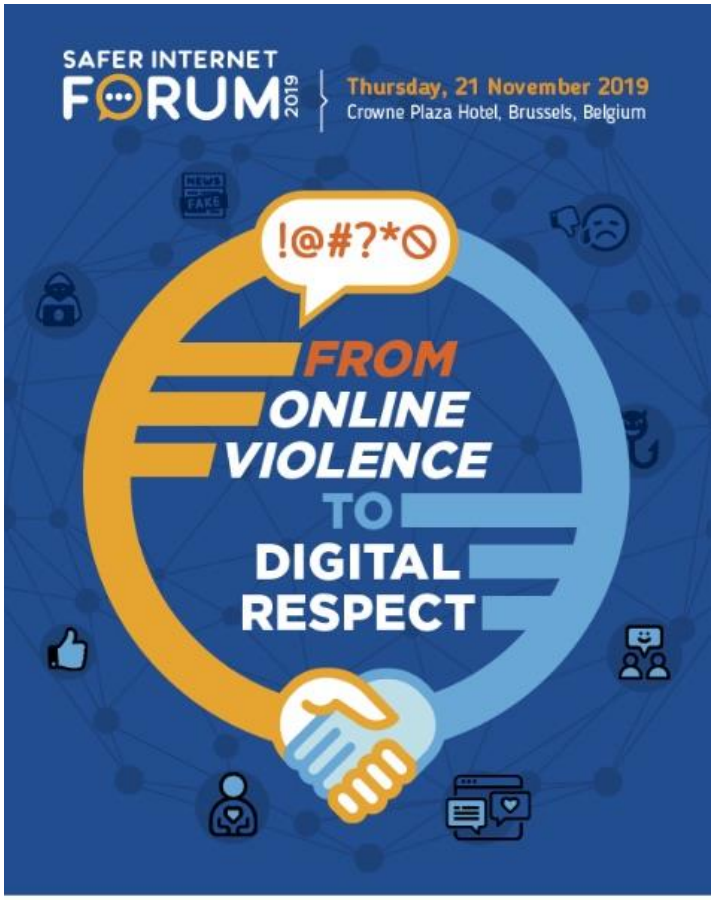
Report on the proceedings of Safer Internet Forum 2019

Thursday, 21 November 2019
Brussels, Belgium

(including an annex on the preceding BIK Youth Panel)



European Commission

INHOPE insafe

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

Table of contents

Introduction

Building on the European Strategy for a Better Internet for Children, the Safer Internet Forum (SIF) is an annual international conference delivered under the Connecting Europe Facility (CEF). Bringing together young people, parent and teacher representatives, industry and government policy makers, technological and awareness-raising experts, and political, educational and social leaders from Europe and beyond, this one-day event takes a multi-stakeholder approach to considering the impact of technology on individuals and society.

Following a welcome by the European Commission (EC), SIF 2019 opened with a keynote address during which Thordis Elva, writer, speaker and journalist, first provided an overview of the key issues at stake when considering online violence, including online hate speech, image-based sexual violence, and other forms of technology-facilitated gender-based violence. She then went on to elaborate on some of the strategies and resources that have already been put in place to address the issues, including the role that government, policy makers and regulators can and are playing, while also looking at some of the successful campaigns that have raised awareness of the issues. During her keynote, Thordis shared examples of good practice and gave a call to action for participants to reflect on what they can do to encourage and foster digital respect.

Given the importance of youth participation in the Safer Internet Forum, the opening keynote was followed by a youth-led session. Starting from a broad understanding of what digital violence and respect means to them, BIK Youth Panellists delivered an upbeat and interactive session using the "flipped classroom" model with the aim of shifting the consultation perspective. In advance of SIF, BIK Youth Panellists have been working collaboratively to identify a set of concrete problems, based on their personal views and experiences of digital violence. During the session, they shared some of the challenges they face, while explaining how digital respect should look in order to make a difference. Forum participants then took part in small-group discussions – together with the young people present – in order to deepen their understanding of what is at stake, while building towards remedial strategies and solutions.

The afternoon was given over to a series of highly interactive "deep dive" sessions. Through detailed discussion, debate and practical exercises, forum attendees had the opportunity to explore issues around online sexual violence and misogyny in gaming; sexual violence against men and boys; online sexual harassment (with a focus on the successes of the deShame project, which aims to increase reporting of online sexual harassment among young people, and improve multi-sector cooperation in preventing and responding to this behaviour); online hate (with a focus on the SELMA project, which builds upon a social and emotional learning (SEL) approach to empower young people to become agents of change); and using AI as a solution to some of the problems encountered.
A parallel deep dive stream, INHOPE@20, provided a celebration of the work of the INHOPE network as it turned 20, reviewing what has been achieved over that time in combatting illegal online content and, specifically, child sexual abuse material (CSAM).

The final plenary session of the day showcased a number of inspiring stories of how young people have used social media and online platforms to bring about positive change. Emma Holten was a victim of nonconsensual pornography back in 2011; she then launched an online campaign/activist project to successfully raise awareness of the issues. Gina Martin was a victim of upskirting and successfully campaigned to change UK law and make this a crime. Her success has spurred on lots of others across the world to take similar action. Sara Sjölander worked on an online harassment platform Näthatshjälpen, where victims of hatred and harassment online can get support and advice on specific situations. She is also working with Flickaplattformen, an organisation that fights to improve the life of girls.

Following the formal close of the day by the European Commission, participants were warmly invited to remain for a reception, hosted by INHOPE in celebration of its 20 years of operation.

SIF 2019 was an opportunity for participants to:

- keep track of emerging online safety trends and issues,
- facilitate knowledge, experience and good practice sharing, and
- establish opportunities to collaborate with others on new ideas, resources and projects.

We hope that participants found it to be both a thought-provoking and inspiring day and look forward to continuing to work with a wide range of stakeholders in the future, to continue the mission of creating a Better Internet for Kids.

Find out more at www.betterinternetforkids.eu.

Welcome by the European Commission

Speakers:

- Lora Borissova, Head of Cabinet of European Commissioner for Digital Economy and Society Mariya Gabriel, European Commission
- Gail Kent, Director, Directorate Data, DG CONNECT, European Commission

Karl Hopwood from the Better Internet for Kids (BIK) Team at European Schoolnet (EUN) opened the Safer Internet Forum (SIF) and welcomed all participants, mentioning that this year's SIF is the largest it has ever been. Creating safe spaces online is a priority for the European Commission (EC), which funds the BIK project. As such, Karl gave the floor to two representatives of the EC – Lora Borissova, Head of Cabinet of European Commissioner for Digital Economy and Society Mariya Gabriel, and Gail Kent, Director of the Directorate Data at DG CONNECT.

Lora Borissova began her address by thanking and welcoming all of the dedicated participants to SIF, whether they are researchers, education professionals, young people, Safer Internet Centre (SIC) representatives, policy makers, and so on. She wondered whether we are moving from homo sapiens to homo digitalis.

Over recent years, the EC has attempted to contribute actively to online safety, emphasising the key values of dignity, respect and solidarity which are fundamental offline and also apply online. In that context, the EC launched the #DigitalRespect4Her campaign earlier in 2019, aiming to *"raise awareness about online violence against women and promote good practices to tackle this issue"*.

With one in ten women having experienced unwanted behaviour online, online safety cannot be taken for granted. The good news is that European countries are united to face borderless digital challenges together, and policy makers need to collaborate and make digital transformation a success, while protecting children. Making Europe fit for the digital age is a high priority on the EC's agenda, as are children's rights.

Commissioner Mariya Gabriel will shortly inherit a new portfolio, which will help equip people with the knowledge, the skills and the experience they need to thrive in the digital age. Interinstitutional cooperation is also important; the EC works together with institutions such as the Council of Europe (CoE), for example. Lora Borissova highlighted, in particular, the work of the INHOPE network in preventing child sexual abuse online, which builds upon the United Nations Convention on the Rights of the Child (UNCRC), and the CoE's conclusions on fighting against the sexual abuse of children. Lora Borissova also welcomed the young representatives from 20 European countries taking part in the BIK Youth Panel.

Gail Kent, Director of the Directorate Data at DG CONNECT thanked the Commission for their work on the BIK project and stated that DG CONNECT's efforts strive to empower young people to fully benefit from digital technologies. Gail Kent also thanked the event coordinators from European Schoolnet. She then gave an outline of the proceedings of the day and congratulated the INHOPE network for their being the first line of activity to be funded under the first BIK programme in 1999. Over these 20 years of activities, there has been a strong paradigm shift from the protection of children online, to their empowerment as active creators. This again links to the UN Convention on the Rights of the Child which states that children have a right to active participation and creative expression.

Gail Kent also mentioned the involvement of many young people in the SIF, outlining in particular the youth-led flipped consultation, and the final plenary session on young people use social media platforms to effect positive change – on that point, Gail Kent emphasised the very tangible benefits of positive online content (POC) in our "real", offline lives.

To close this welcome address, Gail Kent introduced the keynote speaker, Thordis Elva, writer, speaker and journalist from Iceland, who fights against the abuse of women and girls and supports the #DigitalRespect4Her campaign.

From online violence to digital respect

Keynote speaker: Thordis Elva, Writer, speaker and journalist

Panel:

- Frida, BIK Youth Panel 2018 and 2019
- Roger Loppacher, President, Consell de l'Audiovisual de Catalunya (CAC)
- Thomas Myrup Kristensen, Managing Director EU Affairs, Facebook
- Stephen Turner, Head of Public Policy, Government and Philanthropy, Twitter

Chair: June Lowery, Head of Unit, Accessibility, Multilingualism and Safer Internet, DG CONNECT, European Commission

Thordis Elva is a writer, speaker and journalist from Iceland. She observed a lack of discussion in Iceland around issues related to harmful online content or intimate topics and so, to address this, she has deployed several initiatives. She has published two books on gender-based and sexual violence, which were published in 14 countries. She is also the author of three award-winning, educational short movies about online abuse and image-based exploitation, bodily integrity and sexual consent. In her country, she is a member of a parliamentary committee overseeing the national action plan against violence against women and children, and she was commissioned by the Icelandic government to make educational material for children and teenagers to prevent sexual abuse. From 2012 to 2014, she has been the Chair of the Board of the shelter for battered women and girls in Reykjavik – she has been a board member since 2010. She has been a prominent public speaker for two decades, delivering a TED talk about her personal connection to the issue of sexual violence – the video has been watched over 5 million times to date. Thordis has also given

workshops to 18,000 people in five countries about image-based sexual abuse online. She has been working within the media for 15 years, including on television, on print and online.

Thordis Elva opened her keynote speech by providing an overview of the challenges faced by children and young people online, with a focus on the online abuse of women and girls. The internet has revolutionised how we communicate, including in areas such as banking, education, health and so on.

Gender equality is a persistent problem, both offline and online. It manifests itself in many forms. Women are underrepresented in the media and in the political arena – they hold only 24 per cent of the world's parliamentary seats, and only a quarter of the people featured in European news media are women. The gender pay gap is significant, since it remains in double digits even in the most gender-equal countries. Additionally, unpaid labour and housework is still largely in the hands of women.

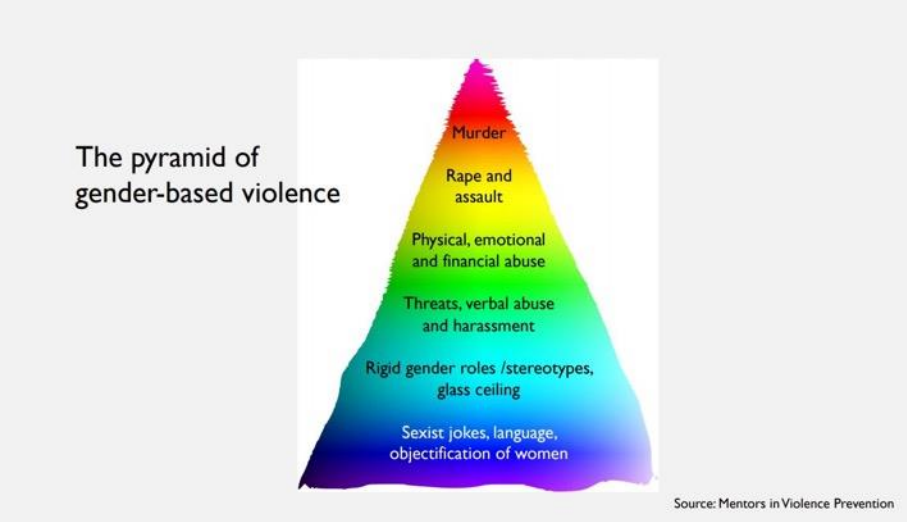
The fact that women own less and have less influence than men is a result of laws and traditions that made it impossible for women to inherit property, educate themselves, vote or otherwise have full citizenship and civil liberties.

Globally, one in three women is subject to physical and/or sexual violence at the hands of a man in her lifetime. According to the UN Broadband Commission, women and girls are 27 times more likely than their male counterparts to be abused. 73 per cent of women have endured online violence, and this figure rises even more when we consider minority groups (LGBTI, ethnicity, disability). Moreover, women aged 18-24 are at an increased risk of being abused online. In the EU-28, 18 per cent of women have experienced a form of serious internet violence since the age of 15, which corresponds to about 9 million women.

The consequences of this online abuse are very real. 41 per cent of women who experienced online harassment felt that their physical safety was threatened. According to figures established by Amnesty International, 1 in 2 women experienced lower self-esteem or loss of self-confidence as well as stress, anxiety or panic attacks as a result of cyber violence and hate speech online. Even worse, the risk of suicide attempt is 2.3 times higher for a victim of cyber harassment compared to non-victims, according to UNICEF. Meanwhile, the FEMM Committee (the European Parliament's Committee on Women's Rights and Gender Equality) reports that illegal online hate speech targeting gender identity makes up only 3.1 per cent of reports to internet platforms in the EU, clearly indicating that the online abuse of women and girls is an underreported problem.

Thordis Elva conceptualised it as a continuum, defined as a "continuous series of elements or items that vary by such tiny differences that they do not seem to differ from each other". In that context, she introduced the pyramid of gender-based violence. The most extreme elements at the top (murder) are resting on and enabled by all the other layers – rape and assault; physical, emotional and financial abuse; threats, verbal abuse and harassment; rigid

gender roles and stereotypes, glass ceiling; sexist jokes, language, objectification of women, and so on.



Thordis Elva then went on to examine how exactly gender-based violence is manifested online. First is verbal violence, which takes the form of sexist hate speech, defined as all the expressions which spread, incite, promote or justify hatred based on sex, as well as the use of sexist and insulting comments, slut-shaming and victim-blaming. It can also be mob attacks. Cyberbullying is also frequent; in this case, a person is targeted by repeated aggressive online behaviours with the objective of frightening and undermining that person's self-esteem or reputation – which sometimes pushes vulnerable individuals to depression and suicide. Cyberharassment is another common phenomenon, including unwanted sexually-explicit emails, text (or online) messages; inappropriate or offensive advances on social networking websites or internet chat rooms; threats of physical and/or sexual violence by email, text (or online) messages; hate speech, meaning language that denigrates, insults, threatens or targets an individual based on her identity (gender) and other traits (such as sexual orientation or disability). Cyberstalking consists of monitoring someone using electronic means with the intent to cause fear and/or distress. Finally, doxxing consists of publishing someone's personal information without their consent.

Next to verbal violence, there is graphic violence. This category manifests itself in the form of image-based sexual abuse (also known as revenge porn), including fakes and upskirting; unsolicited nudes (including "dick pics"); sextortion, which consists of using intimate material as a means of blackmail; hacking; impersonation (for example, stealing someone's identity and using it to advertise prostitution); trafficking and recruitment; and child sexual abuse (including "grooming").

Men and women can both experience violence online, but it affects women much more and has heavier consequences on the lives of women, possibly because the violence directed at

women often has sexual undertones and runs deeper. According to the Swedish Centre of Crime Prevention, 70 per cent of online harassers are men. According to the Pew Research Centre, men are also affected by online abuse, but it is more at the surface level (with name-calling being the most frequently reported form). Men are less likely to find it upsetting (only 16 per cent of them find it "very" or "extremely upsetting"). Meanwhile, 63 per cent of women who had experienced online abuse said they had not been able to sleep well as a result of it. Well over half (56 per cent) of women said online abuse or harassment had meant that they had been unable to concentrate for long periods of time, according to a study by Amnesty International.

Amnesty International showed that this phenomenon leads women and girls to self-censor; they take precautions to prevent sexual violence, which affects their participation in society. To be precise, 76 per cent of women who said they had experienced abuse or harassment on a social media platform made changes to the way they use the platforms. This includes restricting what they post: 32 per cent of women said they had stopped posting content that expressed their opinion about certain issues.

The result of this is a loss of millions of euros, because gender-based online violence engenders lost wages; reduced participation in society; chronic physical conditions and loss of life expectancy; mental health conditions; sexual and sexual health issues, sometimes causing problems with reproductive health; substance abuse and organised crimes; social isolation; and individual and public expenditure on medical protection, judicial and social services. Regarding cyber violence happening in the context of intimate partner violence, researchers from the YWCA (Young Women's Christian Association) have estimated the cost associated with responding to technology-based victimisation to be *"$1,200 compared to $500 for survivors of non-technological abuse"*.

Much more importantly, the future of the planet is at stake – women are much more affected by climate change now, and they will be too in the future. Simultaneously, they are silenced much more than before, so their voices are more needed more now than ever.

Thordis Elva then mentioned the famous internet expression *"do not feed the troll"*, which normalises violence and leaves victims silent. Studies have shown that female users are "feeding the trolls" just by existing as women in the online environment.

- Having a female name – a study by the University of Maryland's A. James Clark School of Engineering found that chatroom participants with female usernames received 25 times more threatening and/or sexually-explicit private messages than those with male or ambiguous usernames.
- Expressing an opinion, especially on topics like politics, religion and feminism, as seen in higher levels of abuse towards female journalists, bloggers, politicians and activists.
- Uploading a picture of yourself.

As such, for women, the only guaranteed way to avoid abuse is not existing at all. In addition, Thordis Elva questioned the whole conception of "trolls", saying that *"by calling a person who shares hateful views towards women and girls online a "troll", we are giving them a name we would not give them in the offline world. This creates the misconception that "trolling", which involves trying to install fear in women and girls via threats, humiliation and silencing tactics, thereby undermining their agency and right to participate in democratic society, is an online phenomenon. But there are no trolls. What we have are people with sexist beliefs, misogynists who threaten women's rights online as well as offline."*

Instead, how can women and girls react to online hate? Thordis Elva suggested building communities to defend one another and speak up. There is not one single way to respond to all attacks. Ignoring the abuse is an option, but it should not be the only one nor should it be the most common one.

Thordis Elva then moved on the topic of sexting – defined as consensual sexual communication – often photographs – that depict nudity or have a sexual undertone. Indeed, sexting is becoming more and more common place (54 per cent of young people in a US study have received or sent sexting messages before the age of 18).

Regarding the motivations for sexting, participants to the "Ungt Folk 2018" study of 10,450 Icelandic teenagers revealed that there are positive aspects to it. It is a way of expressing sexual desire in a consensual relationship; of having sexual relationships without the risks of sexual acts in person; of obtaining sexual pleasure easily; and of discovering one's sexuality. Some girls also mentioned that sending nude photos is a form of initiation into sexual maturity and girls often feel pressured into doing it. Indeed, girls experience six times more pressure than boys to share sexually-explicit content – this puts them at heightened risks of "revenge porn" (which is a misnomer and should be named as the assault that it actually is).

The sharing of nude and sexual imagery online poses great problems since 88 per cent of sexually-explicit material takes off when uploaded to the internet. 17.5 per cent of sexually-explicit photos depict children under the age of 15, and 7.5 per cent depict children under the age of 10. A growing number of children post such photos; the majority of them girls, according to the Internet Watch Foundation (IWF). The sharing of nude and sexual imagery without consent, also called "revenge porn" (although inappropriately, as is "non-consensual pornography") is the result of different things. It can stem from hacking or theft, or the photos may have been shared with consent, before being forwarded or distributed without consent or even without knowledge. It can also be the result of coercion, grooming,

blackmail/sextortion, or violence. It can be taken/filmed without the photographed individual's knowledge or be the result of digital manipulation. It embodies the next generation of sexual violence.

When image-based sexual abuse meets doxxing, it very easily leads to a reputation hijack that can limit the victim's employment, social and economic status. Thordis Elva also mentioned fakes, emphasising that "not taking nudes" is simply not a solution anymore. When a person's intimate pictures (whether real or fake) are online, it also creates the possibility of the sexual assault being replicated, which makes it especially psychologically harmful for the victim. As such, such abuse has very real consequences, with some young girls going as far as committing suicide because of it.

Thordis Elva also said that we should address the elephant in the room that is the effect of pornography, especially the prevalence of violence in porn and the early contact children have with (violent) pornography. Educational materials about this exist, but they are not widely distributed.

So what can we do? Thordis Elva mentioned several avenues for action: education; local resources for victims of online violence; legal frameworks and law enforcement; and synergising treaties and collecting data.

In terms of education, children need to be educated on the rights and responsibilities that come with their digital citizenship, by putting it on the curriculum in schools. Words like "trolling" need to be replaced with terms that fully hold the assaulters accountable, like "hate speech" and "harassment". Media literacy should be integrated to school curricula, if that is not already the case. Traditional sex education should comprise age-specific digital sex education, with an emphasis on consent, if that is not the case already. Education stakeholders should invest in awareness campaigns for parents and for wider society in collaboration with stakeholders (NGOs, victim support groups, and so on) about what online abuse/harassment is; what cyber civil rights are; how to report online abuse/harassment; and where support is available in case of online abuse/harassment.

In terms of local resources for victims of online violence, governments should invest in these by:

- Strengthening organisations/NGOs/initiatives that offer support services to victims, including psychological help.
- Maintaining a hotline or 24/7 reporting service that can help victims of online abuse, with skilled staff who can react immediately to help stop the spread of harmful material.
- Making removal help available in the local language for victims of image-based sexual abuse – in that regard, Thordis Elva pointed to the removal guides from the Cyber Civil Rights Initiative.

In terms of legal framework and law enforcement, a gender perspective should be applied when writing and adapting existing laws that criminalise all forms of online violence, including re-sharing or harmful content, as well as of threats to do so. Criminal and civil causes of action should protect the privacy of victims, avoiding the secondary victimisation that comes with having their case made even more public. Image-based sexual abuse should be treated as a sex crime and anonymity should be extended to victims. As online abuse consists of cross-border crimes, synchronising the definitions of online abuse would be helpful in terms of collaborating in the pursuit of perpetrators, swapping best practices and conducting international comparisons. Authorities should ensure effective regulation on internet intermediaries that prohibit any forms of violence against women, in accordance with local law and international treaties. Governments should hold social media platforms to account when it comes to preventing and removing online abuse. They should also equip law enforcement with the funding, technical equipment, knowledge and personnel resources needed to effectively handle cases of online abuse.

In terms of synergising treaties and collecting data, Thordis Elva pointed to the different legal documents that mention online violence against women:

- The Budapest Convention on Cybercrime and additional protocol (2001) – three articles of the Budapest Convention can apply to cyber violence against women, including article 4, 5 and 9.
- The Istanbul Convention (2017) – several articles of the Convention can be applied to the specific topic of digital violence, including articles 33, 34 and 40.
- The Lanzarote Convention – the Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse requires criminalisation of all forms of abuse against children, including online abuse.
- Image-based sexual abuse could fall under the GDPR (General Data Protection Regulation) provision on “processing of personal data” and would consequently trigger application of the Regulation. The individual responsible for uploading image-based sexual abuse material as well as the publisher of such material could be considered joint data controllers, and hence fall under the obligations and sanctions imposed by the GDPR (154).
- The Treaty on the Functioning of the European Union (TFEU) includes the possibility to develop legislation on violence against women in the framework of judicial cooperation.
- Last but not least, both the Istanbul Convention and the Victims’ Rights Directive require Member States to report statistical data and to produce gender-disaggregated data on cyber violence and hate speech.

Thordis Elva thanked the participants for their attention and the panel discussion ensued.

Roger Loppacher, President of the Consell de l'Audiovisual de Catalunya (CAC) thanked Thordis Elva and introduced the CAC's work on fighting online violence. The CAC began monitoring risk content on platforms, focusing on identifying content that is harmful to minors. They set up the eduCAC programme, offering educational resources to primary and high schools and to families. The topics identified as harmful content are content that promotes anorexia; incitement to the hatred of women; content that incites to suicide; content that promotes child sexual abuse; incitement to hatred of LGBTI people; content that promotes gambling and betting; content that promotes cyberstalking women; and content that sexualises videos of minors.

Roger Loppacher gave the audience a brief overview of the scale of the problem, and what the CAC usually does to respond, such as reporting to platforms, complaining to the public prosecutor's office, carrying out public presentations with partners, and drafting guidelines. He also talked about a programme the CAC created called eduCAC, developed in collaboration with the Department of Education of the Generalitat, the Professional Journalists Association of Catalonia, the Catalan Audiovisual Media Corporation, and "La Caixa" Bank Foundation. eduCAC offers educational resources to primary and high schools and to families, with the aim of fostering a critical attitude towards audiovisual content and promoting responsible use of mobile devices.

In this context, the CAC, the Catalan Audiovisual Corporation and "La Caixa" Bank Foundation developed the awareness campaign #AMiNoMenganyen (They don't fool me), a message to empower young people in their screen use. The overall aim is to encourage critical analysis and responsible technology use.

A group of Catalan influencers and YouTubers (together accumulating 1 million followers) will participate in the campaign, giving their take on the internet and social network use via Instagram, YouTube and TikTok stories.

Frida, BIK Youth panellist in 2018 and 2019, said she recognised these challenges very well through the eyes of youth, since young people encounter these types of violence, as perpetrators or as victims. According to her, talking about such issues is fundamental, whether at home or with friends. In her Finnish high school, such topics are part of ICT classes. She believes education is the best way to tackle these problems, and it cannot start early enough – it should start from an early age and be lifelong.

Stephen Turner, Head of Public Policy, Government and Philanthropy at Twitter thanked Thordis Elva for the "reality check" she provided through her presentation. He reflected on how his own ICT education was very skill-based, and how necessary it is to take into account communication and interaction online.

Young people use Twitter quite differently from older people, and Twitter tries to keep the public conversation free of abuse, without silencing any voices as a result of receiving hatred. Twitter is trying more proactively to take the responsibility off the individual. He said that more accounts are being reported and removed, but Twitter is also trying to minimise individual users' exposure to malicious content and hate speech. For example, changes were made in 2017, such as notification filters and safe search, which aim to find that harmful one per cent of content and keeping it away from users.

The most important progress Twitter is currently seeing relates to the improvements made to the way in which the company communicates with people who violate the user agreements. Since the initiative commenced, among this group of users, 65 per cent have

not violated the rules again. This goes to show that building a knowledge base and raising awareness work, as do providing education and resources for educators, and collaborating with other online services within the ICT Coalition.

Thomas Myrup Kristensen, Managing Director of EU Affairs at Facebook, said prevention and first aid are important, but education remains key. Facebook takes the fight against online violence seriously; it is embedded in the platform's Community Standards. Facebook is currently experimenting with the right way of tackling these issues, relying both on humans and artificial intelligence (AI). However, it is not possible for one company to do it all on their own, the whole community needs to be involved. Thomas Myrup Kristensen mentioned the example of the community helping to build features such as muting messages, or super-blocking people.

Thordis Elva replied that these testimonies create the hope that technology is evolving, but in order for such tools to work, the community has to have faith in such technologies. She stated that, currently, the numbers are not very promising, especially for females.

After these presentations, a Q&A session ensued, facilitated by June Lowery, Head of Unit, Accessibility, Multilingualism and Safer Internet at DG CONNECT. The panel was asked whether industry players communicate with one another to remove content across services. Stephen Turner replied that Twitter has been building up more collaboration, it is formalised for some topics – terrorist content and child sexual exploitation – but for others, such as harassment and safety, it needs to be improved. All platforms are different in their approaches, and each user is specific in its use of the service. However, this is evolving positively, with consultations between YouTube, Twitter and Facebook; while it can be difficult to involve smaller services, this is the next step. Thomas Myrup Kristensen added that there is no central database for illegal content, although it does exist for terrorism. Facebook also trains smaller companies to remove content in an adequate and efficient manner. Facebook has an interest for people to feel safe, as they want them to communicate freely on Facebook. Reporting is only one tool; AI has the potential to help so much. Frida agreed that harmful content is everywhere; it cannot be stopped, despite significant education efforts being made in Finland.

June Lowery then asked the panel whether the industry have an idea of why people engage in violent online behaviour. Stephen replied that it can be difficult to see patterns, especially for a platform that covers a broad variety of different regional contexts. However, some are evident, such as mob harassment. The panel was then asked whether platforms would consider blocking sexualised keywords from being sent to children and whether this would work across languages. Thomas Myrup Kristensen replied that Facebook has all languages covered and they do look at specific slurs, trying to figure out which ones cross the line – these are then detected automatically.

June Lowery then asked Thordis Elva about women who lose their confidence in the early teenage years, and how she builds their confidence in her workshops. Thordis Elva replied that there is no simple answer, but that she underlines that everyone has equal worth. She highlighted the fact that it is no coincidence that women's confidence levels drop at the exact age when they start being sexualised by the outside world. It is important to empower them to be active participants in a democratic society.

June Lowery thanked all panellists and concluded the session.

Flip the consultation – a dialogue led by youth

Panel: Better Internet for Kids Youth Panellists

In line with the theme of the day, the BIK Youth Panel began their session with a striking "slur word performance" and a theatre play about scenarios Insafe helplines encounter. After this performance, the panellists welcome the participants and introduced the group, comprising of 26 young people from 20 countries across Europe (see more about the formation and preparation of the BIK Youth Panel in Annex 1). They kicked off with an interactive session with table discussions around the room, each led by a youth panellist.

After these discussion, each youth panellist reported back in plenary on their chosen theme and the discussions that took place at their respective tables. Key topics and issues included:

- Self-harm content – we have to distinguish harmful from violent content.
- Doxxing – we have to realise that online and offline are part of the same world.
- Sexting – education is key.
- Cyberbullying – this phenomenon should be seen from all perspectives and tackled at all ages.
- Identity theft – to prevent identity theft, you should not reveal too much information online.
- Online sexual harassment of youth – we should listen to each other. Education is key, even for adults, in order to empower them to talk to young people in the right way.
- Identity theft – don't be lazy; be careful with your data!
- Cyberstalking – this problem is unavoidable, but users can take precautions when sharing their personal data.
- Peer pressure – talk about it and open up, use hashtags, create solidarity.

- Cyberbullying – victims need help, but so do the bullies. Boost young people's self-confidence at school to open avenues for talking about it. Prevention efforts are needed through education and Social and Emotional Learning (SEL), and social media platforms need to be more pro-active.
- Online violence in video games – teach players how to be careful during bans.
- Online harassment on social media – everything starts with education.
- Trolling and anonymity – anonymity makes everything easier; it has good and bad aspects.
- Hate speech and hate crimes – it has real consequences offline and should be treated as such. It is an intersectional issue that needs government solutions.
- Harassment – government solutions are needed.
- Private content – be careful when posting online.
- Fake profiles – distinguish between harmful and helpful fake profiles.
- Representation in the game industry – more diversity is needed in games and among game developers.
- Nude photos – educate children on what to do about it at an early age, teach them how the community can help them, and be clear about the possible consequences.
- Sexting – it is not violence in itself, but we need increased education about its various forms, and we need to address parents as well.
- Hidden marketing – we need to create awareness and better guidelines for apps.

After this, Frida called upon all stakeholders present in the room to take responsibility for keeping children and young people safe online. She underlined the importance of building a community, and having open ears for those that are targeted by online violence in any form.

The youth panellists then presented their Instagram account, BIK.YouthforYouth, and examples of what they have been doing during five weeks of preparatory meetings preceding the SIF. When asked by a member of the audience whether they are on other social media platforms, they replied that the campaign was carried out only on Instagram, but that the BIK Youth Panel is also carrying out a take-over of the @BIK_Youth Twitter account on the day of the SIF. They were then asked at what age they think education should start; in which form they experienced that; what works and what can be done better. One of them replied that educating adults is key, so that they can educate children adequately regarding online risks. As such, education efforts should start as soon as kindergarten, if possible.

Another question from the audience related to the reasons why some people do not feel comfortable talking to their parents, and what parents can do better. A youth panellist replied that everyone's parents are busy, so they might feel like they are wasting their time. Also, young people often feel like their parents will not be able to help them with problems encountered online so, once again, educating parents is key. Moreover, some issues online can also be very personal. They explained this miscommunication with parents by the fact that the internet became mainstream not so long ago and, as a consequence, they are the first or second generation to face these brand new issues. Their parents have not and, as such, they cannot relate to their problems, and generally go for the easy solution: they advise their children not to use the internet altogether.

Another question from the audience related to what the young people would miss most if they lost their phone. Among the replies given by the young people were the ability to communicate with parents, grandparents and friends; keeping up to date with schoolwork; and developing their creativity and sharing their work with others.

Another member of the audience asked them whether they would find awareness-raising videos for adults about specific issues encountered by young people online interesting. The youth panellists replied that it would be, as it takes away the personal side which can be embarrassing. They also suggested giving parents tips on how to talk about common issues, so that they can start the conversations. Parents have to realise that it is their problem too, even if they themselves did not grow up in the digital age.

After receiving many congratulations from the audience, the youth panellists thanked the attendees. Karl Hopwood thanked them and invited them on stage, highlighting the importance of involving young people in the discussions around their own online safety.

Deep dive sessions

DD1: Online sexual violence and misogyny in gaming

Session leader: Lavinia McLean, Head of the Department of Humanities, Technological University Dublin

Lavinia McLean, Head of the Department of Humanities at the Technological University Dublin began her session by providing an overview of female gamers' experiences of harassment in online gaming. There has been a lot of research on that topic; an interesting statistic is that female gamers represent almost half of those who play videogames, according to a study carried out by United Kingdom Interactive Entertainment in 2016. The social aspects of gaming are becoming a significant motivational factor for both men and women, according to another study conducted by the Entertainment Software Association in 2018. The structural factors within gaming encourage players to increasingly seek social interactions. There are individual differences depending on the partners the player communicates with during gaming. The aim of this deep dive session was therefore to look into how negative social interactions impact women.

Social interactions are numerous and important in gaming. Gaming strengthens pre-existing relationships (for example, a female gamer is introduced to gaming by her father or brother), and emotionally sensitive players make more online friendships. Studies have shown that social support in gaming represents a significant motivation for female gamers. However, female gamers in particular also have many negative interactions in gaming, such as harassment and sexual harassment; sex role stereotyping; cyberbullying (which has been proven to be higher among female and LGBTI gamers); and linguistic profiling (hearing the

female player's voice). Females reported being treated differently to male gamers in online gaming, often excluded, and they felt like their value is not recognised, even though they are doing well in the game. The threat of being stereotyped led many female gamers to underperform in games, and notably to avoid using their microphone to communicate verbally with other players.

After this presentation, Lavinia McLean organised an activity with participants, who split into groups. She presented three different female gamer profiles, and distributed a set of quotes to each group. Based on these quotes, participants had to describe the person's gaming identity: whether they are a serious gamer, a non-gamer, a part-time gamer, or a female gamer. They also had to consider the gamer's behaviour online, other people's behaviour towards them, and what impact this had. Based on this information, participants had to guess which female gamer profile the sets of quotes corresponded to.

- "Isabelle is 19, describes herself as shy with a small number of friends. She enjoys gaming daily and spends a large portion of her free time playing online games with others. She has made some friends online but regularly leaves games and clans and changes the games she plays."
- "Kate is 53 and plays games in the evening time and weekends online. If people ask what her hobbies are, she describes enjoying cooking, talking to friends on social media and going for walks. Her close friends do not know anything about her gaming hobby."
- "Michelle is 25 and was introduced to gaming by her two brothers at age 4. She enjoyed playing games as a child and teenager with them online, even after they all moved away from each other. She has stopped gaming in the last year."

After this activity, a discussion on the outcomes of the game followed. Because of the toxic environment in gaming, the lack of social support and the impact of negative interactions, female gamers feel stress and anxiety, and feel like they have a new insecurity which they do not need. How do they deal with it? Many female gamers choose not to show they are females, and therefore put internal pressure on themselves, which creates a tense environment for women. This leads them to deny their identity as a female gamer. Women often feel that they need to prove themselves in gaming, as female gamers. What Lavina McLean wanted to emphasise with the three female gamer profiles described above is that none of the three figures have had a choice in shaping their identity. They are female gamers because their gender had a huge impact on their experience.

In general, female gamers are quite accepting of this situation; they take the burden of managing other people's negative behaviours upon themselves, rather than doing something to change this negative environment. But how do we change this negative environment? A first step is by preventing harassment and sexual harassment of women in gaming, but also by adopting a "netiquette", by empowering women and not accepting the current situation as normal. People with a wide audience reach need to roleplay appropriate game playing.

DD2: Sexual violence against men and boys

Session leader: Nick Dunne, Psychosexual Therapist, Brook

Nick Dunne introduced Brook – a UK charity giving sexual health and relationship advice to young people under the age of 25. Brook also has free and confidential clinics, provides online information, carries out relationship and sex education in schools across the UK and in Europe, and trains professionals in these issues.

Nick Dunne began the session by making a group agreement: "respect each other", "listen to each other as well as each other's opinions", "avoid jargon", "ensure confidentiality", "ask questions when needed", and "participate as fully as you are able to". The learning outcomes of the session were to understand forms of child sexual abuse/exploitation (CSA/E) and how these apply to BYM (boys and young men); to take a closer look at online sexual violence and explore the vulnerabilities of boys and young men in relation to CSA/E; to understand the impact of gender in the grooming process and identify the barriers to disclose; and to gain knowledge to safeguard BYM in participants' own environments.

The World Health Organisation (WHO) defines sexual health as *"a state of complete physical, mental and social wellbeing, and not merely the absence of disease or infirmity"*. Sexual health requires a positive and respectful approach to sexuality and sexual relationships, as well as the possibility of having pleasurable, safe sexual experiences, free of coercion, discrimination and violence.

Nick Dunne initiative an activity in which participants had to split into groups, with each group receiving three different scenarios. The groups had to respond to the question: "How

at risk do you think these young people are based on the information presented?", evaluating the risk on a scale of 1 to 10 (10 being the highest risk).

There were two versions of each scenario. In one version, the protagonist was a male and in another one, the protagonist was female. The groups graded the scenarios in which the girl is the protagonist with a higher risk. Participants also highlighted they had different perceptions in their groups depending on their country of origin.

The examples shown were real-life cases. For example, Freddy, aged 17, was introduced to heroin by a girl he was often seen with. However, the police saw him as the negative influence. When making judgements on risk we need to carefully consider our response to ensure we are complying with the Equality Act 2010. Nick Dunne insisted on the fact that we need to respond equally and not respond to boys less than to girls. He mentioned the example of a case he worked on – a babysitter who pleaded guilty of sexual activity with the child she was baby-sitting (aged 11) and of online grooming. She received a six-month suspended sentence, two-year supervision order and sex offender registration for seven years. Would a man have got the same sentence?

Sexual abuse is any sexual activity with a child. One thing to be aware of is that many children and young people who are victims of sexual abuse do not recognise themselves as such. A child may not understand what is happening and may not even understand that it is wrong. Sexual abuse may involve non-contact activities.

According to the Council of Europe, about 1 in 5 children in Europe are victims of some form of sexual violence, and about a third of abused children never tell anyone. A study of young adults (aged 18-27) in ten European countries from 2015 showed that 27.1 per cent of young men and 32.2 per cent of young women have already had to deal with sexual violence prior to reaching the age of consent to sex in their country. In Belgium, the age of consent to sex is 16 years. For Belgium, this was 10.1 per cent of young men and 20.4 per cent of young women. A 2014 study in Flanders with LGBTI people found that 31.7 per cent of transgender people had already been confronted with sexual violence at least once in their lives. In general, this study showed that men who have consensual sex with men are up to six times more likely to experience sexual violence than men who only have heterosexual relationships.

According to a study conducted in the framework of the deShame project, the top five barriers to seeking help for young people are:

- "Too embarrassed" – 52 per cent
- "Worried about what would happen next" – 42 per cent
- "Worried about being targeted by those involved" – 42 per cent
- "Worried that they are to blame" – 39 per cent
- "Would rather sort it out themselves" – 39 per cent

In addition, the top reason for not telling a teacher was that they are "worried that their school would overreact" (50 per cent). The top reason for not telling the police was that they would not "want them to involve their family" (53 per cent). The top reason for not reporting on social media was that they did not think "it would help" (43 per cent). Sexual abuse is not solely perpetrated by adult males. Women can commit acts of sexual abuse, as can other children (peer-on-peer abuse).

There is more risk to LGBTQI people because they are less likely to talk about it; explaining a case of grooming implies explaining that they are gay and often their parents do not know it.

Child sexual exploitation (CSE) is a form of sexual abuse where children are sexually exploited for money, power or status. The exploitative element can be financial gain, discharge of "debt", free tickets/gifts, access to parties, shelter, protection, love, and so on. When it comes to boys and young men being groomed, the groomer may use their gender to their advantage, for example by access in a changing room, or through online gaming. The groomer may use the boys' masculinity and reinforce negative male stereotypes ("be the big man"). The groomer may also use boys' inexperience or confusion regarding sexuality ("prove their sexuality"). Touch can be used in a much more manipulative way with boys. Moreover, sending topless male photos could seem harmless. There are different models of CSE: online; peer on peer; abuse of a position of trust; party model; boyfriend/girlfriend model; gangs/organised network, and trafficking/county lines.

Although technology can be a positive for many children and young people, it can also pose potential real dangers. Technology often plays a key role in the grooming of young people, whether this is via their phones or social media. Below is a mosaic of the various social media apps where cases of grooming have been reported.

Groomers online often target males via interactive gaming, such as Xbox Live, FIFA or World of Warcraft. Online dating apps can facilitate age-inappropriate contact with people seeking sexual interactions. Snapchat can reveal your exact location and allow the user to send images that "disappear". NetAware is a website where you can look for information about the risk of different apps and how they work.

A 2017 Brook online survey showed that significantly more gay young people (9.9 per cent) had met up with an online contact who was not who they said they were, compared to straight young people (4.9 per cent). Nick Dunne therefore also discussed some less-known gay dating apps such as Squirt, Scruff, Wapo, GUY SPY, and Jack'd.

He then moved onto the topics of sextortion and webcam blackmail. Child sex abusers use the internet in many ways, in that regard. It can be to swap child abuse images in chat areas or through instant messenger with other adults or young people. It can also be used to target and build mutual trust with young males. They also form networks with other child abusers to share tips on how to groom more effectively and how to avoid being caught. It can be to swap personal information about children that they have collected. They also participate in online communities such as blogs, forums and chatrooms to groom children (for images and sex). They also target vulnerable single mothers to gain access to their children.

Nick Dunne then presented the Child Exploitation and Online Protection Centre (CEOP) – which operates across the UK to tackle child sex abuse and provide advice for parents, young people and children, and the Internet Watch Foundation (IWF) – which works internationally to make the internet safer by removing images of child sexual abuse. Some of the things children and young people have reported to the CEOP include: "Someone online has asked me to send them nude images", "I shared a nude image with someone online and they are threatening me", "I did something that I was embarrassed about on webcam and someone has turned nasty towards me", "Someone I don't know is asking me to live-stream and do things I don't want to do", "Someone online kept asking me to meet them face to face and I feel pressured by them", "Someone online was talking to me about sex and it made me feel uncomfortable", "Someone online is putting pressure on me to do things I don't want to do", and "Someone I met in an online game keeps trying to talk to me privately".

There are five stages to online grooming: friendship, forming a relationship, risk assessment, exclusivity, and sexual images/meet, which Nick Dunne introduced to the participants using a case example.

Nick Dunne then introduced ThinkUknow (www.thinkuknow.co.uk), an educational initiative from CEOP. Access to the resources is free upon sign up, and the materials can be used with all age ranges of young people

He then moved on to the topic of gender, and especially the related barriers to disclosure. Males do not perceive themselves as being vulnerable or at risk and believe females are more at risk. They believe perpetrators are more interested in females, and they believe they are tough and can look after themselves. There is also the fear of "getting in trouble" if they are also involved in illegal activities. Besides, being the victim of rape and sexual assault is not considered a very masculine thing to admit by some of them.

Which signs should adults look out for to help them to detect child sexual exploitation? Nick Dunne mentioned new expensive items, unexplained money, appearance in "adult clothes", missing school/education, periods of absence, use of alcohol/drugs, anxiety, physical injury and fights, multiple phones or a new phone, excessive time online, reoccurring STI's, repeated pregnancy tests, abortion, requesting lots of condoms, and so on.

When it comes to actually tackling sexual exploitation or abuse, Nick Dunne also suggested a variety of avenues for action:

- Talk about CSE, sexuality and consent early.
- Talk about these issues as a team.
- Teach and model respectful relationships.
- Do not allow sexual name calling/comments.
- Discuss online grooming and issues such as sexting and pornography.
- Be approachable and listen.
- Understand healthy sexual development and distinguish it from harmful behaviour.
- Include and communicate with parents and carers.
- Ensure teaching on relationships and consent is accessible for those with additional needs.
- Raise awareness for males and females about sexual bullying/harassment and how to report.

Nick Dunne presented the #WeSeeYou campaign, aiming to raise awareness about male sexual abuse and assault. It is a campaign aimed at acknowledging male victims/survivors and letting them know that they are not alone. He also introduced the Sexual Behaviours Traffic Light Tool developed by Brook – by identifying sexual behaviours as green, amber or red, professionals across different agencies can work to the same criteria when making decisions and hence protect children and young people with a unified approach.

Nick Dunne advised participants on how to appropriately respond to young people. One should listen and take complaints seriously; record and report; take every opportunity to educate; preserve confidentiality at all costs; and pay attention to incidents online.

He pointed participants to free resources for professionals on ThinkUKnow, as well as to the Brook e-learning platform.

DD3: Online sexual harassment (deShame)

Session leader: Maithreyi Rajeshkumar, Policy and Communications Manager, Childnet

Project deSHAME is a European Commission funded project aiming to tackle peer-based online sexual harassment. It is a collaboration between Childnet, Save the Children (Denmark), Kek Vonal (Hungary) and UCLan (UK). In close consultation with young people, professionals, industry and policymakers, it aims to increase reporting of online sexual harassment among young people, and improve multi-sector cooperation in preventing and responding to this behaviour.

In developing the project, the partners started from focus groups in the UK with young people and based their action on the needs observed. A large-scale research was carried out across the three partner countries with young people, teachers and professionals. The deShame project also consists of an expert and a youth advisory boards to help them in the process.

@redbarnetdk
@kekvonal
@childnet

Maithreyi Rajeshkumar first introduced how online sexual harassment is understood in the context of the project deShame. It is difficult to define and it took the project about a year to find a viable definition. As such, it is "unwanted sexual conduct on any online platform" – Maithreyi Rajeshkumar assured that there are challenges with this definition. Regarding the scope, the project focuses on online sexual harassment that occurs between young people, consisting of images, videos, posts, messages on public and private platforms; overlapping with offline behaviours; and representing a form of gendered sexual violence. It can make a person feel threatened, exploited, coerced, humiliated, upset, sexualised or discriminated against.

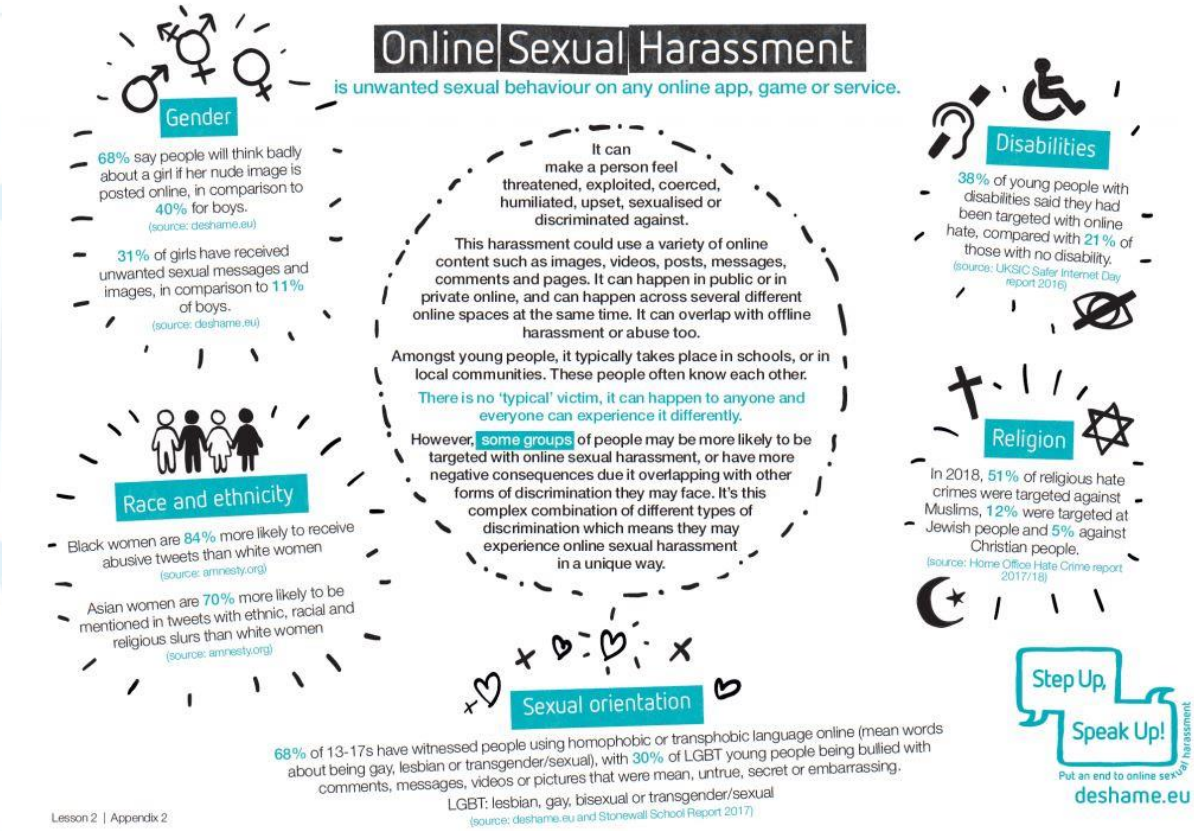
Then, Maithreyi Rajeshkumar organised a group discussion based on the question "What behaviours do we think are happening among young people in regards to online sexual harassment?" The conclusion was that it covers quite a wide range of situations, and this was a clear challenge for the project as well.

Non consensual sharing of intimate images and videos	Exploitation, coercion and threats	Sexualised bullying	Unwanted sexualisation
• Sexual images/videos taken without consent ('upskirting/downblousing/creep shots') • Sexual images/videos taken consensually but shared without consent ('revenge porn') • Non-consensual sexual acts (e.g. rape) recorded digitally (and potentially shared)	• Harassing or pressuring someone online to share sexual images of themselves or engage in sexual behaviour online (or offline) • Using the threat of publishing sexual content (images, videos, rumours) to threaten, coerce or blackmail someone ('sextortion') • Online threats of a sexual nature (e.g. rape threats) • Inciting others online to commit sexual violence • Inciting someone to participate in sexual behaviour and then sharing evidence of it	• Gossip, rumours or lies about sexual behaviour posted online either naming someone directly or indirectly alluding to someone • Offensive or discriminatory sexual language and name-calling online • Impersonating someone and damaging their reputation but sharing sexual content or sexually harassing others • Personal information shared non-consensually online to encourage sexual harassment ('doxing') • Being bullied online because of an actual or perceived gender and/or sexual orientation • Body shaming • 'Outing' someone where the individual's sexuality or gender identity is publicly announced online without their consent	• Sexualised comments (e.g. on photos) • Sexualised viral campaigns that pressurise people to participate • Sending someone sexual content (images, emojis, messages) without them consenting • Unwelcome sexual advances or requests for sexual favours • 'Jokes' of a sexual nature • Rating peers on attractiveness/sexual activity • Altering images of a person to make them sexual

Maithreyi described four categories of online sexual harassment:

- Non-consensual sharing of intimate images and videos, with 51 per cent of young people reporting having seen people sharing (nearly-) nude images of someone they know, and 23 per cent admitting they have seen people secretly taking sexual images of someone and sharing them online.
- Exploitation, coercion and threats, with 10 per cent saying they have been sent sexual threats online, and 7 per cent saying that someone used sexual images of them to threaten or blackmail them.
- Sexualised bullying, with 66 per cent saying they have seen people sharing things about someone else's sexual behaviour, and 80 per cent saying they have seen people using terms like "sket" or "slut" to describe girls online in a mean way.
- Unwanted sexualisation, with 23 per cent saying they have received unwanted sexual images, and 47 per cent saying they have seen someone editing photos of someone to make them sexual.

Who is online sexual harassment happening to? Maithreyi Rajeshkumar said that there are more reported cases about girls, but it also seems that boys report it less. One should not only consider the gender, but other aspects as well (for example, non-binary people). In reality, it can happen to everybody and everyone can also experience it differently. The consequences can also vary quite a lot from case to case. She therefore presented the slide below with five key characteristics which the deShame research project explored.



The key factors of online sexual harassment are developmental, relationship, peer group, and societal. There was a group discussion about the reasons why young people might engage in online sexual harassment. Participants mentioned peer pressure, power and lack of self-esteem, and imbalance of power in general. Maithreyi Rajeshkumar presented the top five perceived motivations why others might engage in online sexual harassment, according to the study: “as a joke” (54 per cent), “to hurt someone” (52 per cent), “to retaliate because someone else started it first” (50 per cent), “to get their own back on an ex” (47 per cent), and “to get respect from friends” (45 per cent).

What stops young people from reporting online sexual harassment? What are the barriers? How do they respond to it? Young people respond to it by “blocking the people involved” (82 per cent), “speaking to friends” (67 per cent), “telling the people involved to stop” (65 per cent), or “speaking to parents or carers” (48 per cent). But there are many barriers to seeking help, with the top five being “too embarrassed” (52 per cent), “worried about what would happen next” (42 per cent), “worried about being targeted by those involved” (42 per cent), “worried that they are to blame” (39 per cent), and “would rather sort it out themselves” (39 per cent).

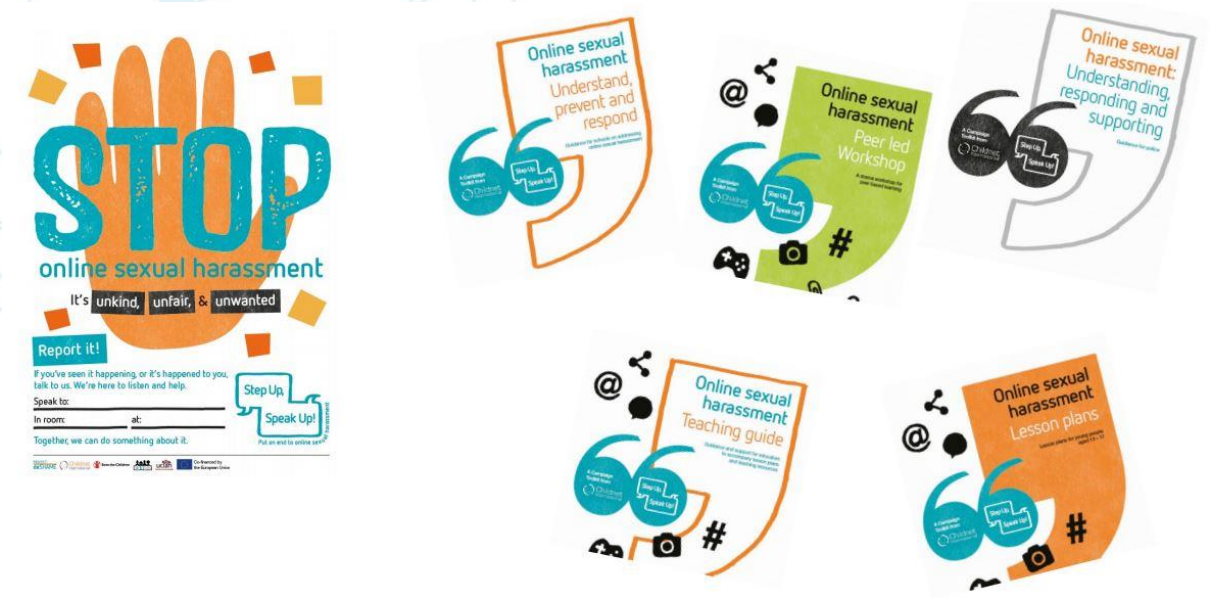
The top five barriers to reporting to teachers are “worried school would overreact” (50 per cent), “worried it would make it worse” (43 per cent), “would not know which teacher to

speak to" (32 per cent), "don't think I would be taken seriously" (23 per cent), and "teachers are too busy to speak to" (20 per cent).

The top five barriers to reporting to the police are "I wouldn't want them to involve my family" (53 per cent), "I wouldn't want to get into trouble" (46 per cent), "I would think it wasn't serious enough" (39 per cent), "I think it would be too difficult" (37 per cent), and "I wouldn't know how to" (36 per cent).

And finally, the top five barriers to reporting to social media are "I don't think it would help" (43 per cent), "I don't think they would do anything" (40 per cent), "I would be worried that the people involved will get notified" (33 per cent), "it's too much effort" (18 per cent), and "I don't know how to" (18 per cent).

Victim blaming also appeared to be very strong among young people in the study. 55 per cent of respondents said they felt that if someone's nude or nearly nude image is shared online, they are partly to blame. 68 per cent said that they felt girls are judged more harshly for sexual rumours about them than boys.



Maithreyi Rajeshkumar then introduced the Step Up, Speak Up! Campaign Toolkit. It is easy to use, practical, inclusive, and based on real-life situations. She then carried out a demonstration of a lesson plan, distributing different scenarios across the room, and showing participants a chart with a continuum between "Fun and flirting" to "Banter and harassment". There were discussions on each scenario, trying to position each of them on the continuum.

Maithreyi Rajeshkumar then shared the lessons learnt throughout the project:

- Ensuring young people are consulted every step of the way.
- Interactive and practical format of resources.

- Increase understanding of how and where to report.
- National variations reflect differences in education systems, different levels of prior attention to issue.
- Importance of safe space for discussing complexities of issue (such as gender dynamics, victim blame, consent).
- Long-term and whole-school approach needed.

When it comes to the next steps, the project partners are now exploring the prevalence of online sexual harassment happening among children aged 9-12, engaging parents and carers more, and developing a toolkit for EU member states.

DD4: Online hate (SELMA)

Session leaders:

- Ken Corish, Online Safety Director, South West Grid for Learning (SWGfL)
- Stefanie Fächner, Media Education Consultant, German Awareness Centre
- Niels-Christian Bilenberg, Helpline Coordinator, Cyberhus

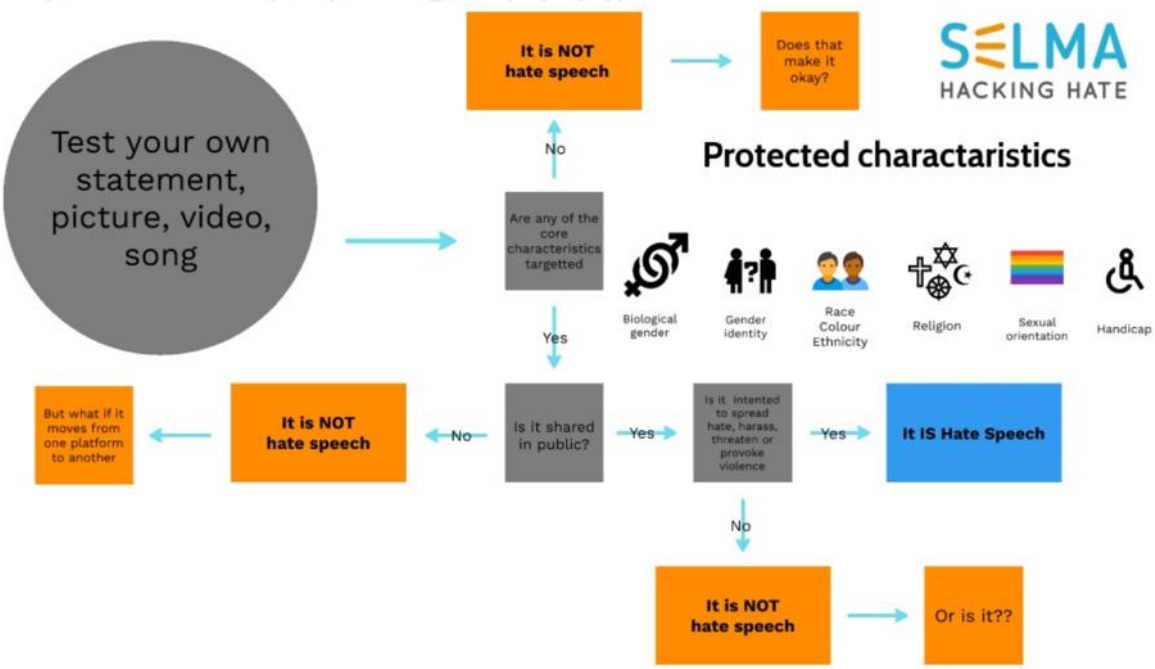
In this session, Ken Corish, Stefanie Fächner and Niels-Christian Bilenberg shared information about the SELMA project and its pedagogy. Online hate speech is a difficult issue to discuss with young people; it is complicated to understand and to distinguish from other forms of harmful content.

Ken Corish opened the session by presenting SELMA, which, according to him, is not just another resource, because of its highly active and customisable components. The SELMA project has a Social and Emotional Learning (SEL) background, which is part of the SELMA acronym (Social and Emotional Learning for Mutual Awareness). The motto of SELMA is "Hacking hate". The hacking flow, according to Ken Corish, is to identify, acknowledge, explore, understand, create, apply, disrupt and change – SELMA aims to teach this to young people as they need strategies to stand up to hate speech.

Niels-Christian Bilenberg gave participants a definition of what online hate speech consists of. Online hate speech is defined as *"any kind of statement expressed and spread by an individual or group of people through any form of digital communication targeting an individual or group of people based on a core characteristic of them with the intention to spread hate, harass, threaten and provoke direct or indirect violence"* – in short, *"any online content targeting someone's core characteristics with the purpose of spreading hate, threatening or provoking violence against them"*. These core characteristics depend on a

person's biological gender, gender identity, race, colour, ethnicity, religion, sexual orientation, or disability.

Niels-Christian Bilenberg then highlighted how the sheer amount of content uploaded to social media platforms every day makes it simply impossible to imagine all of it being checked by moderators. Indeed, every day, 95 million Instagram posts, 350 million Facebook comments, 500 million tweets, 3.5 billion snaps, 60 billion WhatsApp/Messenger messages, and 600,000 hours of YouTube videos are uploaded. Therefore, Niels-Christian Bilenberg introduced the SELMA algorithm for checking hate speech, as shown below.



Following this presentation, participants were divided into groups, with each group becoming an algorithm to try to determine whether a specific piece of content is hate speech or not. This activity saw lively group discussions around seven images of online communication for groups to decide whether something is hate speech. There were disagreement within and between groups regarding what a protected characteristic should be and what qualifies as intent to incite hate. Ken Corish and Niels-Christian Bilenberg underlined how difficult it is to give an answer to certain questions and that it is not necessarily about being wrong or right, but about discussion.

They then went on to explain the importance of hacking/disrupting hate. Ken Corish gave important points of intervention, like identifying the context, what medium to use to defuse the hate, and so on. A short exercise followed, with Ken Corish advising participants to tackle online hate speech using https://pablo.buffer.com.

Ken Corish then summarised the session by emphasising the collaborative aspect of hacking, giving the example of Greta Thunberg and the Parkland shootings. He also repeated the importance of SEL in this project and invited people to explore www.hackinghate.eu.

DD5: Using AI as a solution

Session leaders:

- Julie Dawson, Director of Regulatory & Policy, Yoti
- Milan Zubicek, Government Affairs and Public Policy Manager, Google

Hans Martens from European Schoolnet chaired this session, setting the context by stating that, nowadays, it would be difficult to organise an edition of the Safer Internet Forum without a session on artificial intelligence (AI). AI is everywhere right now; we hear about the opportunities and solutions for cyber challenges provided by AI approaches but, at the same time, there are concerns about having AI embedded in the systems and platforms we use. Inclusive design approaches, safety by design, privacy by design, and attention to accessibility issues are all important in delivering better and safer online experiences for children and young people (and indeed all users), and should therefore be a priority in AI-based approaches. Hans commented, however, that this session would have a specific focus on using AI as a solution to some of the challenges encountered online.

Julie Dawson, Director of Regulatory & Policy at Yoti, kicked off the session by giving an overview of the Yoti solution and some of its current applications. As a global identity platform, Yoti provides services in more than 175 countries accepting 1,000s of government identity documents as proof of identity; as a result, 1,000s of businesses now accept Yoti as part of a trusted network. The premise to the service is that once a user creates their Yoti identity, it can be used multiple times in multiple settings and applications. The users' details are encrypted into unreadable data that can only be unlocked by Yoti; nobody else can access or decipher it, not even Yoti staff. Images are instantly deleted after the age estimation takes place. The anonymised face and year of birth data then helps to build the

neural network to further improve the accuracy of the technology; however, all subjects have the option to opt out from this usage.

Yoti started out as a free-to-download consumer app, but has now developed into a B2B application also. As such, there are now two main approaches to employing the technology:

> ***Yoti app and trusted network***
> Provides identity verification, age verification, biometric e-signatures, biometric authentication, and access control. The processing takes place within Yoti's private, secure identity platform. A user can create their own trusted identity once and use it many times.
>
> ***"Powered by Yoti" technology***
> In this application of the technology, service providers can embed Yoti into their existing web or mobile services. Services provided include document scanning, facial recognition, liveness detection, age estimation and voice recognition.

Ultimately, Yoti wants to be the identity verification provider of choice but still maintains a human element alongside the tech environment. Yoti are mindful, however, that there is no silver bullet to identity verification; in brief, whatever is being done now is still not good enough. For this reason, they seek to act differently in this space; to both scrutinise and invite scrutiny.

Yoti has an internal ethics and trust committee who oversee the development and implementation of the company's ethical approaches and provides a "guardian" responsibility, acting as extra eyes and ears internally to raise any issues. The group has very clear principles which they adhere to, namely:

- Always act in the interests of the user.
- Encourage personal data ownership.
- Enable privacy and anonymity.
- Keep sensitive data secure.
- Keep the community safe.
- Be transparent and accountable.
- Make Yoti available to anyone.

Julie Dawson then went on to provide an overview of some of the Yoti solutions, include age scan which has many applications such as social media, online dating, retail and e-commerce, gambling, gaming and e-sports. In doing so , Yoti is a signatory of the "Safe Face Pledge", which aims to:

- Show value for human life, dignity, and rights.
- Address harmful bias.
- Facilitate transparency.
- Embed commitments into business practices.

The algorithms behind the technology are constantly being monitored for accuracy by age, gender and skin tone, and accuracy is continually improving. A Yoti age scan white paper is available for those who want to know more.

Yoti is being used in some specific environments to protect children and young people. To give an example, a key challenge for Yubo (a live streaming app for teenagers with over 20 million users globally, which aims to help users make new friends) was to make sure only users from the right age group can chat together: 13-17 years and 18+ have separate communities on the app, and under 13s aren't allowed to use it. Enforcing these age groupings is a critical priority for Yubo. This is why Yubo joined forces with Yoti.

As part of its safety measures, Yubo uses Yoti's age estimation and verification solutions to detect risky accounts and create a safer and more-trusted environment. The result has been that over 50 million users have been age scanned, and thousands of accounts have been suspended. Equally, hundreds of Yubo users voluntarily verify their identity everyday using the Yoti tools. The typical process is as follows:

1. Yubo uses Yoti Age Scan to analyse users' profile pictures and flags suspicious profiles to its moderation team.
2. Yubo's moderation team reviews flagged accounts and can decide to suspend them. Suspended accounts are required to verify their identity via Yoti in order to continue using Yubo.
3. Every Yubo user has the option to verify their picture and date of birth via Yoti. Verified users are rewarded with a yellow "verified" tick on their profile.

Other applications are being developed, such as age gating content at 15 and 18, examining unintended consequences of verified profiles, and looking at the age of victims and perpetrators in child sexual abuse cases.

In conclusion, Julie Dawson identified some key challenges in this space going forward:

- The language around the practices of facial detection/recognition/matching etc., and public awareness of that is important to help build trust – common language is important: one to one, one to many, surveillance, etc. FPF – the Future of Privacy Forum – is conducting some research in this space.
- Building consented data sets (using data from over 13s only).
- Consideration of what different skill sets are needed, and establishment of oversight organisations (ethics committees, researchers, consumer rights, human rights, online harms, and so on).
- Consideration of where AI applications could it be useful going forward.
- Examination of different approaches that border AI approaches.

Next up was Milan Zubicek, Government Affairs and Public Policy Manager at Google. Milan Zubicek commenced by stating that Google has a strong experience with using AI and

machine learning – search tools can boost the performance and functionality of Google's products and services. They are also learning what the challenges and issues are linked to this space, and how Google can tackle these. As such, Google has established some AI principles which guides its ethical development of AI solutions. These include:

- AI should be socially beneficial.
- AI should not contain bias.
- Safety and privacy should be integrated by design.
- There must be accountability in all AI uses.
- All AI applications should seek to deliver scientific excellence.

Google's AI solutions are only available for uses that accord to the above principles. Conversely, Google's solutions should not be used for:

- Anything dangerous.
- Mass surveillance.
- Anything which is in contravention of national laws.

All of these principles are tested over time, and Google works with various sectors to conduct ongoing research and development. Equally, Google has developed various tools to test the new developments. One such example is the Google "What-If Tool"; a tool to test what the result of machine learning might be if the input data is different.

Google try to be transparent across all areas of this work, sharing principles, research data, data sets and tools with the wider community, and making APIs (application programming interfaces - a set of functions and procedures allowing the creation of applications that access the features or data of an operating system, application, or other service), such as those for translation and image analysis. This mean that others can utilise and benefit from the advances which Google has made.

Milan Zubicek then provided a few case study examples. Every minute, 500 hours of video content are being uploaded to YouTube. In this case, the scale presents the challenge; content cannot be moderated by human moderators alone, and machines are needed to detect and flag problematic content. Removal still requires human intervention – there is not yet the nuance in machine learning to determine, for example, political speech versus hate speech. When human moderators respond to flags, that data is fed back into the system to further improve the machine learning.

Another use of machine learning is to tackle hate speech in the comment sections of publisher websites, such as the New York Times. Machine learning can measure the level of toxicity of comments; publishers can then make a choice of how much toxicity they allow through to their public platforms, and prevent the most harmful comments from being published. The tools can also provide direct feedback, telling the user that their comments will not be published in their current form, and giving them the option to rephrase.

The floor was then opened to questions. One participant commented that, under new legislation, there will be more responsibility for platforms such as YouTube to show age levels for sensitivity in content. What are Google doing in this respect? Milan Zubicek responded that Google's policy teams are working with local experts, NGOs, policy makers and similar on local implementation in all Member States.

Another participant asked how age verification is being used to make sure platform users are the appropriate age. Milan Zubicek responded that Google provide tools to users (controls), and try to educate parents. Google Familylink, for example, gives control to parents on how their children can spend time on YouTube. Google are also developing specific tools/platforms of relevance for younger users (such as YouTube Kids). They are also exploring providing more relevant content for different age groupings of young people.

When asked how machine learning can limit the biases that are very close to human nature, Milan Zubicek gave an example of Google image where a search on "famous scientists" would typically present images of middle-aged white males, with grey hair. Although the images presented are factually correct, this is possibly strengthening the bias prevalent in human nature. He then gave another example of coffee mugs – the direction in which the handle is facing in images, for example, can reinforce the bias that most people are right handed. The algorithms can obviously be tweaked, but what is the right ratio? These sort of issues can't be solved by Google alone.

On a question regarding transparency, Julie Dawson commented that companies need to say how good or how bad things are. When Yoti first published their white paper back in January 2019, they were flooded with comments along the lines of "the results aren't especially good, but at least you're putting it out there". A key challenge in terms of external benchmarking is that there are no comparable benchmarking organisations in Europe. Julie Dawson went on to comment that, in some respects, Yoti benefits from being a smaller company that has started from the ground up – for example, this has allowed it to set up an ethics committee "with teeth". Some things are easier in a small company; but many of the larger organisations have been very helpful, while also bringing invaluable scrutiny to the work which they are doing. Milan Zubicek concluded by echoing Julie Dawson's comments. Understanding the concerns, debunking misunderstandings, transparency, explainability, and so on is key. Google are working to develop as a company, but in collaboration with wider industry also. Google seeks to set high standards for others to follow, but equally they work with – and learn from – smaller companies in this space.

DD6: INHOPE@20: The impact of a global network in combatting online child sexual abuse material

Session leaders:

- Denton Howard, Executive Director, INHOPE
- Fred Langford, President, INHOPE

Keynote speaker: June Lowery, Head of Unit, Accessibility, Multilingualism and Safer Internet, DG CONNECT, European Commission

Chair:

- John Carr, Senior Technical Adviser, ECPAT International, Thailand

Panellists:

- Jean-Christophe le Toquin, President, Point de Contact, France
- Barbara Schlossbauer, Hotline Manager, Stopline, Austria
- Michael Busch, Senior Policy Officer, Unit G3, DG CONNECT, European Commission
- Antonio Labrador Jimenez, Team Leader, Fight Against Child Sexual Abuse, Unit D4 Cybercrime, DG HOME, European Commission
- Jean-Charles Schweitzer, Criminal Intelligence Officer, Europol

INHOPE and its extensive network of member hotlines work to eliminate online child sexual abuse material (CSAM). It is critical to the work of the hotlines that members of the public who stumble upon illegal content report it and not ignore it. The consequence of not reporting illegal content are numerous and impact victims: CSAM remains on the internet and is not taken down. This means that every time that this material is viewed by anyone anywhere in the world, the victim depicted is re-victimised. Indeed survivors of recorded child sexual abuse say that knowing it is online for anyone to see continues to impact their lives for many years after the abuse has stopped. The significance of reporting illegal content is vital in helping survivors of child sexual abuse reducing the repeated trauma they could suffer, as well as keeping the internet safe for all legitimate users. INHOPE marked 20 years as the leading global organisation that fights child sexual abuse material (CSAM) this year with a special deep dive session, INHOPE@20, at the Safer Internet Forum.

INHOPE@20 was an opportunity for current member hotlines, founding member hotline colleagues, policy makers, law enforcement and child safety advocates to come together to talk about where we have come from, where we are today and where the network is going. With 45 member hotlines in 40 countries working together to eliminate online CSAM, victims know that there are people and organisations fighting for them to no longer live in fear of images of their abuse being found and viewed.

INHOPE rebranded

INHOPE@20 provided an opportunity for INHOPE to share its rebranded website and communications, which represent the INHOPE network of hotlines standing for one vision and being stronger together.

DG CONNECT keynote speech

June Lowery, Head of Unit Accessibility, Multilingualism and Safer Internet at DG CONNECT, gave the keynote speech, highlighting the following:

- 800 million children use social media and are the fastest growing demographic. By 2022 there will be another 1.2 billion new social media users.
- NCMEC (National Center for Missing and Exploited Children) received 18 million reports last year and 800,000 of these reports concerned materials hosted in the EU, so there is still a lot of work to do.
- There still isn't a common definition in European law of what child sexual abuse material is, which makes the jobs of analysts and law enforcement much harder.
- End-to-end encryption is proving a huge challenge as it helps offenders hide their identity and location.
- Artificial intelligence has the potential to help us better combat CSAM significantly by lessening the burdens on analysts and law enforcement.
- There is increased political attention to the issue of CSAM at EU level as evidenced by the reaffirming of EU and Member States' commitment to fighting sexual abuse of children with a three-pronged approach, being legislation, cooperation and funding. Find out more information on this commitment.

Panel 1 – INHOPE yesterday, today and tomorrow: How did we get here? A contribution from our founding and long-standing members

John Carr (Senior Technical Adviser, ECPAT International, Thailand) was the discussion chair, with panellists Jean-Christophe le Toquin (President, Point de Contact, France), Barbara

Schlossbauer (Hotline Manager, Stopline, Austria) and Fred Langford (Deputy CEO, Internet Watch Foundation, UK and President, INHOPE).

John Carr opened this panel by discussing recent New York Times articles highlighting the lack of action from technology companies in fighting CSAM online. The panellists then shared their thoughts, with the discussion highlighting the following points:

- Technology can and should play a huge role in the fight against CSAM in the future, notwithstanding that we will always need humans to do part of the work, including the work of the hotline analysts.
- Companies should consider scanning on upload and take on that responsibility.
- The New Digital Services Act will see a revision of the e-commerce community divisions and seek ways to take all legal and proportionate steps to mitigate risk concerning CSAM on IT systems.
- European Internet Services Providers (ISPs) have no real reason to act (meaning that now is the time for regulation), while the US tech giants are doing more than Europe and the rest of the world today.
- There is a need for common legislation across Europe (at least).
- All citizens in all countries should have a place where they can report illegal material found online, either to a hotline or, in countries where hosting is minimal, possibly simply through a reporting mechanism that requires minimal resources such as an online reporting portal.
- The content analysts are INHOPE's heroes, but their work is not recognised or respected as much as it should be.
- In a post-encryption age, new technology and techniques must be sought. Indeed, as companies employ strong encryption in environments which are used to store, post or otherwise exchange messages and files, they are making CSAM invisible (by making it undetectable).
- INHOPE was needed 20 years ago at the dawn of the internet, and while it has come a long way and has been the glue that has held the network together as the leading global authority tackling CSAM, the work is in many ways just beginning.

Panel 2 – What the INHOPE network of hotlines has achieved and why we support them: A contribution from some of our stakeholders
The panel chair was Fred Langford (President, INHOPE) and the panellists were Michael Busch (European Commission, DG CONNECT, Unit G3, Senior Policy Officer), Antonio Labrador Jimenez (European Commission, DG Home, Unit D4 Cybercrime, Team Leader, Fight Against Child Sexual Abuse) and Jean-Charles Schweitzer (Criminal Intelligence Officer, Europol).

Michael Busch reflected on INHOPE@20 and highlighted that the first decade was a time when the foundation of the network was being built. The second decade looked to, firstly establish an unprecedented and unique cooperation and trust between INHOPE members, civil society, and police, and secondly the concretisation of the INHOPE network to cover all of the member states. The European Commission is proud to have funded the fight against CSAM through funding INHOPE's work today, and from the very beginning.

Jean-Charles Schweitzer talked about the relationship between INHOPE and Europol, discussing how the two organisations work together on capacity building, training, awareness, exchange of expertise and knowledge. This collaboration aims to further and always advance the fight against CSAM through better detection and investigation. Jean-Charles Schweitzer also talked about how INHOPE can improve its systems to help provide the police with actionable intelligence.

Antonio Labrador Jimenez, Team Leader Fight Against Child Sexual Abuse in Unit D4 Cybercrime at DG HOME, talked about the key role of hotlines in the Directive on combating sexual abuse of children, and how it has changed the European landscape. An example was given that, the day prior to this meeting, President Emmanuel Macron had given a speech about measures to be taken in France concerning online child protection. This is a direct

result of the EC's work and the infringement procedures the Directive sets out. In terms of impact, Antonio also touched upon the other ways in which the EU helps its 500 million citizens, who benefit from decisions made and implemented as Directives, driving forward democratic resolutions made and negotiated by elected officials. Indeed, there will also need to be a review of the e-Commerce Directive under the new European Commission, which took office on Sunday, 1 December 2019.

Young people using social media to bring about change

Speakers:

- Emma Holten, Human rights activist
- Gina Martin, Author and activist
- Sara Sjölander, Girl Child Platform

Chair: Lili Leißer, Austrian Safer Internet Centre and BIK Youth Ambassador

Karl Hopwood welcomed the speakers the chair to the final plenary session of the day. Lili Leißer, Youth Coordinator at the Austrian Safer Internet Centre and BIK Youth Ambassador, chaired the session, introduced all three speakers, who then took to the stage to share their stories.

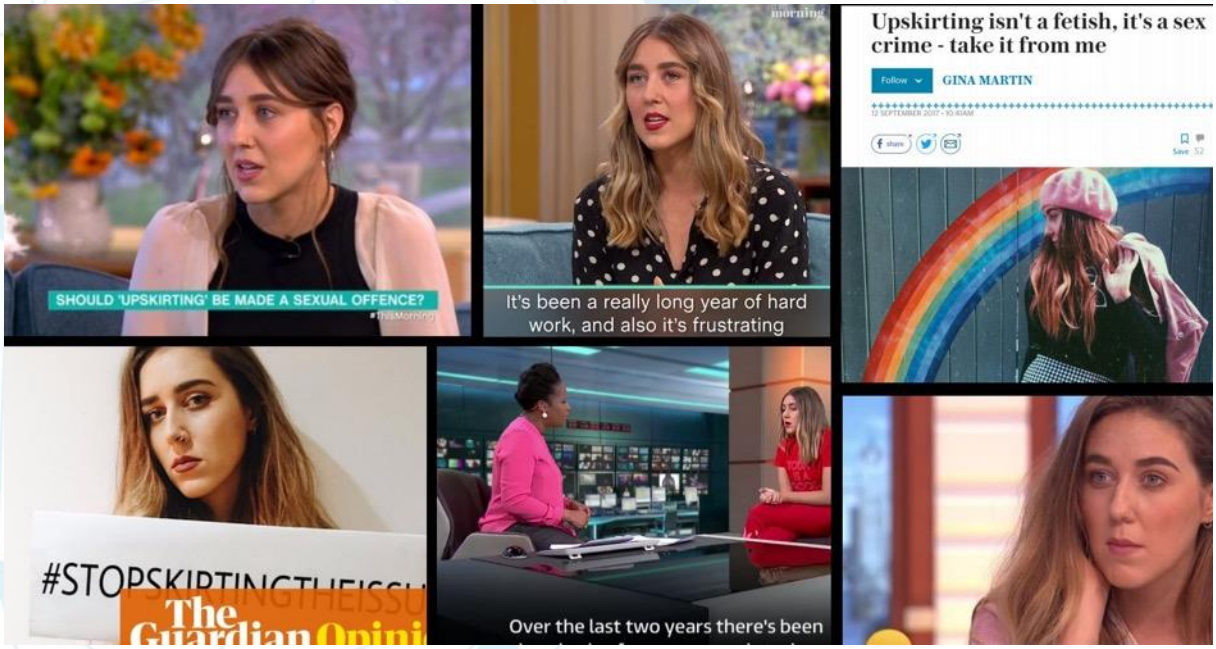
Emma Holten is a human rights activist whose personal data – including phone number and pictures – were stolen and posted with an inducement of violence towards her. She then started speaking out and experienced victim blaming.

She reflected on the fact that online harassment is often framed as a reaction to something someone else has done, but we need to look at it as an action. Victim blaming happens because people seem to frame people as “normal” or as “exceptional”, and the latter are isolated from a structure of justice. A person writing sexist comments under videos is not a reaction to the video, but an action based upon that person’s sexism. That person was a problem for society long before they are committing an act in itself. Sexism is not a mistake; it serves a purpose, it is meant to silence women online. We need an analysis of power structures in society.

Online violence is not an individual act in a vacuum, it is part of a societal structure, it is about exclusion. Many marginalised groups seem to have accepted that they need to do the emotional labour of being able to go about their day – but this should not be considered normal. A member of the audience echoed this remark by saying that society at large needs to tackle this more, especially because some public figures legitimise it. We need to understand which purpose it serves – mobilising specific sentiment among the public, leading attention away from other issues. We should not focus so much on whether someone is a racist or misogynist, but on the analysis of what their actions are doing and the intention for their public performance of sexist or racist comments.

Gina Martin, author and activist is known for her online campaign against upskirting, the outcome of which was to make this practice illegal in the UK. She was attending a festival with her sister in July 2017, when a man took a picture up her skirt. Upon contacting the police, she was told that "nothing could be done". She then found out that upskirting was not illegal in the UK, although it had been in Scotland for a decade. Since there was no legal way to tackle the issue in the UK, Gina Martin started a social media campaign.

With her social media reach and a petition, she went to television stations and other media. While this was frustrating at times, it placed the problem of upskirting in the spotlight, with many people coming forward to admit that it had happened to them too – including children. The story gathered pace and gained a lot of media echo.



Gina Martin then briefly explained how she went about making upskirting illegal. She built allegiances inside the UK Parliament to build support, then went to legal authorities up and down the UK to raise awareness, before finally bringing the bill to Parliament.

She insisted on the fact that social media does have different sides. For her, changing the law was possible thanks to social media. However, there was no protection against online harassment on the social media platforms, and she was targeted by many attacks. She then shared a few tips on how to get started with using social media for activism, suggesting to:

- Make your cause super clear to understand.
- Connect with related communities.
- Build an army across platforms and groups.
- Support your online work with offline efforts.
- Be an active online bystander.
- Be human not a faceless entity.

A member of the audience asked Gina Martin who or what helped her keep going when things became difficult. She replied that she kept going because she was convinced of the relevance of the cause, thanks to the support she was getting on social media and thanks to her friends and family. Another participant asked whether the law had an impact since it came into effect in April 2019. Gina Martin replied that reporting of upskirting has increased significantly in the UK, and there have been five prosecuted cases since it became law.

Finally, Sara Sjölander, Project Manager of the Girl Child Platform, a network of girls rights organisations, took to the stage. She previously coordinated and developed the digital platform Näthatshjälpen (the Cyber Hate Assistant) for the Swedish equality foundation Make Equal.

She began by sharing how cyber hate is defined in the framework of these projects, which she defined as an umbrella concept. She also wanted to address individual experiences with online hate, not just considering the legal aspect, because some things are illegal, but some are legal yet still hurtful and with negative consequences for the victim. We all play a part in creating our online culture – as such, the focus solely on young people is too narrow; it is important to also educate adults, as she claimed most people crossing boundaries online are in their fifties or sixties. For NGOs, there are external threats but also internal vulnerabilities.

She adopts an intersectional approach, defining intersectionality as *"a lens through which you can see where power comes and collides, where it interlocks and intersects"*. It is important because it is both an analysis and a tool.

Sara Sjölander then described the Cyber Hate Assistant, which provides guides, tips, facts, tools, information on where to get further assistance, and a form to report to the police. She especially highlighted the Code of Conduct to refer to in cases of cyber hate; a guide on gathering digital evidence of cyber hate, a guide on developing a plan for distribution of responsibility in situations of cyber hate, and some facts about sexual harassment and sexual abuse.

A member of the audience asked Sara Sjölander how her organisation reaches parents and adults. She replied that it is problematic that funding organisations do not see this as an intergenerational issue. Some initiatives might target the elderly, but the cohorts in between are often left out.

Lili thanked the panellists and closed the session.

Close of Safer Internet Forum 2019

Claire Bury, Deputy Director General of DG CONNECT gave the closing address, thanking all people who spoke up during the SIF, for their openness and the general organisation. She underlined the importance of young people actively getting involved in decision-making fora and processes. She also emphasised the potential – but also the responsibility – of social media platforms to effect positive change, both online and offline. She also stressed the importance of educating parents.

Claire Bury thanked and congratulated the INHOPE network, and encouraged participants to be active on Safer Internet Day (SID), taking place on Tuesday, 11 February 2020. On SID 2020, the EC will focus on involving young people in an initiative to help simplify the terms and conditions of online platforms. She also stated that the new Commissioner, taking up post the week after SIF, will have specific responsibilities regarding children's rights, including digital rights.

Finally, Claire Bury thanked European Schoolnet and her colleagues from the European Commission.

Annex 1: BIK Youth Panel 2019

26 youth panellists from 20 countries (Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Latvia, Lithuania, Luxembourg, Norway, Portugal, Spain, and the UK) came together in Brussels, Belgium to attend the Safer Internet Forum (SIF) 2019 and the preceding BIK Youth Panel on 20 and 21 November 2019.

Throughout the months of October and November 2019, the youth panellists gathered in six online meetings as part of the BIK Youth Programme, in order to discuss and set out their ideas about shaping their plenary session during SIF. During this period, they launched an Instagram campaign (BIK.YouthforYouth) and planned the structure of their session, which comprised a sketch followed by table discussions and campaign presentations.

On Wednesday, 20 November 2019, under the supervision of privacy expert Chris Pinchen, Austrian Safer Internet Centre representative Barbara Buchegger and members of the BIK Youth Coordination Team, youth panellists started working on a detailed plan of their session. They started off with energiser activities and then moved on to a problem-solving activity in which they took the roles of helpline representatives and callers to simulate typical helpline calls. Following this activity, they summarised the cases and discussed possible solutions to issues pertaining to online violence.

In the remainder of the morning session, the young people moved on to the discussions on the survey which they had prepared and conducted in parallel with their preparatory online meetings. They talked about how they would evaluate the results of their survey and in what fashion they would present the findings during their session during SIF. An initial idea in this regard was to pick a few striking responses to present in the plenary session.

The youth panellists started sharing various ideas on the dramatic entrance and sketch that would open their SIF session. At this stage, they also started thinking about the general structure of the session, with discussion covering the following ideas:

- A dramatic entrance with insults/rude comments commonly seen online shouted and displayed on boards.
- A sketch of a helpline call where, following an initial call from a victim of bullying, the "bully" calls back for support years later.
- Consideration of how the findings of the survey could be presented in the sketch.
- Consideration of how the Instagram campaign should be presented at the end of the session.

At the end of the morning session, the group also discussed the roles they would take such as creating the sketch, acting in the sketch, facilitating the session, tweeting about the event, content-creation for table discussions, and presenting the Instagram account, among others.

The afternoon session started with Barbara Buchegger providing the panellists with an overview of the timing of their youth-led session at SIF. Following the discussions on how the SIF session would unfold and how each planned activity would fit in, the group started to

determine the topics for table discussions. During the brainstorming, the group came up with a list of possible topics, some of which included:

- Self-harm on social media and online challenges.
- Hate speech and fake social media accounts created for offensive comments online.
- Sexualisation of women in video games.
- Doxxing and identity theft.
- How people start bullying.
- Cyberbullying – How far can it go?

In the final stages of the preparations, panellists broke into smaller groups to rehearse their acts, and prepare their presentations and the posters to be used during the SIF session.

Throughout the following day, youth panellists participated actively in various sessions at SIF where they also led their plenary session. There was great interest in the youth-led "flip the consultation" session from participants of the Forum, and the congratulations and praise received afterwards reflected the success of the session.

For more information on the BIK Youth Panel and for an overview of the BIK Youth Ambassadors, please visit the Better Internet for Kids (BIK) Youth portal.