to work together to provide safe spaces online, so when someone goes from one platform to the next, they can expect the same level of support and safety.

Following the presentations, several questions were posed by the audience, mainly relating to safety and privacy measures on Roblox. On the point of the privacy restrictions based on the age of consent, Laura responded that Roblox has recently launched an additional verification system to include further checks on under 13-year-olds. This allows older members of the community to have a slightly less-moderated experience. At the same time, those verified as above the age of 18 will be able to access voice chat. When asked about how Roblox collaborates with other platforms, taking the example of cyberbullying which can easily proliferate across multiple domains by a single user, Laura shared that Roblox participates in a working group with the National Crime Agency. Due to GDPR, explicit data cannot be shared, but trends and issues are disclosed within the group. There have also been times when Roblox has had to reach out to other platforms in relation to users of concern. In turn, discussions have been taking place in conjunction with law enforcement about what the future might look like, especially regarding exchanging information and data while protecting users' privacy.

DD5: Youngest users

The recording from this session is available from www.betterinternetforkids.eu/sif.

This session explored what we know about risks and opportunities online for the youngest users of technology. Evidence suggests that children (aged 0 to 12) are going online earlier than ever. These children will be teenagers and young adults by 2030 and will have to live with the decisions we take now. Speakers in this session therefore shared their experiences and discussed possible solutions for this age group.

Deep Dive Session 5

SAFER INTERNET FORUM 2021

Youngest users

Speakers:

Professor Jochen Peter
Full Professor, Amsterdam School of Communication Research (ASCoR), University of Amsterdam

Shanta Arul
Director, Global Technology and Innovation Public Policy, Netflix

Matthias Jax
Social media expert and Project Manager, Saferinternet.at (Austrian Safer Internet Centre)

SAFER INTERNET FORUM 2021

Better Internet for Kids

European Commission | INHOPE insafe

Professor Jochen Peter, Full Professor, Amsterdam School of Communication Research (ASCoR), University of Amsterdam, The Netherlands, began the session by explaining that the future of technological development is difficult. He went on to identify five crucial trends that may help us to understand what the future will bring.

First, there has been a trend of change from mass communication to human-machine communication. Mass communications (such as newspapers and TV) used to be the most common type of communication, along with face-to-face communication. When internet use became widespread, it changed how people communicated: communications became computer-mediated. However, mass and computer-mediated communications are still communications between humans. What we see now is that many communications no longer take place between humans but can be between machines (for instance, the Internet of Things (IoT)), or between humans and machines (such as voice assistants).

The second trend is related to the source of information. With mass communications, the source was primarily a journalist. With computer-mediated communications, the sources are people: that is, anybody can be a source of information. In these two cases, the sources are humans. But with human-machine communications, technology is the source (bots or voice assistants, for instance).

The third trend is the change in cues which users get during communication. Cues used to be only two dimensional: visual in newspapers (text), auditory for radio, and also visual for television and the internet. But now we are facing a major change since cues can now be special (for instance, virtual reality), and even haptic (such as connected toys, or social robots that you can touch).

The fourth trend is the change from distant to intimate technology. While technology used to be "between us" (social media for instance), it then became technology "about us" (with tracking devices, for example). Technology can now be "like us" (human-like robots) and even "inside us" (with implanted devices). The differences between technology and us then become smaller.

The last trend is the change from physical reality to mixed and virtual reality. Augmented reality (such as the overlay of virtual information on the real world, as seen in Pokémon GO for example) and augmented virtuality (overlay of the real world on the virtuality) lead to a mixed reality which has increased in the past years. Virtual reality is a reality completely created by computers. The share of experience of children with the physical reality is decreasing as worlds that are completely or partially virtual are become increasingly common.

These five trends, all together, can help us identify the direction in which we want to go. They culminate in what is called the metaverse. Tech companies are strongly pushing the development of such a metaverse. A metaverse is persistent (it stays, it always continues), it is synchronous (it is live), and there is an unlimited number of concurrent users. It connects the analogue/physical and the digital/virtual worlds. It offers interoperability and it depends on the content the users generate. There will be a full economy in the metaverse since enormous profits can be made.

These developments must be taken seriously, especially when it comes to children. Technology becomes more "natural", and interaction is increasingly easy and accessible. Children can also be highly attracted to technology because there a strong link to gaming and entertainment, but also because children are more open to interaction and communication with machines. Additionally, the metaverse provides immersion and is always on, which can further attract young users.

All of this provides opportunities:

- It may be handy for education and can provide new ways of teaching.
- It may offer new tools for therapy.
- It can create new inclusive communities, sometimes more so than in the physical world.
- It may offer a way to compensate for difficulties encountered in the real world.

However, risks also exist:

- The lack of regulation and control leads to inappropriate content and experience, mis- or disinformation, or antisocial behaviour.
- The creation and collection of ever-more personal data raises the question of privacy and inequality in division of learning.
- The automation of personal decisions (predictive algorithms) limits the opportunities which children are provided with.

- The risk of necessity, dependency, the foreclosure of alternatives, and enforced ignorance. We keep using internet applications even though we do not want to. It becomes difficult not to use it and we become increasingly dependent on it.

These opportunities and risks are speculation, but Professor Peter believes that several things could be done:

- Increase awareness of development far beyond the internet.
- Develop a stronger legal framework by putting pressure on industry.
- Increase education on technology: how it works and why.
- Increase the social acceptance of being offline.

The next speaker, **Shanta Arul, Director, Global Technology and Innovation Public Policy, Netflix**, focused on how Netflix in supporting parents to control what their children are watching and to limit screen time. Netflix wants to offer parents the freedom to watch content on their own or with their children, and ensure that children are only able to watch appropriate content. Contrary to television where users switch it on and have no control over what is broadcast, Netflix users have more control over what they watch. Netflix therefore offers information about content, including what is appropriate (or not) for children. Parents can then choose what they want their children to watch. The rating is always visible before launching a show (or at the beginning) to ensure that parents are informed. User profiles allow for additional controls; depending on the age of each user, content can be controlled and set by age. A pin code system also enhances parental controls over what children can watch.

Kids profiles, which are a default setting, only offer content that is suitable for children, and ensure that children access Netflix via a controlled experience, designed using research-based insights. User opinions and needs are taken into account through interviews, customer feedback, surveys and social media. Ethnographic research and third-party academic research methods were also used. Parents can have very different attitudes, needs and expectations when it comes to their children engaging with a service like Netflix. As such, Shanta presented four different parenting styles identified through their research: the “free range” (you’re on your own), the “peerents” (let’s talk about it), the “velcro” (I need to protect you) and the “pedagogical” (be all that you can be). Netflix aims to offer a service that matches these different parenting styles.

The first goal for parental controls on Netflix is to be easily accessible. The profile hub is an easy tool to manage the different profiles. It offers a content restriction option which allows parents to filter content within an individual profile, based on maturity ratings. To control screen time, the autoplay option can be disabled for any profile, and the viewing activity history is available for each profile to keep an eye on what children are watching. On top of that, the profile lock function restricts access to profiles using a pin code. A recap email is sent to every account with kid’s profiles, providing an insight to parents on what their child is engaging with. In this way, parents can bring the online experience offline, and engage in a dialogue with their children about what they are watching on Netflix.

Work is ongoing to raise awareness about parental controls, and this must be done not only with parents, but also with NGOs and ministries. In Europe, this is done with the European Commission, Better Internet for Kids (BIK) and national Safer Internet Centres (SICs).

Next up, **Matthias Jax, Social media expert and Project Manager, Saferinternet.at (Austrian Safer Internet Centre)** presented a study on children under 6 years old and digital media, conducted by the centre. One of the main findings is that 72 per cent of children under 6 in Austria use digital media. This implies that consumption does not start when children get their first cellphone, but before. On average in Austria, children are just one year old when they use an internet-enabled device for the first time. More than 50 per cent of their usage is to watch videos, take pictures, listen to music, or play video games. Talking to people is significantly more important among those aged 0 to 2, while playing games is significantly more important among those aged 3 to 6. 50 per cent of children use their parent's devices; this presents a particular problem because the algorithms will use data based on the adults use the smartphone.

Parents are on the move digitally. 99 per cent of the parents surveyed use the internet daily for private purposes and spend an average of 2 hours a day doing so. However, they have no or little experience with media education from their childhood, so they have had to learn everything themselves. 75 per cent of the parents agree that they are great role models when it comes to using internet-enabled devices, and 9 out of 10 parents take certain precautions before allowing their child to use an internet-enabled device. However, 17 per cent of them confirmed that their child had already encountered unsuitable content. On the child's side, for 10 per cent of 3- to 6-year-olds, watching videos before falling asleep is important. 30 per cent of parents had sent or posted a picture of their child before his or her birth.

Matthias then went on to address the question of what can be done. Digital pacifiers bring several issues, and there is a lack of clarity about whether there are psychological developmental effects and, if so, what they are. Another issue is to be unable to engage the self or to process emotionally difficult situations without digital devices. Digital pacifiers can also be an issue because of the frightening content children can be confronted with, and other issues such as abusive use of photos.

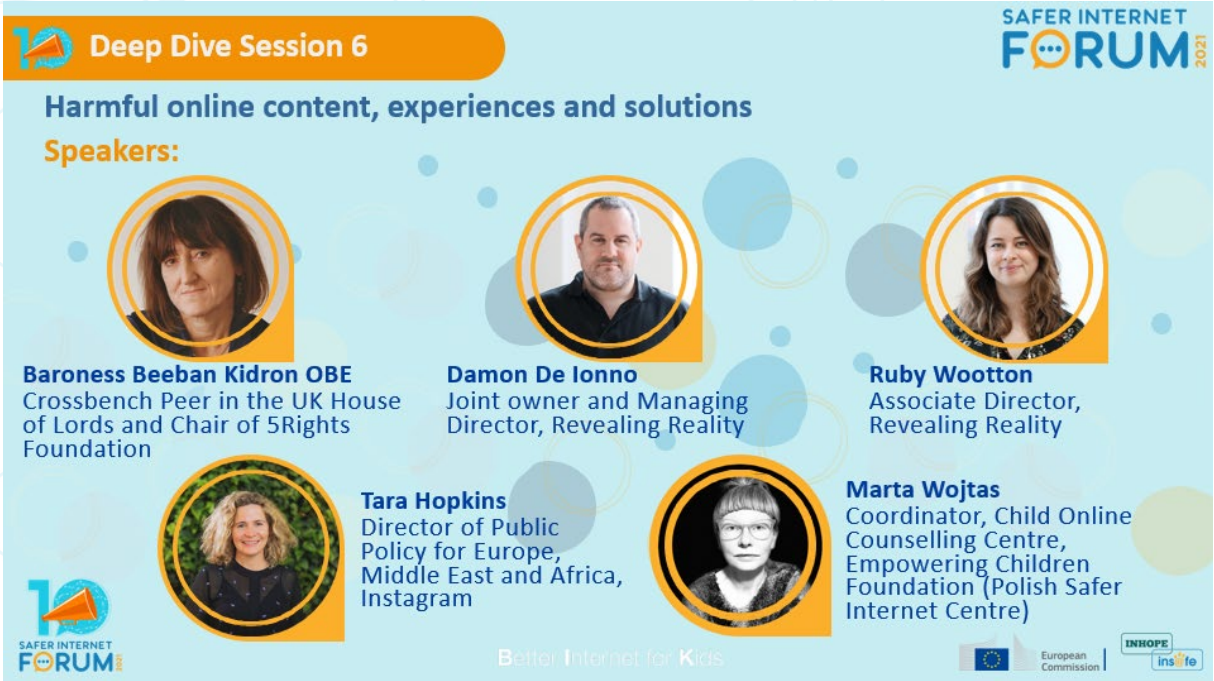
Tips can be given to parents. For example, they should be aware of being a role model. They also should give the children full attention, delay use of digital devices as much as possible, use digital media only in exceptional cases, set rules and be consistent, select suitable content, and send selected photos of the children to only a few contacts.

The Austrian Safer Internet Centre has created various resources including a video, a folder translated into several languages, and brochures (Mum, can I go on your phone?) to raise awareness on this topic. For the youngest users, a handbook for kindergartens with exercises and games was produced, along with a book translated into several languages.

DD6: Harmful online content, experiences and solutions

The recording and selected presentations from this session are available from www.betterinternetforkids.eu/sif.

This session focused on harmful but not illegal content and experiences. Recent research suggests that children, some as young as 13, may experience potentially harmful content and experiences from the moment they sign up to some of the most popular social media platforms and services. How big a problem is this and what can be done to address it? Speakers in this session shared their perspectives.



Deep Dive Session 6

SAFER INTERNET FORUM 2021

Harmful online content, experiences and solutions

Speakers:

Baroness Beeban Kidron OBE
Crossbench Peer in the UK House of Lords and Chair of 5Rights Foundation

Damon De Ionno
Joint owner and Managing Director, Revealing Reality

Ruby Wootton
Associate Director, Revealing Reality

Tara Hopkins
Director of Public Policy for Europe, Middle East and Africa, Instagram

Marta Wojtas
Coordinator, Child Online Counselling Centre, Empowering Children Foundation (Polish Safer Internet Centre)

Baroness Beeban Kidron OBE, Crossbench Peer in the UK House of Lords and Chair of 5Rights Foundation kicked off this session, highlighting that we want children to participate in the digital world. As we work out solutions, we must ensure that they are included. Through its work, the 5Rights Foundation looks at privacy and data protection, age-appropriate design, children's rights, and the concept of child-centred design. Importantly, the question we need to ask if we are to prevent harm is how would we design the digital world if the end user was a child? Baroness Kidron reflected on the recent testimony of former Facebook employee Frances Haugen to Congress, as it provides a relevant backdrop to today's conversation. Frances Haugen described a situation which we have collectively allowed to develop in which people who own the technology have little responsibility to those who use it; the people who design it are only responsible to those who own it; and the people who own and profit from it are allowed to do so without oversight, accountability or basic safety measures, even when the end user is a child.

Baroness Kidron provided an overview of the workshop structures used by the 5Rights Foundation, the result of which is the young participants leave with a solid understanding of the fundamental asymmetry of power between them and the tech which they are using. Crucially, 5Rights Foundation also gain a better understanding of what young people see, do and feel about the digital world. She also commented on the UK's Age appropriate design code; a set of 15 standards that online services need to follow, which has influenced the biggest redesign of tech platforms over the course of summer 2021. The recommendations in the code are coupled to specific children, with real concerns about their online experiences. What was learnt was that what upset them and harmed them were not bugs in the system but 'features' of the digital world that amplified, pushed, recommended and demanded content and behaviours that undermined, exposed and harmed them. 5Rights subsequently commissioned research to explore how the design choices of platforms manifest in children's lived experiences, and to illustrate how optimising platforms for business objectives was directly impacting on children's experiences. The findings were quite miserable, as will be shown below.

Baroness Kidron stressed that this research does not exist in a vacuum; it mirrors Facebook's own findings, it mirrors what the regulators have found in the UK and, most importantly, it mirrors what children and young people have been telling us for years that profit is put ahead of child safety. In short, we need to accept that the system is not working, and what we need law makers to establish the rules of the road.

Damon De Ionno, Joint owner and Managing Director, Revealing Reality then introduced the research work. Revealing Reality is an independent research agency that carries out a lot of work on children's use of technology and online harm. It has no political agenda; they just wish to understand – and help others understand – how people experience the world around them.

Named Pathways, the research explored how design decisions made by digital companies influence children's behaviour and experiences. They started by interviewing a series of professionals across the tech industry, from different platforms including social media but also organisations that work alongside them. Companies tend to start with a business model, based around gaining attention (i.e. advertising-funded models for the most part). Incentives tend to focus on increasing reach, without necessarily thinking about the consequences. KPIs tend to focus on more users, more time, more activity, more attention. In contrast, there is very little incentive to design ethically or responsibly. Various techniques are used to encourage uses to consume, connect, interact and create content, using gamification techniques. This taps into user motivations based around popularity and perceived value of the individual. In summary, there is a huge power sitting behind the screen all geared towards shaping user behaviour towards business objectives.

Ruby Wootton, Associate Director, Revealing Reality then picked up the presentation, focusing on the power imbalance online when the user is a child. As part of the research, Revealing Reality also spoke to 21 children and young people from across the UK, aged 11-18. The research mapped their journey with digital platforms, what they had experienced online, and what they felt about them. They were also asked to share screen recordings of their interactions with platforms. The findings included that respondents were spending a significant amount of time online, the average being 4 or 5 hours a day, but sometimes upwards of 10 hours a day. They reported losing sleep playing games or scrolling late into the night, and finding difficulty in stopping even when they knew it was the right thing to do. Additionally, most of the girls in the sample, but also some boys, said they would never post a photo without editing it first. The number of likes or comments those received was a top priority, and was seen as a value of self-worth.

Ruby reflected on the challenges of conducting research with minors, with responses limited to what children choose to tell researchers or what they can ethically be asked about. To counter this, an experiment was set up. A series of profiles were set up on digital platforms which mimicked the experiences and behaviour of the real young people they had encountered during the research. These 'avatars' were a proxy for a real child; social media accounts set up with fake names, but populated with the age and interests of real children. A series of adult profiles were also set up to see if there were any differences in the findings.

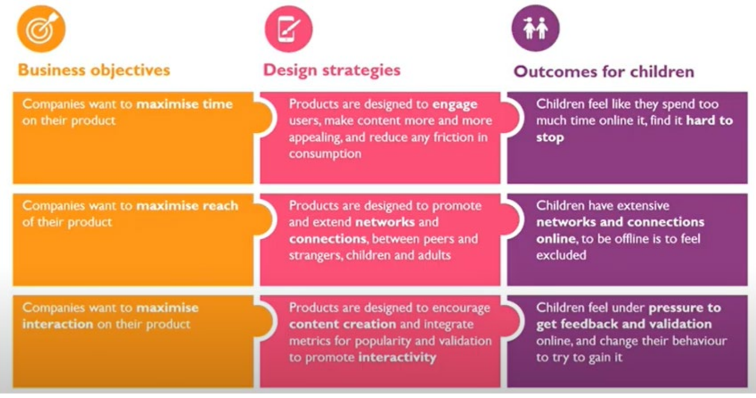
In terms of findings:

- Avatars were proactively contacted by strangers, including from drug sites, highly sexualised sites, or dark memes. They were often sent direct messages, or placed in group chats with strangers.
- Avatars were quickly recommended more of whatever they engaged with (for both the child and adult avatars).
- Avatars were easily able to search for and access content relating to eating disorders, suicide, self-harm, and sexual images.

All of the above were true for both the child and adult avatars. However:

- Child avatars were served child-targeted adverts alongside potentially harmful content.

Ruby concluded by contrasting some of the business objectives and design strategies of social media platforms with some of the challenges children expressed:



Business objectives	Design strategies	Outcomes for children
Companies want to **maximise time** on their product	Products are designed to **engage** users, make content more and more appealing, and reduce any friction in consumption	Children feel like they spend too much time online it, find it **hard to stop**
Companies want to **maximise reach** of their product	Products are designed to promote and extend **networks** and **connections**, between peers and strangers, children and adults	Children have extensive **networks and connections online**, to be offline is to feel excluded
Companies want to **maximise interaction** on their product	Products are designed to encourage **content creation** and integrate metrics for popularity and validation to promote **interactivity**	Children feel under **pressure to get feedback and validation** online, and change their behaviour to try to gain it

Next up was **Tara Hopkins, Director of Public Policy for Europe, Middle East and Africa, Instagram**. Instagram is a place to connect with the people and the things that you love, to share experiences, to build a business, and to find a community. Instagram wants to protect its community from seeing harmful content, but also to balance space and voice for people to share, even if not every user will like all content.

Instagram takes a multi-pronged approach, and different rules and tools are in place to make sure Instagram provide a good experience. You need to be 13 to use Instagram, but verifying age can be problematic. Various methods are used to find and remove underage accounts, plus content reviewers can also trigger an age verification process. Instagram wants to provide an age-appropriate environment, and artificial intelligence is increasingly being used to do this.

Age gating is used to restrict certain content, while the community guidelines are there to make sure that it is clear for everyone what you can and cannot share on Instagram – sometimes these guidelines are stricter than country rules.

A combination of technology that can be used at scale and human reviewers are used to verify content. The technology is typically used to detect potentially harmful content, and then it is flagged for human review to better understand the context. Hashtags are also used to manage violating content. There is no one algorithm; many algorithms work in parallel to serve suitable content. While this is not perfect, continuous improvements are being made. The concept of 'nudges' is being trialled to encourage users to limit screen time or to move away from potentially problematic topics.

Various features are provided for younger users:

- Instagram encourages young people to have private accounts; new users under the age of 18 are automatically placed in a private account experience, while existing users under the age of 18 are being encouraged to make their accounts private through onscreen prompts and similar. It is not allowed for accounts to reach out to young people, and advertisers cannot target young users.
- A feature which was trialled with mixed results was the hiding of the likes; users now have the option to show or hide depending on their preference.
- Parental control options are being developed and implemented on an opt-in basis, recognising that circumstances will differ significantly from user to user.
- For topics such as eating disorders and suicide prevention, there are strict policies in place to ensure there is not promotion of the issues, but recognising that promotion of recovery or connecting people to support services is important.

Marta Wojtas, Coordinator, Child Online Counselling Centre, Empowering Children Foundation (Polish Safer Internet Centre) rounded off the formal presentations in this session by focusing on harmful online content, experiences, and solutions based on findings from the helplines for children and for teachers and parents, and the child online counselling centre in Poland. Marta shared a number of case studies to illustrate the issues.

A specific example is a trend known as 'Pathostreaming' where influencers strive to get more likes by streaming themselves doing anti-social things. It typically includes vulgar content showing drug or alcohol use, humiliating other people, and doing dangerous challenges for money. The content has not been banned by social media platforms. Linked to this is Patho music, which is again not illegal but highly problematic. Videoclips were available on mainstream platforms, such as YouTube, that are not in contravention of terms and conditions, but the lyrics are harmful for young people. The songs were promoted in primary schools, so very young children were singing lyrics about rape, violent sex, and violence against women. It was reported to the Prosecutors Office, but only a part of the content could be blocked; the rest is still available for anyone to access.

The Polish Safer Internet Centre is also aware of a significant problem with suicide groups, whereby young people get together online to reinforce suicidal tendencies. However, these groups are often private, so although the centre knows that they exist, and knows that they are harmful, they are unable to do more about it. This is a significant gap and we need to cooperate with social media companies to find solutions.

Sexual abuse in the plot of role-playing games (RPGs) on Messenger has also been an issue. In one instance, the plot turned sexual

and a child was abused as a result. In this case, both the victim and the perpetrator were teenagers. A problem here is that we only know it is happening after the fact. Generally, there has been an increase in grooming cases on both Instagram and Facebook, especially during the pandemic. Young people want to make contact with other people, but often they cannot check who they are really talking to or verify their identity hence leaving them vulnerable.

A further example of harmful content are videos which model inappropriate behaviour patterns or promote dangerous challenges. While these typically don't violate terms and conditions. Some can have significant longer-term effects. For example, games on cosmetic surgeries can later influence the body image of children, or children adapt their behaviours to mimic those people they see online. Dangerous challenges, especially those on TikTok (such as the skullbreaker challenge), pose a big problem. Such challenges are often popularised by influencers, and they are also becoming monetised to try to get money from observers.

Dropping out of school has become a significant issue during the pandemic and times of remote learning. It was found that young people often felt anticipatory anxiety because of cyberbullying and hate speech. This anxiety sparked a fear of being seen on camera – "*if they see me, they can/will record me, they will laugh at me, and I'll become a victim*". This problem is global; this culture on the internet needs to be addressed.

In terms of possible solutions, Marta suggested a number of potential areas to tackle:

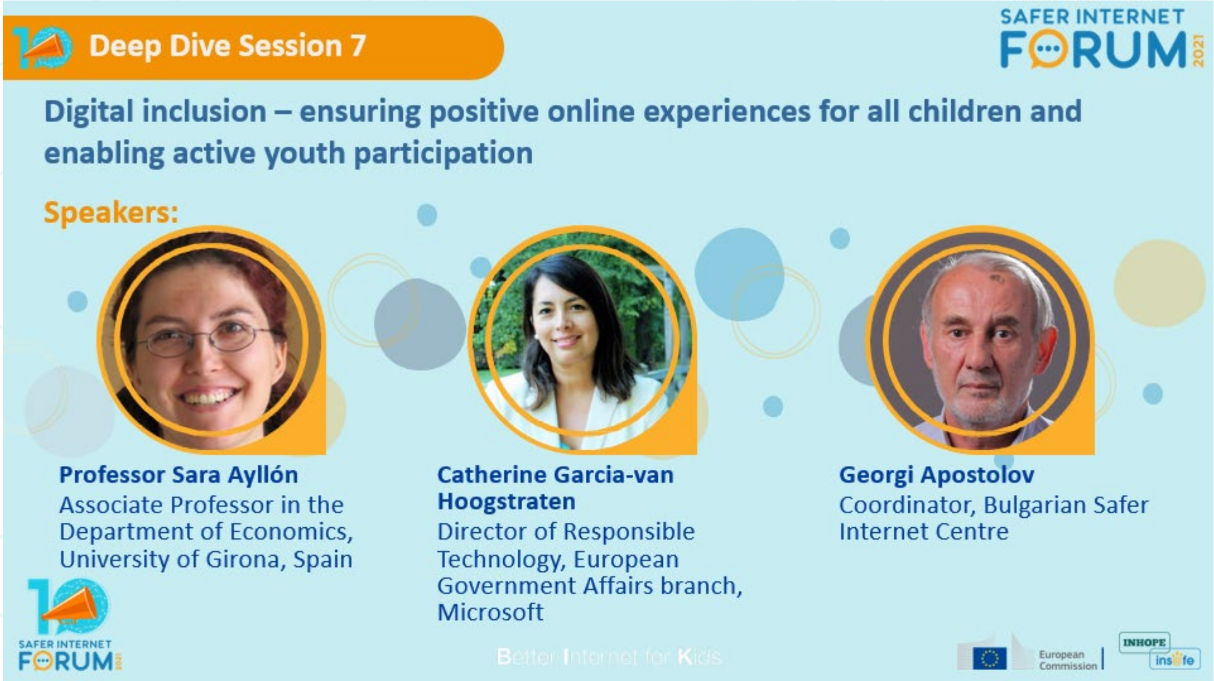
- We need to continue the dialogue with platform providers and have more direct links to report issues.
- We need to address the way that algorithms work by suggesting more of the same content; this is clearly an issue if platforms are serving more and more content on harmful issues.
- A new attitude to harmful content is also important; not every content is harmful, and we cannot necessarily categorise it as harmful. Sometimes patterns need to be taken into account.
- Parent control tools need to be addressed, especially if content isn't immediately recognised as being harmful.
- Education is very important, especially as children often do not recognise threats online.
- Artificial intelligence could be useful for identifying harmful content that we know exists but have difficulty in locating.
- Education is changing and we are trying to feed a changing word. However, we are still the people who are responsible for a safer internet, while social networking sites can also do more to educate users.

To draw the session to a close, Baroness Kidron reflected on the discussion which had taken place as a way of looking forward. We need to shape behaviour in different ways; we need to move away from takedown, blocking and parental controls, and instead explore how systems can be detoxified for children and young people and, essentially, made better up front. We need to challenge the way that platforms serve content; for example, they are quick to take down content that contravenes copyright, but less so in dealing with harmful content. We therefore need to 'follow the money' and recognise that children are currency in this space and hence have value. Finally, we need to invest more on algorithmic oversight, and conduct risk assessments on recommendation loops to determine if they are creating risk, harm and damage.

DD7: Digital inclusion – ensuring positive online experiences for all children and enabling active youth participation

The recording and presentations from this session are available from www.betterinternetforkids.eu/sif.

This session focused on digital inclusion and how we ensure positive online experiences for all children, and enable active participation for younger generations.



Deep Dive Session 7

SAFER INTERNET FORUM 2021

Digital inclusion – ensuring positive online experiences for all children and enabling active youth participation

Speakers:

Professor Sara Ayllón
Associate Professor in the Department of Economics, University of Girona, Spain

Catherine Garcia-van Hoogstraten
Director of Responsible Technology, European Government Affairs branch, Microsoft

Georgi Apostolov
Coordinator, Bulgarian Safer Internet Centre

Better Internet for Kids

Professor Sara Ayllón, Associate Professor in the Department of Economics, University of Girona, Spain began this session by presenting the DigiGen project, funded by the European Commission. Within this project, a study was conducted on the consequences of the use of new technologies.

COVID-19 has changed the need for internet connectivity and for technological devices across the population, but particularly among children. In terms of education, many countries moved part of their teaching online. Therefore, nowadays, for many children, having a computer connected to the internet makes the difference between being able to keep up with their education or not. Interest and confidence in the use of technological devices are assumed for most children. However, the pandemic showed us that not everybody has access to the internet or, indeed, can use it.

According to the last wave of EU Statistics on Income and Living Conditions (EU-SILC), on average in 2019, 5 per cent of the children in Europe were digitally deprived: their household could not afford to have a computer or could not afford an internet connection for personal use at home. According to the last Programme for International Student Assessment (PISA) wave, in 2018, 6 per cent of 15 years old in Europe were digitally disengaged, while 8 per cent lack confidence in their ICT usage. It is therefore crucial to understand who are the digitally deprived, digitally disengaged, and digitally unconfident children in Europe in order to design effective policies.

To identify the digitally deprived, the EU-SILC study used two variables identified by negative answers to the following questions:

- Does your household have a computer?
- Do you have an internet connection for personal use when needed?

Those that are considered to be 'digitally deprived' are children that either live in a household that cannot afford a computer and or live without an internet connection. On average in 2019, 3.5 per cent of children in Europe were digitally deprived. There are also large differences across Europe, and two country-clusters appear, with a certain north/south divide: less than 2 per cent in Iceland, Finland, Norway, and more than 20 per cent in Bulgaria and Romania. Over time, most of the countries have moved in the right direction. There is progress, and the situation is getting better, especially in countries where deprivation is high. Less change can be seen in other countries.

To understand who the digitally deprived are, social factors are keys. The study shows that one characteristic clearly stands out as being very closely linked to children's digital deprivation: living in severe material deprivation. That increases the risk of suffering digital deprivation by a factor of 6.7. Being poor and having low-educated parents are also relevant factors. These variables multiply the risk of being digitally deprived by a factor of 2.9 and 3.3, respectively. Other factors are also at play, even though there are lower, and can vary from one country to another.

To understand and measure digital interest and confidence, the PISA waves of 2015 and 2018 were used, through six of its questions interrogating children's interest, feeling and use of ICT. Those considered as digitally disengaged are the children who have a score of interest towards ICT below or equal to 12 points. The same type of question was used to measure digital confidence. The children who have a score of confidence towards ICT below or equal to 10 are considered as digitally unconfident.

On average in 2019, 6 per cent of 15 years old in Europe are digitally disengaged. We find two country clusters, with a certain West-East divide. Whereas in Belgium (5 per cent), France (4.8 per cent), Germany (3.9 per cent) and Spain (5.2 per cent), the percentages of digitally disengaged children are low, in Eastern Europe such percentages are high: 17.3 per cent in Bulgaria, 15.2 per cent in Albania, and 13.7 per cent in Serbia, for example. When looking over time, we see that countries that had already low percentages in 2015 generally maintain these in 2018. However, a slight increase is found for instance in Estonia, Greece, Spain, Finland, France and Iceland. In contrast, in Austria, Belgium, Hungary, Lithuania, Luxembourg, Latvia and the United Kingdom, the percentages have dropped.

Concerning digital confidence, on average in 2019, 8 per cent of 15-year-olds in Europe are digitally unconfident. A certain West-East divide is found, with high percentages in Eastern Europe: 16.8 per cent in Bulgaria, 15 per cent in Serbia, 14.2 per cent in Lithuania and 11.1 per cent in Finland. Between 2015 and 2018, we find a decrease in the prevalence in Austria, Belgium, Denmark, Germany, Lithuania, Luxembourg, and Sweden. Again, Bulgaria is the country where the number of digitally unconfident children has increased the most, with about 6.5 percentages points. Similarly, Iceland has seen an important increase of 4.1 percentage points.

When trying to understand who are the digitally disengaged, we see that one characteristic is being very closely linked to children's lack of interest in ICT: the grade repetition. Little bonding with their own school, low-educated parents, being bullied, and a low level of wealth also increase the likelihood of being digitally disengaged. We find no statistically significant differences in immigrant origins and with low level of home possessions. The same factors appear when trying to understand who the digitally unconfident children are. Subjective feeling of little bonding with the school is the most interlinked factor to lack of digital confidence. Grade repetition, low level of home possessions and being bullied also increase the risk of being digitally unconfident by a factor of 1.5. As for wealth, low-educated parents, and immigrant origins, we do not find a statistically significant relationship.

As a conclusion, digital deprivation is a problem among school-aged children in certain European countries particularly regarding the inability to afford a computer. The phenomenon is particularly widespread in Southern and Eastern European countries. It affects children that cohabit with low-educated parents, in poverty, and especially in severe material deprivation. However, the heterogeneity of characteristics that describe a digitally deprived child is large across countries. Concerning digital disengagement and lack of confidence, we find a rate of approximately 6 per cent of 15-year-olds in Europe. The prevalence of such phenomenon differs across European countries in a similar fashion to the results concerning digital deprivation. Despite the disparities in children's socio-economic characteristics linked to ICT lack of interest and confidence between country clusters, we find that grade repetition, below average home possessions, and no sense of belonging to school to be the main determinants of both problems.

DigiGen proposes policy recommendations to tackle this issue:

- Ensure that lack of monetary resources in not the reason why children lack access to a computer and/or an internet connection.
- Add the inability to afford a computer to the definition of material and social deprivation (PSD) rate. Add additional indicators to commonly used databases such as the EU-SILC.
- Prompt children and young people’s interest and confidence in ICT as both are an essential pillar in today’s educational system
- Ensure that students are equally prepared for the digital age, regardless of where they live or the location of the school they attend.

Catherine Garcia-van Hoogstraten, Director of Responsible Technology, European Government Affairs branch, Microsoft presented the initiatives taken by Microsoft for digital inclusion through accessibility. At some point in our lives, each of us may rely on assistive technologies. Inclusive design is about creative a responsive system. Disabilities affect over 1 billion people worldwide (visual, hearing, cognitive, speech, mobility, neural), and diseases can span disability segments. Accessibility should not be considered as a 'bolt on', but rather accessibility should be included early in the process through inclusive design, solid engineering processes, thorough testing, and customer validation.

Microsoft has developed learning tools for people with dyslexia. The Xbox adaptative controller is a tool for people with mobility and dexterity disabilities who might not be able to reach all the bumpers and triggers or hold a controller for an extended period of time. The Surface Adaptive Kit guide is a series of add-ons to customise the accessibility of Microsoft's range of laptops and tablets, that help users to find specific keys, locate ports, or flip open a device. Microsoft also presented a project of co-designing accessibility to the Youth Pledge. This process will feed into an update for a more age-appropriate visual design including design changes in the UX that emphasises the child-centric controls, helping young users to exercise their privacy rights.

Georgi Apostolov, Coordinator, Bulgarian Safer Internet Centre provided an understanding of the digital divide during the pandemic. The situation in Bulgaria was difficult because a lot of pupils were not able to participate in remote learning due to digital deprivation, and teachers were not prepared either. However, important progress was made.

Bulgaria is one of the countries with the most important Roma minorities, and Roma children are by far the most digitally deprived in Bulgaria. Out of 2,212 schools in Bulgaria, 1,060 enrol pupils from vulnerable groups (mainly Roma). The concentration of vulnerable children varies among schools. Some schools have around 20 per cent of children from vulnerable groups, but we see more and more segregated schools with sometimes 100 per cent of pupils from vulnerable groups. This is due to parents not wanting their child to study together with Roma children.

By July 2021, among the 706,000 pupils in Bulgaria, 43,000 of them did not own a device suitable for learning and 34,000 did not have access to internet. According to a study conducted by the largest Roma organisation in the country, in June 2021, 61 per cent of schools interrogated were able to involve between 76 per cent and 100 per cent of pupils in remote teaching. 31 per cent of schools involved between 50 per cent to 75 per cent, and 8 per cent of schools involved less than 50 per cent of pupils.

The main causes of digital deprivation and the difficulty to implement remote learning is poverty. The ghettoisation of Roma people reinforces poverty, while the school's segregation causes lower education quality and a demotivating environment. Rampant illiteracy in families, the absence of internet access (for pupils and some teachers), and lack of devices (again for pupils and some teachers) are also part of the poverty situation of vulnerable groups.

Measures taken were taken to tackle this situation. The Ministry of Education pushed to create profiles in Microsoft Teams for all teachers and students, distributed 20,000 laptops, tablets and ready-to-use mobile internet sticks. A campaign for donations of devices and internet access was organised and many NGOs initiated and supported donation campaigns (some telecoms and IT companies responded). National networks of education and health mediators in local communities were involved, and these were supported by local authorities. The Bulgarian Safer Internet Centre developed and disseminated short tips and guidelines for remote teaching to teachers and parents.

As a conclusion, to be able to narrow the digital divide, joint efforts are needed and should involve governments, civil society, and industry. The root causes should be addressed both at the national and European level. Strategic and planned measure should be taken to fight poverty and ghettoisation. To do so, mixing the communities is key, and good results can already be seen from this strategy. Strategic policies at the European level, that require national governments to take action to reduce poverty and the social divide, are also needed. Vulnerable children should not be left behind.

Close of Safer Internet Forum 2021

The recording from this session is available from www.betterinternetforkids.eu/sif.

Dr Hans Martens, Head of Digital Citizenship, European Schoolnet hosted the closing session of the 2021 edition of the Safer Internet Forum, to both reflect back on key takeaways from the event, and to look forward at next steps.

In the first part of the session, Hans introduced three members of the BIK Youth Panel – Anisa from the United Kingdom, and Billie and Molly from Ireland. Molly started by providing a brief overview of an additional video which the BIK Youth Panellists have developed, giving a vision for how they would like the online world to look by 2030. Their main hope is to reduce online hate and online bullying, and to make the internet an inclusive place for all (jump to timestamp 8:17 in the session recording to watch the video). In the video, they call upon industry and policy makers to help create an internet of discovery and positivity, by making policies and monitoring requirements stricter, and by expanding keyword trigger lists to reduce hate speech. More importance needs to be placed on education – by educating users both online and offline, cybercrimes can be reduced and a more inclusive, educated society can be created. The young people also reflected on their roles as members of Gen-Z: "*As a generation, we have come together to accept each other in a way that's never been done before, online and offline, and will continue to strive for total inclusion and equality in the future*". The video concludes with an extremely compelling statement: "*Alone we have power, but together we are powerful. Industries and our generation need to unite to reach our common goal of a better internet for kids*".

In the next part of the session, **Yevgeney** and **Lili** from the **BIK Youth Advisory Group**, shared their views on the #DigitalDecade4YOUth consultation process and the resulting report. Yevgeney reflected that, from the report, it is clear that children and young people are aware of the negative aspects of the internet. He also valued the fact that parental views were gathered to allow them to better support their children online in the future. Lili commented on how it was great to ask young people directly about their experiences and concerns online, and the fact that youth ambassadors were able to contribute to the design of protocol and the process, highlighting the key issues which are important to younger internet users. Reflecting more generally on key thoughts following their involvement in the Forum, Yevgeney commented on the urgent need to increase digital inclusion and ensure that all children and young people have equal access to digital tools and services. Lili reflected that policy makers need to provide real answers to real questions and issues, and not just work from a pre-written script. She also reflected on the importance of safety by design, but also the fact that similar strategies should be employed to reverse engineer existing services. She concluded that young people want to be taken seriously in their views, and stressed that this is not a request, but a demand.

Jane McGarrigle from the Irish Safer Internet Centre was asked to reflect on her highlights from the Forum. She especially welcomed the active involvement of the BIK Youth Panel across all sessions of the Forum. She commented particularly on the Deep Dive session on AI, which was particularly active in terms of young people's involvement. The speaker, Dr Baines, especially highlighted the potential of AI to help and support children in our work which is of course an exciting prospect, but also strongly reflected on the considerations, ethics, transparency, accountability and responsibility which needs to be a big focus of our ongoing work. Investment, research and education will all be important cornerstones for this. Jane also mentioned the session on harmful content, quoting from the session "*we need to move upstream, we need to make the system better, we need to recognise that children have a value, we need to make risk assessments of the system*" and "*it's our job as adults to make products safe for children*". She concluded by saying there is much work to be done in the decade ahead of us, but that collectively we – the better internet community – look forward to the challenges.

June Lowery-Kingston, Head of Unit Accessibility, Multilingualism and Safer Internet, DG CONNECT, European Commission also shared what stood out for her from this year's Forum. A particular highlight was the quality, thoughtfulness, confidence and competence of the youth contributions – the BIK agenda needs to be a team effort, and the honest and open exchange of ideas and information throughout the event has been key. She also commented on the value of peer-to-peer education through the quality of sharing ideas and resources through the chat throughout the course of the event. She further commented on one of the key challenges of reaching those communities which are hard to connect with moving forward, and how young people can possibly help to facilitate that.

In the discussion that ensued, Jane reflected on the importance of the national youth panel in Ireland in driving ahead the political agenda and shared some of the great work that is being done in ensuring youth are represented in both national and European research projects; a model which is replicated across Europe through the network of Safer Internet Centres (SICs). On some of the challenges ahead, she commented on the need to ensure that the digital divide is addressed, and that opportunities are provided for everyone's voices to be heard. She questioned how we represent and hear from vulnerable children, children from different ethnic backgrounds, those with different abilities and disabilities, and those from different socio-economic settings. Jane concluded that we've seen some great ideas and innovative tools over the last two days but that there is still much more to be done.

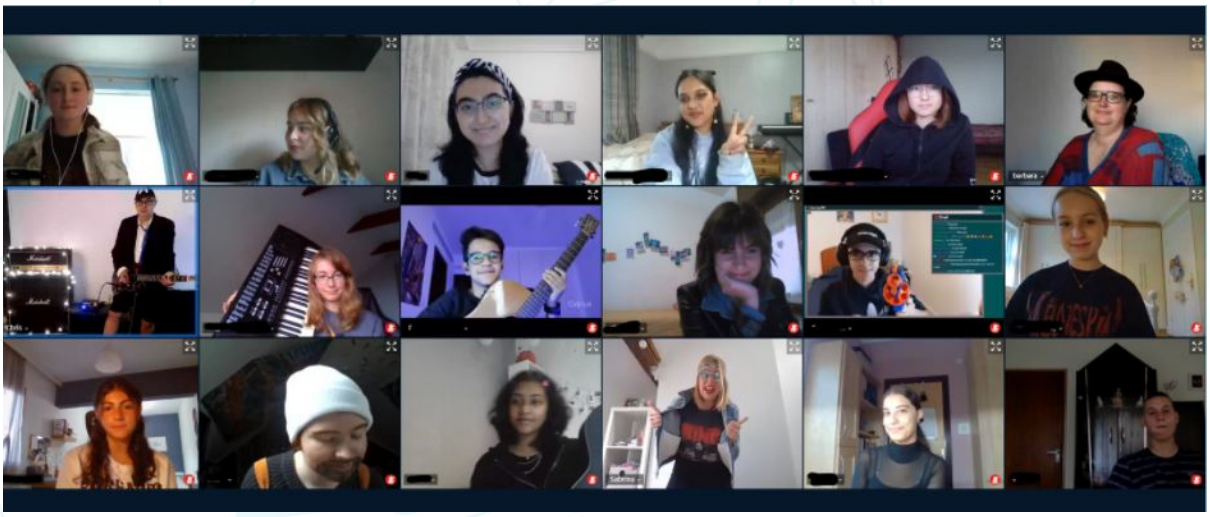
June then updated on next steps. She commented that consultation with young people is something which the European Commission is aiming to mainstream to ensure that the voice of youth is heard across a wide range of policy areas. She confirmed that the outputs from the consultation are being used for two purposes. The first is a set of digital principles, agreed between the Commission, the Parliament and the Council, which will serve as a guide to policy makers and other actors, such as industry, across the EU. It is anticipated that there will be references to the empowerment and protection of young people within this, which is due to be published before the end of the year. The second is the update to the BIK Strategy which will be launched in the second quarter of next year; outputs from the Forum and ongoing consultation work with a whole host of stakeholders will ensure that a range of perspectives are considered.

The final word of the Forum went to **Yvo Volman, Acting Director of the Data Directorate, DG CONNECT, European Commission**. He reiterated the commitment of the European Commission in terms of creating a better, safer, more inclusive and ethical digital space for children and young people in Europe, commenting that the Forum represents a starting point for ongoing work, and in particular the update of the BIK Strategy. He further reflected on the vast policy work that has already taken place in recent years in terms of actions, initiatives and proposals to help our children seize the opportunities of the digital world in a safe way. Trust and confidence in digital skills will be key as we move forward. He thanked participants and called on all present to continue the important work which they are doing to create a digital space that our children deserve, for both this and future generations.

Annex 1: BIK Youth Panel 2021

In the framework of the Better Internet for Kids (BIK) project, each year, a BIK Youth Panel is organised prior and during the Safer Internet Forum (SIF), encouraging a group of youth panellists to voice not just their personal opinions and challenges regarding safer/better internet issues, but also those of their peers whom they are representing at a European level. The BIK Youth Panellists are typically involved in other activities too at both national and European level, with many of them going on to become BIK Youth Ambassadors, representing the BIK agenda at high-level events such the annual **Internet Governance Forum (IGF)**.

As a result of the ongoing travel restrictions and safety measures in place due to the COVID-19 pandemic, the BIK Youth Panel was once again organised online in 2021. Similar to the previous year, a suite of secure open-source online meeting and collaboration tools, which included the BigBlueButton videoconferencing tool, Nextcloud document storage, PeerTube video sharing platform and Matrix chat client, among others, were set up for the purposes of BIK Youth Panel 2021 activities.

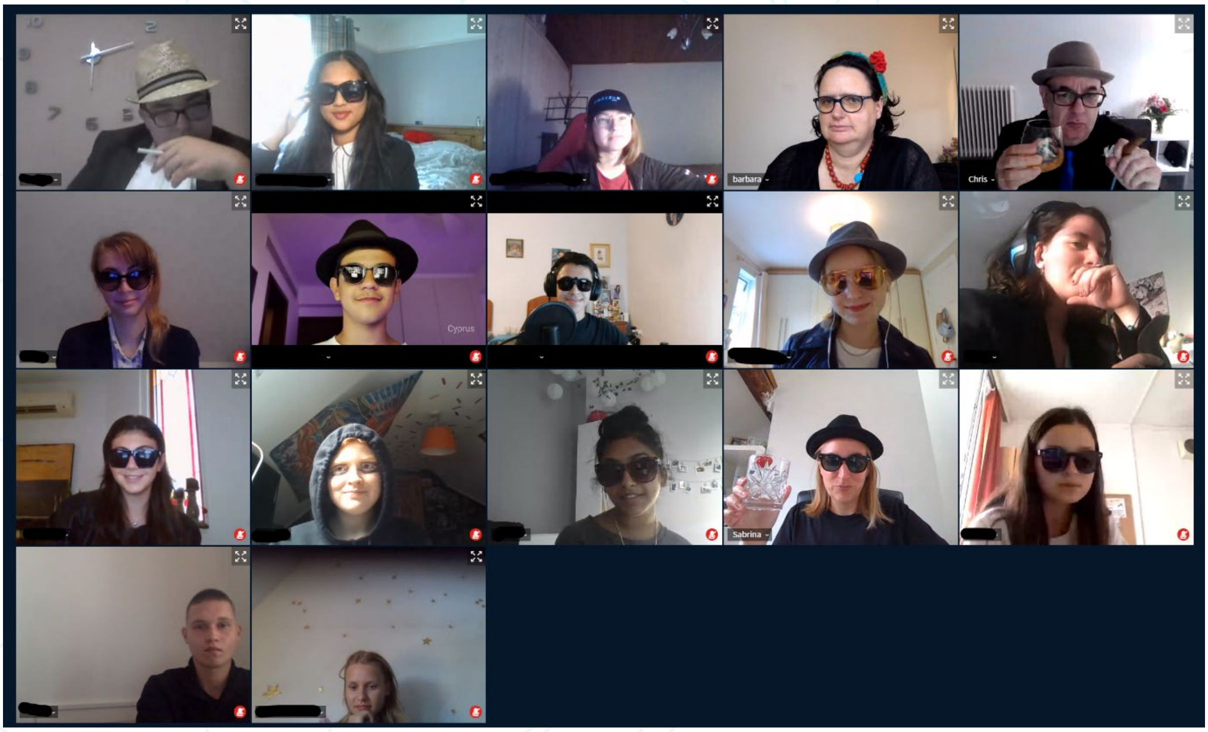


Approximately two months prior to the Safer Internet Forum, 32 young people from 19 countries joined a total of six preparatory online meetings, where they identified the topics they would like to focus on and the groups they would be working in. Throughout these meetings, BIK Youth Panellists started to work out the details of how to present their topic in a video presentation. With guidance from privacy expert Chris Pinchen and Austrian Safer Internet Centre Youth Coordinator Barbara Buchegger, panellists created their video script for three diverse topics which explored the following questions:

- Why is it important to create a better online school environment?
- Why is our data being collected?
- How do we wish the internet to look in 2031?

Click on the links above to view the youth panel videos as published on the Safer Internet Forum 2021 section of the Better Internet for Kids (BIK) website.

To make the preparatory online meetings a more fun experience for the youth panellists and to establish a more relaxed work environment for them, the 'theme nights' approach adopted last year was continued. During these nights, everybody dressed or presented skills based on a pre-selected theme. These ranged from musical instruments to favourite hats, and from pyjamas to a beach party, as seen in the image below:



Following the conclusion of preparatory meetings, two days of BIK Youth Panel activities, which would traditionally take place in Brussels prior to SIF, took place online on 4-5 October 2021. Panellists used most of these two days to finalise their videos and to prepare for their presentations during SIF 2021.

On the afternoon of 5 October, a pre-event to the SIF was organised. During this pre-event, the outcomes of the #DigitalDecade4YOUth consultation was presented followed by a youth-led discussion with the 2021 BIK Youth Panel. As part of the session, participants had the opportunity to discuss the future of the internet with BIK Youth Panellists and engaged in more in-depth discussions on the following topics in breakout rooms:

- Online school environment.
- Social networks and advertising.
- Online society.
-

Read more about the BIK Youth Panel 2021 on the Better Internet for Kids (BIK) website or find out more about the BIK Youth programme generally at www.bikyouth.eu.