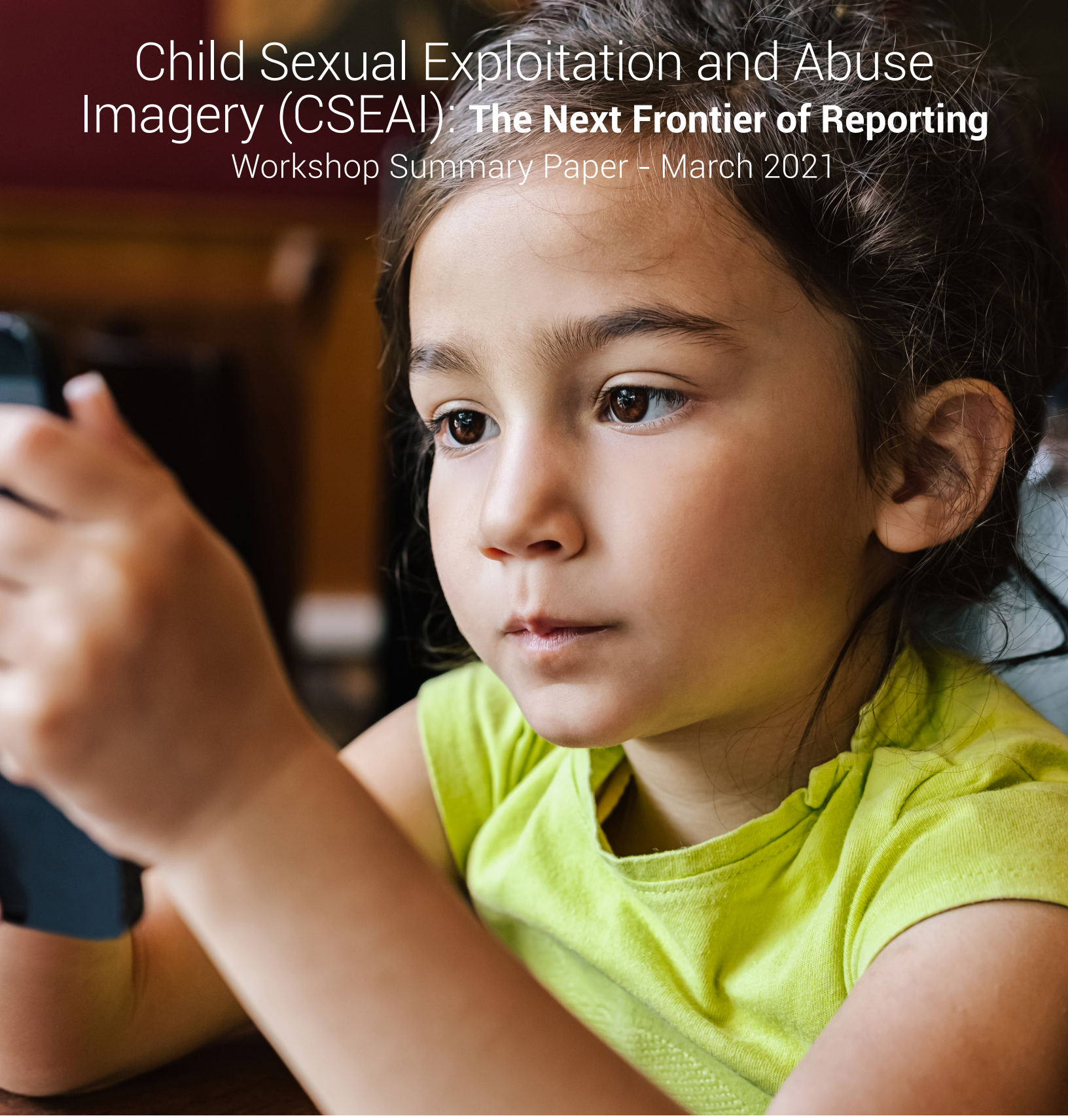
Child Sexual Exploitation and Abuse Imagery (CSEAI): **The Next Frontier of Reporting**

Workshop Summary Paper - March 2021



TECH COALITION

Introduction:

On 24 and 25 March 2021, the **Tech Coalition** hosted a two-day event to bring together over 100 policymakers, civil society, law enforcement and companies from 23 different countries to explore the next frontier of reporting Child Sexual Exploitation and Abuse Imagery (CSEAI) to help increase our understanding of current reporting structures and jointly explore potential paths for improvement. This is the first of a series of events convened by the **Tech Coalition** to facilitate multistakeholder dialogues for the purpose of increasing our collaboration on protecting children from online sexual abuse and exploitation.

Child sexual abuse is a horrific crime, and governments around the world are working hard to ensure that there is a clear and systematic response to tackle and prevent these crimes. As images of this abuse are increasingly finding their way online, it is critical that there is an effective mechanism to report and investigate CSEAI so that the abuse can be stopped. Currently, several governments are considering measures to help address these crimes, including potential new reporting obligations on service providers. There are foundational issues of national sovereignty at stake with each government seeking to fulfill its fundamental obligation to protect the children within its borders. At the same time, in an increasingly digitally connected world where images and crime instantly cross borders at the click of a button, multiple independent reporting regimes increase the risk of a fractured and inconsistent response that ultimately may hinder our collective efforts to keep children safe.

Discussions across the two days showed that there is a robust reporting ecosystem that exists globally, and there are parts of this ecosystem that can be built upon and improved in order to deliver on our mission of preventing and eradicating online child sexual exploitation and abuse. The global nature of the crime requires a global and coordinated solution.

The event had two parts, an open-to-public webinar and a targeted workshop discussion. Below we summarise the key themes of both.

Summary of Workshop Presentations:

The workshop offered an opportunity to gain a better understanding of how the current system operates from the perspective of policy makers, the hotlines working to fight CSEAI online, law enforcement and industry.

European Commission perspective - strategy for a new EU reporting centre.
We started the workshop hearing from the European Commission about their strategy to more effectively coordinate the fight against child sexual abuse and exploitation and

proposals for a European centre to support this mission. Cathrin Bauer-Bulst, head of the unit for the fight against cybercrime and child sexual abuse in DG Migration and Home Affairs highlighted four main gaps that they have identified in the system, namely: (1) the fact that, while some organisations are truly committed to the fight against CSEAI, not all are, with the vast majority of reports coming from few companies; (2) the quality of reports, with some being of poor quality or that they may not meet the legal thresholds for CSEAI in specific jurisdictions; (3) the speed of analysis, which combined with restrictive data retention laws means some reports cannot be effectively followed up; and (4) the reaction to reports, with takedowns not always taking place expeditiously or, even, at all.

According to the Commission, the proposed Centre would support in coordinating efforts in the fight against CSEAI, creating more transparency and accountability for these efforts, developing and maintaining a reliable hash database and making tools available more widely.

Cathrin's presentation noted that the Commission has received strong feedback, urging that the proposed Centre not duplicate existing processes. In this regard, the Commission stressed its commitment to being additive and building on the practices and processes that are working already.

INHOPE network - the contrasting perspective of a German hotline, Eco, and the U.S. National Centre for Missing and Exploited Children (NCMEC)

We then heard from Denton Howard, Executive Director of INHOPE, a network of 47 hotlines around the world that coordinate the response to online child sexual abuse for their members. The network represents a varied set of hotlines, operating in different regulatory environments, with different capabilities and resources. Most hotlines in the network receive reports from the public only. In 2020, over 600k CSEAI related reports were received by INHOPE network hotlines (excluding NCMEC), with over 267k confirmed CSEAI URLs.

The network runs the ICCAM system, which is a tool that enables the secure exchange of information on illegal material portraying child sexual abuse between hotlines located in different jurisdictions, with the aim of quick removal of such content from the internet. ICCAM also provides a service to hotlines worldwide to classify images and videos according to international legislation (INTERPOL's criteria including Baseline) as well as national laws – all in one system.

During this presentation, we learned about the potential for a more global approach to addressing the challenges of child sexual abuse and exploitation, as well as the role that

the network can play given their track record supporting the rapid removal of content on a global scale through their notice-and-takedown processes. The full presentation can be found here.

Eco, the Association of the Internet Industry in Germany

The workshop also featured an intervention from Peter-Paul Urlaub, from Eco - the Association of the Internet Industry in Germany, running a hotline dedicated to the identification and takedown of illegal content, especially child sexual abuse material. Peter-Paul highlighted the specific challenges of a medium-sized hotline, with relatively large volumes of reports but without sufficient automation to deal with them at scale. Eco received 14,420 reports in 2020, the majority from named citizens and anonymous reporters. Some of the challenges faced include geo-blocked content and content kept under passwords or behind paywalls. Eco plays a role in supporting law enforcement by pre-assessing reports. The full presentation can be found here.

NCMEC - the life-cycle of a CyberTip

We next heard from Michelle DeLaune, Senior Vice President, and John Shehan, Vice-President, of the National Center for Missing and Exploited Children (NCMEC). Michelle and John gave an introduction to their CyberTipline, a centralized reporting mechanism for crimes related to the sexual exploitation of children. U.S. Electronic Service Providers are required by U.S. federal law to report child sexual abuse material to the CyberTipline if they become aware of the content on their platforms. NCMEC's presentation highlighted the borderless nature of this crime - approximately 93% of CyberTipline reports each year resolve to non-U.S. jurisdictions, so it is critical for NCMEC to have established connections with countries around the world to help ensure fast and efficient referrals.

NCMEC shared the web-based Case Management Tool they have developed to enhance and streamline the process of downloading and disseminating CyberTipline reports globally. Their presentation underscored the need for any system that is created to be future proofed -- both to accommodate evolving technologies and forms of communication (reports have shifted from just photos to increasingly videos) and increasing volumes of reports coming in to them. They also emphasised the need to invest in technology to help triage and prioritize the most urgent cases. NCMEC principles of "coordination" and "simplicity" are important for all of us to keep front and center as we think of the next frontier of reporting. Full presentation can be found here.

Law Enforcement Panel

The law enforcement panel was moderated by **Guillermo Galarza** from the International Center for Missing and Exploited Children (ICMEC) and included the following panelists: **Liv Almskog**, Swedish Police Authority, Swedish Cybercrime Center (Sweden); **Cathal Delaney**, Europol (Europe); **Michelle Ford-Stepney**, Interpol (U.S.); **Arnold Guerin**, Royal Canadian Mounted Police (RCMP, Canada); and **Hannah Jung**, Federal Criminal Police Office, Child Sexual Exploitation Unit (BKA, Germany).

The panel highlighted the complex ecosystem that exists to action CyberTipline reports throughout the world. Some police organizations, like Germany's BKA, are directly connected to NCMEC's VPN and download reports directly. For the BKA it is critical to be directly connected and not have any delay in downloading reports because of very strict IP retention requirements in Germany.

For other countries in Europe, such as Sweden, reports from NCMEC are first sent to Europol, and then are forwarded on to individual countries. Sweden noted the difficulty in delays for getting reports and also the difficulties of not knowing when or how many reported were expected.

Interpol has the unique role of transmitting and providing support for Cybertips in countries that are not either directly connected to NCMEC's VPN, or provided support through Europol. Interpol is able to leverage its worldwide network to get reports to often underserved countries.

Canada offered a unique example of a country that already has its own reporting requirements. The RCMP built their reporting system based on the NCMEC API in order for the systems of the two countries to work together and because NCMEC already had so much experience and knowledge in the area of developing effective reporting mechanisms. Moreover, under Canadian law a Canadian company can report a URL or an IP address to a foreign body for the purpose of blocking CSAI content similar to CIRCAMP or Project Clean Feed.

All of the law enforcement authorities noted that they are strapped for resources and overwhelmed by the volume of reports. They noted the need for better technology to vet through and prioritize reports, and more human resources to support the effort. They also noted how difficult it can be to get feedback from the field once a report is transmitted. The panelists noted that some of the keys to improved reporting from industry would be more consistency amongst the reports from different companies, and also more context around why a particular image/video was transmitted in order to prioritize high risk cases.

Europol noted that it is supportive of the EU center and wants to ensure the required resources are provided for everything from the IT support needed to work in an efficient manner, to victim identification tools. Europol also stated that the Cybertipline reports offer incredible intelligence and there are many abusers that have been found in Europe based on Cybertipline reporting.

Industry perspective: the Tech Coalition and case study: Yubo

Finally, the webinar included a session on industry'sviews, highlighting tech companies' responsibilities to detect and report child sexual abuse material online and protect children from sexual abuse and exploitation.

From Sean Litton, Executive Director of the Tech Coalition, we heard about the role that industry plays in tackling this borderless crime, by working collaboratively with users, governments, law enforcement and civil society. Safety is not used as a brand differentiator, and the detection and reporting of child sexual abuse material is an area where companies collaborate rather than compete. Examples of the collaboration include open source technology like Microsoft's anti-grooming technology, Google's Content Safety API and Facebook's photo and video matching technology, PDQ and TMK+PDQF, which is shared with others in industry and the wider community in the fight against CSEAI.

Of the 20 member companies of the **Tech Coalition**, 17 are based in the U.S. and are therefore under obligation to report apparent CSEAI to NCMEC as soon as they become aware of it. In 2020, companies made 21.4m reports to NCMEC. Over the years, the system of reporting has been improving, with strong collaboration between companies and NCMEC to improve the quality of the reports and the processes, including investment in NCMEC's case management tools.

According to Sean, key opportunities for the industry going forward include developing technologies that both respect privacy and help detect abuse; continuing to improve responsiveness to take down and law enforcement requests; improving transparency and continuing to facilitate cross industry collaboration. Key opportunities for policymmakers include avoiding duplicative and insconsistent reporting requirements, harmonizing the definition of online child sexual abuse and exploitation across jurisdictions, helping develop a systemic view of the problem, and using data to identify problems and prioritize limited resources. Complete presentation can be found here.

The last presentation of the webinar allowed us to explore the unique perspective of a EU based tech company. Yubo is a French social app that allows users to "meet new people" and create a sense of community. Annie Mullins, Safety Advisor at Yubo talked about how the company keeps teens safe online with safety specialists working 24/7 and

innovative algorithms to detect 'at risk' content, fake profiles, and direct interventions to protect and educate young people about their behaviour encouraging them to make informed choices.

Yubo operates under French and European legislation and as such is legally obligated to report CSAM to the French Law Enforcement Authorities. Annie's spoke of a fragmented system, with limited resources in national Law Enforcement Authorities to work with online platforms. Given their large US user base, since 2019 Yubo has secured dual reporting arrangements and are now reporting directly to NCMEC, even though they are not legally required to do so. Reporting to NCMEC has been simple and they want to see a reporting system that builds on the NCMEC strengths, which could be the European Center in the EU. Full presentation from Yubo can be found here.

Workshop: Key Strengths, Gaps and Opportunities

The presentations were followed by a closed-door workshop with 44 representatives from policy makers, law enforcement, hotlines, NGOs and industry. The workshop offered an opportunity to build on what had been shared and learned during the webinar to think creatively about how the system can be strengthened to offer better protections for victims of child sexual abuse and exploitation.

Participants were selected to provide informed and representative insights into the strengths and gaps of the current reporting arrangements and to identify opportunities coming from current discussions about future arrangements. Participants were split into four different groups of up to ten participants, with Tech Coalition members chairing the discussions.

Strengths of the current system

Workshop participants identified the following strengths in the system:

Participants stressed the importance of the well established process of reporting to NCMEC. In particular, participants highlighted the historical knowledge that NCMEC sits on, the great network of relationships with industry, law enforcement, and other NGOs and the sophisticated technology that they have.

While NCMEC is a US-based organization with obligations under U.S. law, their remit is global, as is the crime that they are set up to tackle. The depth of the relationships of NCMEC with Interpol and Europol as well as individual national law enforcement authorities was highlighted as a real strength.

Gaps

Workshop participants identified the following gaps in the system:

The jurisdictional differences in the definition of CSEAI was identified by participants as one of the difficulties in implementing a truly global response to the problem of child sexual abuse and exploitation.

The lack of clarity over the definition of CSEAI and other legal requirements have resulted in multiple hash databases, often with different hashes but also with duplication of content. It is not clear what we talk about when we talk about "known CSEAI", i.e. "to whom?" and "according to what database?"

While participants recognized the flexibility of NCMEC in taking reports from international companies, participants also highlighted that for non-U.S.-based companies there is lack of certainty over reporting requirements and processes, with companies committed to the fight against CSEAI often having to deal with multiple law enforcement authorities in an uncoordinated way.

Participants highlighted the need to increase resources across the system but also create processes that make the best use of available resources. In particular, participants highlighted problems with law enforcement being overwhelmed by the volume reports, having to deal with them with limited human resources and poor IT systems.

Participants identified some of the reasons behind high volumes of unactionable reports. For example, legal requirements mean reporting often takes place at an image level. Slight variations to an image can result in millions of different reports which doesn't aid, and in some cases can detract, from the identification of perpetrators and victims. Further, automated systems that focus on images/videos rather than victim or account/perpetrator level reporting may contribute to this effect. Additionally, tech companies may take a conservative approach to risk and err on the side of overreporting, resulting in higher volumes of unactionable reports.

Data retention laws are also an issue. For some countries, the very short periods for data retention mean that by the time the reports get to law enforcement the crimes cannot be investigated as all the relevant evidence is no longer available.

Feedback loops are not sufficient to help all stakeholders understand how their actions are having an impact and affecting others in the ecosystem. These lack of feedback loops mean the different entities have limited opportunities to learn what works best and how their actions are contributing, or otherwise, to identifying victims and perpetrators.

The role of the wider network of INHOPE hotlines was discussed, with some participants identifying missed opportunities for better coordinated work and communication between local hotlines and providers.

The current debate on privacy protection in Europe in relation to the ePrivacy Directive derogation is creating legal uncertainty and legal prohibitions over what can be detected and what are the safeguards that need to be in place, potentially discouraging providers from innovating, detecting and reporting CSEAI.

Participants also highlighted the underrepresentation of disproportionately affected countries and victims, linked to adjacent cultural and resources issues.

Opportunities

Participants identified the following opportunities in the system to build on the existing system while helping address some of the gaps identified.

- Integration of existing databases, with regard to legal limitations, or at least improving the consistency across multiple databases.
- Consistency of definitions of child sexual abuse and exploitation across different jurisdictions.
- Provide legal certainty over the basis for data processing and data transfer.
- Clear reporting routes for all companies regardless of geography while avoiding dual/multiple reporting requirements (e.g. Canadian model of reporting requirements).
- Clear taxonomy of reports, with reporting obligations on all CSEAI but a more nuanced approach to how to prioritize reports for investigation that can lead to victim identification and prosecution of perpetrators.
- Further investment to support integrating the system of reporting at the back end, with additional human resources and IT for law enforcement.
- Consistency in industry and LE's framework of risk assessment, prioritization and classification.
- Legal recognition of hotlines at EU and wider international level, with investment on building on the existing expertise on content review and moderation and better routes for international cooperation between hotlines, industry and law enforcement.
- Investment in NGOs and the wider ecosystem to develop a trusted flagger type system, where trusted NGOs have clear routes for reporting illegal content.

- Cross-industry cooperation to support start up and smaller companies develop their understanding of the system of reporting and support them accessing technology to support their efforts.
- Investment on victim support, e.g. local resources for mental health support, victim identification, etc.

Next Steps

The **Tech Coalition** is committed to fostering a culture of dialogue and understanding between all parts of the ecosystem fighting to keep children safe from sexual abuse and exploitation online. This event held on the 24 and 25 March is a testimony of the shared commitment and passion of many individuals across all parts of the system to this mission.

The discussions showed that this is a complex issue that needs careful consideration and attention. There is a robust reporting ecosystem that exists globally through NCMEC, however various parts of the system need to be addressed and all need to work together to better protect children from sexual abuse and exploitation online.

We also know that this is a global problem and that there are different challenges and issues to be addressed in different parts of the world, particularly in developing countries and we do hope to dive deeper into those issues and regions at future events.

This event exploring the next frontier in reporting is part of a stakeholder engagement effort by the Tech Coalition. Future events include:

- A workshop on 28 and 29 April, 2021 to explore the challenges of Self-Generated Indecent Imagery Featuring Youth.
- A Multi-Stakeholder event on 15 and 16 June, 2021 to celebrate the one-year anniversary of the launch of the Tech Coalition Project Protect, where we will be sharing the outcomes of the two workshops on the next frontier of reporting and Self-Generated Indecent Imagery featuring youth and continue to explore ways in we can work together to deliver on our mutual objective of combatting child sexual abuse and exploitation online.