FINISHED FILE

ASIA PACIFIC REGION INTERNET GOVERNANCE FORUM
TAIPEI 2016
A NEW INTERNET ERA
28 JULY 2016
ROOM 402 A-B
1400
MERGER 1
THE ROLE OF THE KEY STAKEHOLDERS IN DISRUPTING THE DISSEMINATION OF CHILD SEXUAL ABUSE MATERIAL (CSAM) ONLINE

Services Provided By:
Caption First, Inc.
P.O Box 3066
Monument, CO 80132
1-877-825-5234
+001-719-481-9835
Www.Captionfirst.com

***

***

>> MARIE-LAURE LEMINEUR: So it is -- sorry. So we will allow another five minutes to just give the opportunity for late comers to join in. Thank you. So can we start? Are we ready over there? So good afternoon. It is 2 p.m. It is a tough time because it is just after lunch, but I hope that we will be interesting enough so that we keep you awake.

So allow me to introduce myself. My name is Marie-Laure. You can call me Mary. I am based in Thailand. We are a network of NGOs, of actually 90 NGOs in 82 countries and our objective is to combat the sexual exploitation of children. I am in charge of the topic of sexual exploitation online through the use of ICTs. A little bit of -- before I introduce the speakers let me clarify that we -- I guess you all know that we are being recorded. There is a transcript over there. We have remote participation. We will have one remote speaker.

And now I think I can -- what we are planning to do is to have a presentation. Each speaker is going to speak around 10 to 12 minutes. Then we will open the floor for questions. And then we will wrap up the session with concluding observations. But, of course, if you want

to make -- to ask questions, you know, before we open the floor, please feel free to do it. And we will take the questions.

So with us today we have Ms. Celeste Yang who is a corporate attorney for Microsoft Taiwan. And then we have Chen Shihying who is a member of ECPAT Taiwan. They do excellent force. Then we have David M., is that correct? David M. So I was briefed but I did a good job. David is the director of community engagement with the DotKids Foundation based in Hong Kong. And then finally we have Ankhi, Ankhi Das who is based in India and is the Facebook public policy director and she is covering the region. She is covering India, South and Central Asia. And we have a remote speaker who is Ms. Bindu Sharma. She works for the International Centre for Missing and Exploited Children which is known as ICMEC. She is based in Singapore. And she is the public policy director for the region, for Asia-Pacific.

So the topic that is bringing us together today is the role of key stakeholders in disrupting the dissemination of what we call sexual abuse materials online and some people refer to it as child pornography. But the terminology is very important to us. But you need to understand this is what we are talking about, child pornography.

So very briefly what I would like to say is that I don't know whether you saw it but the International Telecommunication Union, the ITU, they issued their annual ICT statistics and the statistics were about Internet connectivity. When you look at trends in terms of Internet connectivity you see that 47% of the world is connected. This is beyond 3.5 billion people in the world. And when it comes to the region, Asia-Pacific is almost 42%. It is 41.9%. Those are the latest figures. So clearly here even if there are still a lot of gaps in terms of Internet speed, you know, broadband speed, costs and this -- we are not here to discuss this today. But I mean we all are aware that it is happening. But the spirit behind my comment here is to make you aware there is a trend here. It is increasing connectivity and, of course, with the opportunities that this brings they have, you know, increased exposure to risks and people increasingly being harmed also and especially the most vulnerable sectors of society who are the children. So we have -- we have wonderful, many, many opportunities for all of us and even for the children who can exercise their rights online and the same way they do offline, but they are also exposed to risks and some of them are being harmed.

So this is why there are many, you know, global initiatives and one of them you might have heard is called We Protect Global Alliance that has been launched a couple of years ago by the UK Government. And what is interesting is that they issue the -- what they call a model national response. You might be aware of it. And basically it presents all the areas in one particular country that should be tackled in order to be able to disrupt child sexual abuse materials

online. So depending where you belong, if you are the private sector, if you are Civil Society, if you are social workers, Government, depending on where you are, if you look at the model you can see the pieces fitting together and all coming together, then we will be efficient in disrupting child online abuse materials. And this is why we are here all of us today. We had this idea that none of us alone has the answer, you know, and all of us we have a role to play in disrupting this kind of abuse and exploitation online.

Each of the speakers they are going to present their own perspective about what they do, what they could do and what are the challenges. So I have spoken too much. So now I'll give the floor to Celeste who can further explain what Microsoft is doing in this field. Thank you very much.

>> CELESTE YANG: Thank you, Marie, for the great introduction. And I'm extremely honored to be here this afternoon to talk about this very important issue. As Marie talked about online child sexual abuse images are a really serious problem on the Internet space. So I would like to, yes, to first talk about what our commitment is. So it has been over a decade that Microsoft has been committed to be a trustworthy computing company. We want advocate online safety. And we think it is important everyone understands how to be a digital citizen which means to be -- to provide a safer space, to be a more responsible person. So when we do see these images online what can we do as a person or as a law enforcement or as a company that has access to all these kind of images? So we created a special department in Microsoft called the digital crimes unit. It is known as DCU. And for DCU we have two important goals. One is to keep the Internet safe from malware attacks. So we are fighting malware. And the second part is we want to protect the vulnerable population. And the vulnerable population would include children in this case. And we also work on elderly people's scams, text scams currently. That's the two big projects.

So for the vulnerable population, the problem we are facing now is that here are some statistics I would like to share. So one in five girls and one in ten boys will be sexually abused by the age of 18. And that's a very high percentage. And a lot of times while this abuse occurred images are stored and we have to understand when these images are transferred and viewed every time it is a reabuse to the victim. Okay?

So if we take a look at how many times these pictures are being transferred, so there are 500 images of sexually abused children traded online approximately every 60 seconds. So it is not just the victim itself. Now the images are becoming over and over mailed or sent and received and viewed. So there are about 1.8 billion images uploaded and shared every single day. So the problem now is on the Internet space there are so many pictures, so many images online. How do we find them? Right? Is it by viewing them? But as we just

mentioned every time you view it the victim feels she or he is revictimized again. So this is probably not a very good way to approach it considering the larger amount of images and the possibility of seeing the picture which might cause more damage.

How do we do, what do we do? How do we tackle this problem? So finding a child sexual abuse image out of billions is like finding a needle in a haystack. We want to find it but we want to find it appropriately. Microsoft worked with Dartmouth College and ICMEC to work on a technology called photo DNA. The goal is that we want to protect these children. We want to bring more awareness and also we want to partner with different organizations or law enforcement to do this.

So let me briefly talk about what photo DNA, how it works. Right? First there are five stages, okay? First we would rely on a trusted source. It might be an organisation. Right? Like in the U.S. it is NCMC. In Taiwan it is Taiwan ECPAT. We are very grateful that they are working with us. And we give the technology to them so they have the ability to identify these images. When they have these images they can use photo DNA to transfer the image in to numerical numbers. So it becomes like a digital fingerprint, a hash number. So when you transfer the image in to a number, you don't have to see the image anymore. And the victims they don't have to feel like they are being viewed again. But at the same time they will have the assurance that we are doing something about these images. So that's the value of photo DNA. They can transfer this image in to numbers.

And then once you have this hash, then we start working with different organizations or enterprises or ISPs where content generated by users where they might have a lot of images on their website. Then we would also transfer those images in to numbers and do a matching. Right?

So if the number, the hash matches then we know that on this website or in this organisation there is that particular image, then we can communicate to the law enforcement or others to take it down.

So that's the whole idea of photo DNA. We develop this idea at this technology and we work with different NGOs to spread it out. Okay.

This win. Sorry. So we are now working with different companies including Facebook, Google, and Twitter and different -- and they are all -- we are providing this service for free. So they can really use it to decrease the damage to these victims. So now we have like over 100 organisations using this technology to keep the -- their platform safe. Okay?

And the next step for us is to really bring this awareness to not just this hundred organisations that's been working with us. But we want to have this technology built in our product for all our customers, enterprise customers. So this is telling them that well, it is not just that the images outside of your organisation on the

Internet or websites that you should be concerned about or that you can do something. If this image is within your organisation, and you are using Microsoft product Azure which is already built in with photo DNA technology, the customers get this for free, that they can also do this matching within their organisation. If their employees are viewing these kind of images and there is a match, then the company itself can actually do something as well. They can ask the employees to take down this image and restrict them from sending it further. But this is not a spread yet. It is just a new initiative for Microsoft. So now we are trying to talk to all our customers about this photo DNA cloud solution and it is a free solution for them. We would like to encourage them to adopt it in their environment.

Okay. So it is very secure, right, and it is efficient. The matching can be done in a very efficient way. And the interoperability we have made it in to a REST API and it would work on an Android system as well as an i/OS system or Windows system.

And then another thing we did which was quite recent, it is in December 2015, we also updated our photo DNA skill and now the speed is like 10 to 20 times faster than before. The matching time is 10 times faster. So this is something else that we are doing. We are doing everything we can and hoping that this problem can be decreased. And we do realize that this is something not any single sector could solve the problem. Everyone has to come in and do it together. That's why we protect, is very important initiative in UK. So now apart from -- so for the enterprise customers, of course, if it is a big company, we encourage them to adopt it. And if their Internet service providers like ISPs their content is generated by their users, we strongly encourage them to adopt that because that's where a lot of images will be uploaded.

Okay. And another thing we are doing in this view is protecting the elderlies. I will go quickly. How am I doing with time? Two minutes. I will do really fast. For the elderly people now it is a very big problem that a lot of pensions are being taken away because of their -- a lot of scams, tech scams. So DCU is also working on this with different organisations trying to protect one of our population. So these are just some numbers that we feel we are confident, that we can do because we have a lot of data. We are like a data center. Microsoft has a lot of data because of our products are used widely world wide. And we feel we can analyze that data and maybe come up with better solutions in the future.

So I will quickly go through this and I will probably skip the malware part, but I would like to talk about the latest project that we have done in China. Usually every year inside Microsoft we have an event called Hackathon which they encourage our employees to design new technology, skills that can solve problems that are currently in the world. And then we will pick out the top five or six inventions every year. And last year the Hackathon 2015 they picked out this

technology called photo MC. It is photos of missing children. And in China this is a huge problem. The children go missing because of kidnaps or maybe there's a strong belief boys are better than girls or child labor. So they applied this technology to find these missing children. However there is a problem. Because children you have photo of a child but children grow up much faster and they change. They change. They don't -- like if for me three years later I hope I still look the same.

(Laughter).

>> CELESTE YANG: But for a child three years later they probably change dramatically. So how do we use this technology to find missing children? And surprisingly this technology can -- actually it is the same, do a hash, do some calculation. And it could recognize up to 75%, right? Even if you grow up they can still recognize you. So it is a really exciting project for them in China. It is a pilot project, just a reminder. It is not a proper solution yet. It is just something we are doing. Hopefully this can be used for other uses, that would be great. And let me show you the child that they actually found early this year. So if you take a look, the initiative was last year June. And only within like half a year, right, in June 29th they found someone. So this child he is intellectually a little bit disabled, right? So -- and he went missing in 2012. And then his parents put his picture up and he was actually found very quickly, but he has been missing for four years. And the technology still popped up his picture. And instead it was 75% similarity. Right? So -- and another difficult part is this child is with a disease called -- I don't know how to say English. What's it? Down Syndrome. For us human eyes actually they all look very similar to us. Biotechnology can tell a difference. So that's another thing we discovered. And this is just a great initiative. And we hope that we can bring this over to Taiwan as well, all over the world. Yeah, I think I am using -- over my time. Thank you so much.

>> MARIE-LAURE LEMINEUR: Thank you so much. This morning I was reading on the news in the U.S. right now those days an organisation called Thorn, digital defenders and they are partnering with Microsoft and they are doing a Hackathon over there and exactly working on digital facial recognition solutions. If I may add and build on what you are saying this is useful for missing children but also for children who are portrayed on the images of sexual abuse and exploitation because those kids, law enforcement officers many of them are not identified. They have the pictures on the database, but they don't know who they are. Meaning they don't know where they are. Meaning they cannot rescue them. So these kind of technical solutions are absolutely key and it is a really positive initiative. So let's move on and have Claire make a presentation. Thank you.

>> CHEN SHIHYING: Hello. Good afternoon, everyone. I'm Claire of ECPAT Taiwan. Okay. Today I am going to talk about what

we are doing in Taiwan. First why we start concerning online child sexual abuse over child online safety, because we found that emerging problem is in encoding, children being -- going through Internet contact such as children, Social Networking Sites and the child sexual rage online and child addicted to Internet games and online chatting and imported child sexual abuse and material distributed by Internet and cyber bullying. Therefore we began our child online safety project which including reporting hotline, help line, education, legislation, and we held child sexual exploitation training initiative for law enforcement every year.

Now I would like to introduce what we are doing in our hotline. In 1999 we launched the reporting hotline named Web 547 and it become a member of International Association of Internet hotlines, INHOPE. Follow the line of Taiwan and protocol from INHOPE we deal with, report on the content of three categories of assisting types, including child sexual abuse content, adult pornography and other illegal content like poor video games, drugs and so force.

And last year we received over 8,000 reports from Internet users and among them which -- over 200 reports are child sexual abuse contents. And when we -- if the content is located in Taiwan we will report to our law enforcements. If not we report to hotline members over law enforcement like FBI, HSI or visual team member.

This is a statistic number for -- for six years. Some people may think it is -- it look serious problem because maybe 200 reports or 300 reports compared to maybe in United States or in Europeans, they have a huge number. But I would like to remind you every single report they have hundreds of images in size. So this is the situation in Taiwan.

And in this slide I list related laws and as in Taiwan. Basically they all define producing, selling, disseminating, displayed and position child sexual abuse contained and grooming of sexual content with children should be illegal. Now I would like to show some new development in Taiwan. Two years ago we was reviewing the amendment of the child and youth sexual exploitation Act and it will come in to force this year. The key element of the amendment like we change the concept to sexual transaction to sexual exploitation. This is a major one. And we define four types of child and youth sexual exploitation, including child prostitution, child pornographic performance and child sexual abuse and child as a bar hostess or escort. And we enhance the responsibility of ICT industry. Right now we define that teleservice provider, Internet provider and application service provider. They all should have to complete with the notice of takedown procedure and preserve legal content for at least 90 days and cooperate with police for investigation. And the company who failed to obey will get a fine. Certainly we punish regarding online session exploitation. Like watching child pornography of streaming video should be illegal.

>> MARIE-LAURE LEMINEUR: Can you explain for notice of takedown?

>> CHEN SHIHYING: Right now it is a universal principle. When a company, industry like in our -- like Google or Facebook where they get a report in their spacer, they have some person upload illegal content. When they get a report they should remove the content immediately. And they should serve evidence for the police -- law enforcement to do further investigation. We want to enhance the speed to remove the content because every single second the image lays in the Internet that means that maybe one or two of them, hundreds of persons have the chance to see the image. And for the victim the image is a second or third abuse again. So it is to remove the content immediately. Right now the major company they have to follow this procedure. Yeah.

And the International Centre for Missing and Exploited Children, I think the speaker next she will mention more but I want to highlight some criteria here. They do research in to law that in this around the world to have a better understanding of how countries deal with the problem. Last year the population additional child pornography model legislation and global reviews. I use child pornography because in the United States like officially use this term. In the youth they say male criteria to value a country delay, have a better sufficient law to do with this.

Okay. You can see the first one does have a journal of child pornography and define what child pornography and they do criminalize the computer facilitated offense and does national legislation criminalize possession of child pornography. Does national legislation define -- require the ISP to report child pornography to law enforcement or to some other agency and require the ISP to develop and implement data retention and preservation vision? Why is it important? Because we are not mainly to remove the content, we want to catch the big guy and we want to rescue the victim. So -- if the content just removed, the law enforcement cannot have enough evidence or information to do further investigation. So we -- so this time they highlight the data retention and the preservation is very important. So you can see the industry or company play an important role in combatting child sexual abuse.

But the challenge we are facing now even in the Asia-Pacific Region there are some countries that do not define ISP or ICP like ability to report child sexual abuse content. And the second one you can see in the slide, this is popular in Taiwan. Like Facebook, Youtube, Google, by do online we chat, V block. It is very popular in Taiwan but Facebook, Youtube or Google or Microsoft, Twitter they all come from the United States and they follow the United States laws. And like Line it is based in Japan and we chat, we block, is mainly for in China.

So the international Internet company reports child sexual abuse

to authorities based on the home law. And they report to the authority of the country where illegal user allocate. Take Facebook, for example, there are a lot of users in Taiwan. When they detect child sexual abuse being uploaded to Facebook they will submit to the United States organisation. What if illegal content come from Taiwan? We cannot get the information. So we can get big guy's information. We cannot catch the guy in Taiwan. Like if Google when they detect the person, so it is the same.

And then the third, the global international -- the global Internet company like Facebook, Google, Microsoft, Twitter they have all reached consensus of working together to combine child sexual abuse material, but for regional ones how to make them to be part of a member and dedicate to protect child exploitation like Line, the company made in China. I don't have an answer right now. Actually I have to tell the truth, I don't have an answer right now. That's why we come together. We can have the same conversation.

So I want to emphasize again the picture you see is not just a picture. It is not a pornography picture. They are not -- we are talking about online child sexual abuse content. It is not victimless crime. Every -- so every -- the victim inside they abuse us again and again when the people -- once the people reveal their image. So they will tolerate -- they will live with the trauma for every day of their life. And you will repeat every child when the image of them being victimized as a distribution. Government, law enforcement, NGOs, you, me, industry, everyone we should work together to protect children from online sexual exploitation. Thank you for listening.

>> MARIE-LAURE LEMINEUR: Thank you, Claire. Very interesting points you raised and the last one particularly because many people do tend to think that because those are images they just look at them. They don't touch a child. So they think there is no victim. That's the argument. We don't damage any child. We are just looking at the picture. So that's why the community, those of us involved with this kind of crimes we do insist that it is not a victimless crime. There is a picture of a child who has been physically sexually abused of this picture. David, the floor is yours.

>> NG KI CHUN: Hi. We get some new initiative coming up. So far my presentation is mainly focused on some new initiative and the other sense is advocacy work that we are doing now. As mentioned by Claire, she also mentioned about the United Nations Convention on the Rights of a Child. I think it is a very important principle to adopt it and mention throughout the period of time we mention how we can put children online. In other sense of this workshop we also talk about the collaboration of different stakeholders. So I will also mention about this area in my speech.

And nowadays as we all know ICANN is the cooperators of the Internet. They get a new program called new gTLD program was launched in 2011. On the sense it allows people to apply for new domain names

on the Internet. Right now maybe we -- we will get dot com, dot hk or dot tw but in the coming future they have more to come. This is the new domain names that are coming in our future. In 2014 the ICANN they have written down some related domain names in the new round of gTLD application which is related to children. For example, DotKids, Playskool toys. This is the domain names which is coming up online and some of it already dedicated and will soon appear in our Internet.

Sorry for the -- actually it is a bit late. On us we think these will allow for the DotKids domain names that we want to run as an initiative. We want to create a child friendly Internet from the Top-Level Domain names. From the best interest of children would be one of the sense. As I mentioned about kid friendly or child friendly I think most of us will think about this in this way. Maybe the photos on this website is we have simple language. Maybe easy to understand. More interaction to be done among children and Internet content providers. As I also mentioned about the UNCRP. We like to run a kid friendly Internet in this way. This is the way that we adopt the principles of the UNCRP. These three basic principles is nondiscrimination with child participation with the best interest of children. And I think extending these principles on the Internet it can be like considered best interest of children and always think about how we can protect children, but at the same time we would like to allow children to get their right to access to Internet. And also the information they get will be free to be assistible. For discrimination I think all of us understand the problems of digital divide. On the sense we can understand these ways.

Everyone got the SS to Internet in a sense and we are supporting children to get online. Last but not least is about the children's participation. In a sense of children's participation is very crucial in the stuff because where we consider what is the best interest, children's voice should be put in the consideration, not only just on the perspective from adults and other caregivers but children participation, their voice, consider them will be fit the needs of children themselves. For us I think -- as I have mentioned previously on the collaboration of different stakeholders we are now working on some content guidelines and some back practice of how the top domain names should be run. For example, the child sexual abuse content will be put online. It should be -- but on the other sense you got some great areas on the Internet. For example, how about the commercial advertisement online is McDonald's selling junk food to children is allowed on this website. Because for domain names which seems like putting out -- we are like spotting out a group of children users or target users for the Internet. And then it will be easier for the commercial to provide information and provide content to those Internet users in a sense. This kind of back practice should also be mentioned and also be discussed not only from the child recommend

this but also from the all Internet users, the industry or even like business centers, all of us should be involved in a sense.

And as I have mentioned about the children participation I think for the next experience of Internet it should be about children and youth. How we can better engage them in the discussion process and note about their own rights and responsibility online this crucial issue to deal with nowadays. If we haven't done anything right now, it would be our future Internet and our future development for the substantial development of the whole Internet in cyberspace. For us we have organised the Children's Forum like the ICANN meetings in Beijing which is in 2013. We invited the children's group and China organisation from all over the world, like Cambodia, Egypt, Hong Kong, Indonesia. They will be attending the conference to understand how ICANN is operating and the issues that are the most important. I know that the policy discussion is quite tough for children. Without this type of capacity building we cannot do anything for our children to have a better future. We are working on an initiative in China, Children Summit and just organise in this month. About ten main countries, children have attended this Summit. And it is also adopting the model of the UN IGF is embracing a multi-stakeholder discussion. They got the role play sessions on putting their own position in to different perspectives to think from different perspectives. That will allow them to have a sense of how the governance nowadays is.

In a sense how we can tackle the problems of child online safety, children's participation and your empowerment should be another area we should focus on. This is some of the work we are working on. And, of course, for the new domain names I have mentioned about DotKids is upcoming to be a new revolution on the Internet. We have -- we go through the process and right now is on the last stage. We are rolling it out quite soon. As soon as we get the domain names it is important to let the community to know about the threats and how we can collaborate together.

So I think to building a community is crucial because nowadays the Internet is not just a country, just one country, two countries. But it is affecting various countries in a sense. That's why we are trying very hard to promote ideas and getting support. No matter who runs domain names it should be for the best interest of children and for the well-being of children. That's why the cooperation is crucial. Children participation is crucial. With appropriate guidelines we will put children in high risk. But we can see in other way it has got opportunities. Because it is a new initiative, we can have some campaigns or some advocacy work to be done, to have a platform to engage everyone on discussion. Especially on Internet governance it is different from the past structure. It allows everyone to discuss and also making policies. This is the critical resources will soon appear online. And we will want to invite everyone to give us your

ideas and engage in the discussion process.

And the workshop also mentioned about the collaboration of different stakeholders. Also like to introduce a program we are organising in the coming future which is in the preparation process will soon appear in next month. This is a new help line initiative. DotKids Foundation partner with the Netmission, the youth group for the Asia region and also local partner youth online association. We are based in Hong Kong for this initiative. We want to bring a reporting mechanism on the child abusive content online to Hong Kong to answer reporting mechanism. And we also gain the support from the state of Hong Kong getting some financial support on them. That will be an upcoming initiative, but on the sense of this website we will do on the reporting mechanism which is a beta version right now. Soft launch soon on this coming time. On the sense I would like to also state this is important to get different stakeholders to involve to tackle the problems because as you have seen the organisers and supporters is just coming from the Civil Society. But for the issue is not just community to deal with based on the effort from the communities and from the Civil Society. It also lists the industry support and also the Government support. For example, just list out some objective and outcomes. And the network we have right now cooperating with to state that for the first objective it should be linked with the global network to combat the CSAM, which is the child sexual abuse materials. We got some network with INHOPE. They are doing great work to create a network of reporting those materials online, those CSAM materials online. Because when they got the report on the child abusive content, there is not just on one country's issue. Because sometimes or not sometimes, most of the time the materials is not just host in one countries. It should be hosted in different countries. In a sense a network, a group of networks need to be adopted and collaboration among countries is important in a sense to taking down those materials by collective effort. For the second point I mentioned about is the multi-sectoral engagement to create child online Internet. Because the reporting mechanism if it is just host by a Civil Society, the activity takedown cannot be run that smoothly. It should cooperate with like ISP and also like law enforcement department, like the police force in Hong Kong to do the activity takedown and the process will be one in an efficient weight. So that's why multi-stakeholder engagement and cooperation is crucial. But on the other sense not only the reporting hotline is important but it is also -- it has got some engagement projects or safety projects already done. We know, for example, in Hong Kong we got the privacy commission. They are promoting the data privacy of children and also every Internet users. They are always doing the work on data privacy. And also for some NGOs they are already having some campaigns and Ambassador programs on promoting the issues. So I think on the other sense not just like takedown or stop the images is just one way. We

should also do in other way to have cooperation with other initiative and also existing child safer Internet initiative to get cooperation to free up all the gaps for children promotion, for children protection. Of course, the training and overseas experience sharing is also another sufficient issue to make. We can move the thing and work together.

So in conclusion I think the issue is not just on one country cross-border and multi-country cooperation is needed. For multi-stakeholder collaboration is also needed, a Government industry, NGOs, caregivers like parents, teachers and, of course, children themselves is important in the issue to get them empowered. This is the model we are embracing and looking forward to see some cooperation together. I think to cause it in a slogan maybe, together we can build a better Internet together. So thank you for all for your time and thank you for your attention. I pass the mic back to you.

>> MARIE-LAURE LEMINEUR: Thank you, David. Very interesting. For those of you who might doubt that domain names are not that important, and David, of course, tried to explain that it is important, in the latest report of the Internet Watch Foundation which is the equivalent of ECPAT Taiwan, its online reporting mechanism, one of the biggest in the world for the UK for the first time this year they say that they found many images in websites, using new domain names for the first time in the history since the existence. The domain names are quite new. So that's the first time they show up. And they took action on 436 websites that were created with those new domain names just with the objective of sharing child abuse materials. So this is why this is very important on top of what David just said. Thank you very much. I think now for being due to its -- the turn of Bindu.

>> BINDU SHARMA: Yes, I do hear you. I have been listening to everyone.

>> MARIE-LAURE LEMINEUR: Thank you very much. The floor is yours.

>> BINDU SHARMA: Thank you. Thank you. Good afternoon, everyone. Greetings from Singapore. It is a pleasure and a privilege to be among a group of people dedicated to child protection. I would like to thank David from DotKids Foundation and Marie-Laure from ECPAT. It has been a part since its formation and worked with ECPAT International staff. And I think an ex-colleague of Marie-Laure, pleasure to be here. I guess being the last or one from last speaker makes my life easier for a lot of people have covered much ground on what I was going to talk about.

I will just start with a brief introduction to the International Centre for Missing and Exploited Children and as Marie-Laure said we refer to ourselves as ICMEC. It is a global NGO headquartered in Alexandra, Virginia. Advocacy, training and collaboration. To achieve that we identify gaps in the global community's ability to

protect children from abduction, sexual abuse and exploitation and people resources and tools to help fill in those gaps. Next slide. I think I have been remiss in saying next slide.

>> MARIE-LAURE LEMINEUR: It was my fault. I was concentrating on listening to you and I forgot about the slide. What we do is the next slide?

>> BINDU SHARMA: Yes. Thank you. We do a fair amount of research. And nice to see I think it was Cheryl from ICMEC Taiwan that talked about ICMEC's child pornography model law research. We use research and evidence based studies to advocate for changes to protect children worldwide. We also do -- globally we train and assist law enforcement leading professionals, NGOs and Governments run the whole issue of crimes against children online. And ICMEC had mentioned about law enforcement training. We partnered with ECPAT Taiwan and we did a law enforcement training for Taiwan police. And one program that I will highlight, one of the global coalitions that we lead, one of them being a financial coalition against child pornography and the other being the global health coalition and looking at the whole health issue and protection of children and other child abuse and all of this we do by promoting public/private partnerships.

However as a lot of the other speakers have said I would like to address the use of the term child pornography. There has been an -- ECPAT International came out with an excellent semantics and terminology report. There has been a lot of movement towards using the term child sexual abuse material or child sexual exploitation material. But it represents also -- a lot of the work we do we retain the term child pornography for unfortunately it is the term commonly used in legislation in all countries around the world as well as in the UN Conventions.

Next slide. So why focus on online? I know a lot of others have talked about it. I just want to highlight the fact that it is online and a fair amount of it is commercial. People will pay for these images. Viewing these images or as we have unfortunately seen from the Asia region, live on-demand sexual abuse coming out of some countries.

What I would like to highlight prior to the arrival of the Internet it was extremely difficult to obtain these images. Interested in something like this had to know someone who had these images or did considerable personal risk in producing such images. And also prior to the Internet someone with sexual interest in children felt isolated and alone. Using 1995 as a baseline Interpol reported knowing around 4,000 unique child abuse images in total worldwide in hard copy.

However today we know that cyberspace is home to more than as we heard from the Microsoft presentation, more than a billion images circulating with a huge number, I think I did write the number down, we upload every -- 500 images being traded online every 60 seconds.

So today offenders are able to interact online with people with like interests worldwide. He or she is part of a global community that shares these images, techniques and in some cases even children and all of this is done with virtual anonymity of the Internet.

Next slide, please. I won't go in to the whole issue. It is a victimless crime because speakers ahead of me have done a good job of making a point this is not a victimless crime. Once the image is up there it is there.

So as I said why online. As you can see there are close to 7.4 billion people in this world. And at -- and over 3.4 billion are Internet users. 3.8 billion of these are unique mobile users. The Internet is suddenly rapidly changing that access and therefore the whole issue of risks to children online is exponential.

Next slide. And as we see from one of the reports of the UN Special Rapporteur on the safety of a child, child prostitution or child pornography report at any given moment on the Internet globally there are 750,000 offenders out there trolling the Web looking for these kinds of images exchanging them and that only, you know, highlights the risks that children are at.

Next slide, please. You can see data tells us that anywhere from 7 to 10% over the last three years of images of children -- the majority of these images are of children under the age of 10 to 12. Unfortunately girls are a lot at risk than boys.

Next slide, please. Thank you. And on the commercial side I would like to highlight that over the years anywhere between 9 to 18% of websites confirmed to be hosting sexual abuse materials are commercial in nature and what does that mean. As I said earlier, people will actually use electronic payment platforms like credit cards, debit cards, PayPal accounts, related services, increasing mobile digital wallets as well as digital currencies like net coin to pay for access or I will try to exchange of these images.

Next slide, please. And as we are all aware all sorts of platforms on the Internet are used whether it is just plain websites, where e-merchants are using these as business opportunities, cyber hosting services, social networks as well as bano sites. A range of websites and, you know, Internet platforms are being misused.

And what does the reality of this -- I know Microsoft we got some figures there. But I would like to report just coming out of the U.S. the cyber tip line which is the hotline reporting mechanism in the U.S. which was formed in 1998 has been then through April 2015 received more than 4.3 million reports of prospective child sexual exploitation materials. The national center also runs a victim, child victim identification program which was started in 2002 and again through April 2015. They have reviewed and analyzed over 139 million such images, trying to rescue and look for children who have been abused.

And another statistic that I bring forward was cyber to Canada.

It is the reporting mechanism hotline in Canada. Over a two-year period of 2007 to 2009 they did a survey of payment mechanisms that were advertised in online. And what they found was 27 different payment mechanisms were advertised on various child sexual abuse websites. 85% of these sold memberships was recurring monthly payments ranging anywhere from $4 to close to $500. When you see these kind of commercial enterprise, you know that the financial industry has a role to play. And lastly I bring up the data coming out from the UN ODC report on transnational crime which was put out in 2010. They estimated that the industry generates about 50,000 new images each year. And the global industry is worth about 250 million. So what can we do about it? I was asked to talk about cross-sector partnerships. I give an example of one of the programs that we run. The financial coalition was first launched in 2006 in the U.S. with the National Center for Missing and Exploited Children and the International Center for the Secretariat. The aim here was to disrupt the economics of the child pornography business.

Next slide, sorry. It is a powerful coalition initiative between the financial industry, Internet companies, Facebook, Microsoft, Google and others. We are working collaboratively and voluntarily with the national and international center as well as law enforcement to really understand the business models of the e-merchants that are selling illegal content but using very legitimate corporate platforms for the sale and dissemination of this. In the U.S. we say the coalition is operational. Where the financial industry has provided law enforcement, live accounts to use to do test -- what we call test transactions. And that's what helps us understand what kind of business models these e-merchants are using. And under U.S. law if law enforcement is doing a test transaction it is legal and does not amount to entrapment. There is a robust example of cross-sector partnerships between industry, different industry, financial, technology as well as law enforcement and Civil Society. Next slide.

In 2009 ICME set up the Singapore office and launched the Asia-Pacific financial coalition. To really widen the fight against the commercial dissemination of sale of child sexual abuse materials the aim here once again is to disrupt the economics of it. What we realized initially and at least in this part of the world we had to do a fair amount of awareness building, educating industry as one as Governments around the fact that this happens on very legitimate corporate platforms. And it is not only an issue which I very often heard in my initial days of this work was oh, it is a western problem, it does not happen in Asia. However the Internet shows no borders. And hence it is a global issue and a lot of the effort has been in awareness and education building and more recently it has been to build national networks in targeted countries where we can actually work in the collaboration with law enforcement at the national level,

try to understand with business models. So a fair amount of due diligence through industry and law enforcement cooperation.

Next slide. As you can see the Asia-Pacific membership is quite a diverse stakeholder group here. We have banks. We have the payment industry which is MasterCard, Visa, PayPal. We have different law enforcement from different countries. Industry association taking over the bankers association, card risk, Australia. Technology companies as well as NGO partners. It is a diverse group. It is -- one of the speakers said earlier this is one issue where even industry where there may be competitors of the commercial side have come together to work and fight this fight together.

Next slide, please.

>> MARIE-LAURE LEMINEUR: Sorry but you will need to wrap up please because otherwise we won't have enough time for questions.

>> BINDU SHARMA: I am getting there. Next slide. So they have already said in the Asia-Pacific Region I have done a fair amount of seminars and Round Tables around the issue creating awareness. We have done Round Tables and in New Zealand I run an operational coalition where banks and law enforcement are doing test transaction. And PayPal has been a great sponsor and we have sponsored a fair number of best practice. And we have a webinar around merchant best practices for the banking industry.

Next slide. And here I won't go in to the details. I won't read them out. Several best practice papers that we put together targeting the banks, industry and technology side and also various trends in online crime and migration hosting and these are all resources that are available on our website. So they are all in the public domain.

You can go to the next slide. And, you know, we are all very aware of the challenges here in terms of issue awareness, varying and differentiated policy frameworks and leading frameworks in different countries. Cybercrimes and national, how do we -- certainly undermines the national laws. Legislating and policing globally the cyberspace challenge and all countries are working on that. And new emerging technologies are forever challenging us. You have to keep ahead of how the technologies are being misused. And I leave, you know -- I finish my presentation and leave you with a thought on the next slide in terms of how crucial it is to have cross-sector partnerships. Once again I quote out of the NODC report in 2010 and it is to deal with these markets creative solutions and drawing on techniques not necessarily found in the law enforcement toolkit. I think we will agree in the room here that law enforcement can't prosecute their way out of this. All other players and NGOs have a role to play.

>> MARIE-LAURE LEMINEUR: Thank you. Our last speaker will make a brief presentation and then we can open the floor and apologies for leaving you last and with such amount -- short amount of time.

>> ANKHI DAS: No, I will be very efficient with timing. I do

not have a presentation. Consistent with the philosophy of my platform I will be concise like our Facebook posts are concise and run through some core values and spark discussion here. I want to thank the room and everyone who is here and wanting to engage and we want to make sure that we return some time so that there is interactivity in terms of discussions in the room to allow other people a voice in the discussion. I want to reflect on the values which we have as a company. A few things which, of course, I wanted to share, we just announced quarterly results I think yesterday last -- last night local time, early morning today in the U.S., and Facebook as a platform has crossed 1.7 billion monthly active users which is a great number. And also to reflect in terms of the robustness of our community and the way the community acts as a watchdog in terms of flagging content which comprises safety or creates concerns around safety, something which we value as a core value of the platform a lot.

I want to reflect on some fundamental five point principles which we have. First of all is community standards where we have very clearly laid out what is okay to share on Facebook and what is not. And there is no place for pornography material on Facebook. We do not permit it. We do not allow it. And the second principle is that we have very robust tools on our platform. There is a reporting button on every piece of content to flag content which is harmful and which is a violation of our community standards. These are reviewed 24/7 by different teams which are there in Facebook which have language capabilities because the local language capability is a very essential requirement of the global Internet. And these then get actioned upon for violations. We have a very effective and robust help center with resources which puts information at the hands and fingertips of users to keep themselves safe, control their privacy settings and also make sure that they have adequate information in terms of reporting of any content.

Fourth is the element of partnerships. We are very big in terms of partnering with local NGOs as well as global NGOs to make sure that we are taking feedback in terms of improving our processes, in terms of improving our enforcement and collaborating with them on safety, education and enforcement.

We have as Celeste had talked about we have implemented photo DNA for years now. There is zero tolerance for our CEI, child exploitive imagery on the platform. We work very closely with agencies like NICMEC, Reprotect, the child exploitation online center as well as Interpol and the International Watch Foundation to make sure there is active collaboration in terms of enforcing against such type of content online. With that Marie, I know you want to spark a discussion and a conversation in this room and take input. So I will hand this back to you and then we can see how it goes.

>> MARIE-LAURE LEMINEUR: Very interesting points you raised.

And I for one would like to ask you many questions but I won't be selfish. Please I would like to open the floor and hear your views, comments, criticism, whatever, feel free to intervene and share with us your thoughts.

So who wants to start? For recording we need it.

>> Thank you. My name is Kia from NGO in Malaysia. I have got two questions. One is for Claire. So in your presentation you mentioned about one of the ways to combat child sexual abuse material is to control content which has been broadcasted or posted that may result in child sexual abuse. So could you give me an example of those content that may result in child sexual abuse? That's my first question.

My second question is in many countries in Asia sex is still considered as taboo. So sex education is not even in some school curriculum. How do we engage children in sexual education meaningfully in these countries and not falling in to the trap of adopting a maternalistic approach? Leaders are not part of the discussion because often it is the religious leaders that are like obstructing sex education. Should they be invited in to the discussions? So Claire.

>> CHEN SHIHYING: Okay. I will try my best to answer your question. The content we defined, the child sexual abuse content, basically we follow the INHOPE express point protocol. Including child sexual content it is a real sexual assaultant. You can see victim, girl or boy, they are being sexually assaulted by anything, by human or men or woman or like animal or any objective. So...

>> (Off microphone).

>> MARIE-LAURE LEMINEUR: Maybe it is a language issue. The legal framework criminalizes sexual, images of sexual abuse. I think you are asking images may be, it means in English not necessarily. So maybe it is a translation issue. Is it? Or is it --

>> CHEN SHIHYING: So I can ask my colleague to help me a little bit. (Speaking in a non-English language).

So I can clarify.

>> (Off microphone).

>> CHEN SHIHYING: Okay. As a total depend on the situation that just happen -- really happen because sometimes we think it is a content but maybe in another course, in the United States maybe they think it is not. If like the -- especially when the victim -- the image, the victim in the image they are young, they are a teenager. They may think maybe they are adult. They were thinking adult pornography and not child sexual abuse content. But in this situation we can understand it is a gray area. But if we can certainly confirm, this victim when she or he be filmed, he or she is just in high school and we have official document, we can ask them yeah, we can prove this victim is under 18. So they will help to remove and these were confirmed the child sexual abuse content. So as like the Google. So

if we have a good example, because several years ago they have senior -- a senior high school girl, teenager he -- she took her nude picture to send to her boyfriend and it upload, display on the Internet. So even though the class is go to the -- saying to the prosecutor and the case is closed but right now we can see the picture still on the Internet. And everyone if you type a certain type, certain word you can find a list, URLs of her -- of the content of her nude pictures. So ask Google to remove all the list and we clarify every URL we find we thought and we present then the official document. So right now if you type the content, type the word you cannot find this URL. So this is a gray area.

>> MARIE-LAURE LEMINEUR: It clarifies your question. Very quickly if I may answer the other two because actually our organisation is addressing work with the religious leaders. Those days we are going about to publish two guidelines for action for religious leaders. We produce them with a special list with multi-faith based organisations. So we try to look at the -- to produce material to raise awareness among those communities so that the religious leaders could use it with their own community members. And that's a very valid point you can raise. They can have a lot of impact because we know that this is kind of a struggle to touch upon those issues within those communities. And sex education at least my take would be that we are speaking here of images of children being sexually abused. The sex education would be about teaching them if they are a victim of sexual abuse, how to react and what would be the recommended like talk to adult, like the basic recommendations. If someone touches you, you do this or you do that. But this is kind of a tricky thing because you have to address this in a way it is a very delicate matter and we know that most of the images there are studies showing that family members are the ones doing that actually more than strangers. It is sexual abuse within the family. It is a very complex issue to address. Another question from the floor? You are next and then you come through. Thank you. Do you have a mic over there?

>> Hello. I'm Shupa from Nepal. My question could be on different levels. So the first thing because I'm not from technical background that's why this question might sound odd to technical people. You were mentioning about the photo DNA cloud service. How do you detect certain photos are around sexual abuse? Because, for example, it is not about activity. Abuse is never about what is being done. For example, if I am kissing her in the photo it is just I'm kissing her. But it could be abuse for her for -- from a lens of victim and lens of perpetrator. How do you verify that?

Second is again if there is a guideline of certain things, I am sure, do you have a guideline of these are the things that's called sexual abuse but those guidelines are made with people like us, with our own values and perception? That will be high adjust or wherever they are from. So how do you balance that? It is kind of tricky for

me at least.

>> CELESTE YANG: Yes. You correctly pronounced my name. Yes. Thank you for the questions. I think actually Claire can weigh in on this because I'm not a technical person either. But so our technology should be neutral. We don't make the judgments on what kind of pictures are considered illegal. Right? However we give this power to organisations like ECPAT or police officers. And if they think these are the pictures that should be considered illegal they will give it to ECPAT or other organisations and they will digitize and make it in to a hash, a number.

>> CHEN SHIHYING: Microsoft donates technology to ICMEC. In U.S. court they define if anyone over any company when they follow child sexual abuse content they should report to ICMEC so they have a huge database to collect all the information. And when they confirmed this content the victim inside was children they have a project called project victim identification project. So they will have a different file for a victim. They will collect everyone. So like they use photo DNA in to this system. They should be the worst content. The children is under 14 and the content is really sexual abuse. They were put in to database. So it just makes sure every list standard is showed for every country because every country maybe have a different law. Maybe in Japan they are not so strict. So they just want to make sure this standard is suitable for every country. So yeah. Thank you.

>> MARIE-LAURE LEMINEUR: Yes. Basically the answer to your question is that each -- in each country there is a law. And then in theory when the law is well done there is a definition of what constitutes child pornography. So law enforcement against those legal parameters define whether under their own domestic legislation the picture qualifies as child porn or not. You are raising an issue that is very interesting because depending on cultural, you know, perspectives, social factors also intervene in the way you see the pictures, but here we are not speaking of that. We are speaking of images that are based on the law or legal or illegal.

>> (Off microphone).

>> MARIE-LAURE LEMINEUR: Yeah. It is. And then we consider it -- there is a legal gap. Then, you know, policymakers and law makers in your own country should amend the legislation so that they address the gap. ICMEC part of the model law legislation is to point out the countries and yes --

>> I think the point you raise about normative values is a very correct one. But to add to what Marie says, different national -- there are two ways in which this happens. There is local Civil Society, local community which would be routinely flagging these kind of behaviors which they are seeing on the Internet. So that clears community engagement in terms of police action. That's No. 1.

No. 2 is that there is momentum in different countries. Now in the South Asia region and border also to enact national legislations. In India there is what is known as prevention of sexual offenses against children. And there are very clear sort of detailing out there which sort of incorporates the normative values which are there in the country which has the recognition of the kind of behaviors that you talk about. So that the police has a cause of action to go and sort of issue notices or sort of get to that kind of wrongful behavior. So I think it is a combination of both community action as well as national legislation making.

>> MARIE-LAURE LEMINEUR: Please.

>> This is more from ISOC. At the outset I would like to I mean comment on all the work which you and your respective organisations are doing in addressing this issue. My question is actually for Celeste and David. I'm hoping I pronounce your name correctly. My question is a little technical. I am a technologist. I am not sure if you will be able to answer but hopefully you can try.

>> CELESTE YANG: Yes, I can try and if I can't I'll bring the question back.

>> Yeah. My question is about the photo DNA technology which you talked about. And you referred to that you are helping the big large scale enterprises in kind of addressing this issue within their environment. So I'm -- I'm -- I'm asking is it only related to the Azure environment or I mean is it also applicable to the -- I mean offsite computing environment which Microsoft has? Because I mean still while we have Azure subscription but we are using the computing resources more offline. So data has been stored offline. In my previous employer while I was working we used to do a lot of assessment for different clients, and we have come across a lot of pornographic material which included child I mean -- these materials but there was no proper mechanism which we can probably address and get that rectified. How is Microsoft tackling the offline computing resources issue? So that's what my question was.

And to David my question was about the Top-Level Domains. You talked about the DotKids, if we have a Top-Level Domain which is kind of segregated from the Internet, who will control that TLD and what will the framework under which we will be permitting any online content in that TLD? And I mean who will be deciding which content goes on that TLD and what doesn't go? Is there any framework already in place? Is there any directions towards that.

>> MARIE-LAURE LEMINEUR: Two minutes before we are really over time. Sorry.

>> CELESTE YANG: I will quickly answer. So for the --

>> MARIE-LAURE LEMINEUR: And then another question.

>> (Off microphone).

>> If you can also briefly explain how the Azure system works because I came from a nontechnical background. And also my question

is yeah, this photo DNA when it goes beyond the Azure platform because a lot of the child sexual image share through other platform as well, especially if it is encrypted, do you have a way to decrypt and look at what's inside and dot web, it is a common platform which is used to share images. And does this work on video? Because -- yeah, which is another -- yeah.

>> MARIE-LAURE LEMINEUR: Thank you. So one minute and one minute.

>> CELESTE YANG: Okay. Thank you. So basically the solution we provide is online. It is a cloud solution. So Asia Azure is a cloud solution. Has to be online. And for offline usually we have to work individually with different companies. And then that will be more troublesome I would have to say. That's why we encourage customers to go to the online solution and that's implemented already in our -- so Asia is a product of Microsoft. So the photo DNA technology is already built in the Asia platform. So if the customer that use Azure Asia, use the Windows different kind of products on Azure then they can also have this opportunity to use this technology already. Yeah. But, you know, that's the best I can do for now.

>> MARIE-LAURE LEMINEUR: Thank you.

>> BINDU SHARMA: Can I chime in here?

>> MARIE-LAURE LEMINEUR: Yes. David is going to answer and then we can --

>> BINDU SHARMA: This is Bindu.

>> MARIE-LAURE LEMINEUR: Let David answer and then maybe you can wrap up.

>> NG KI CHUN: Yes. For my short answer yes, there is someone who is doing recreation, but the question is who is taking the action. ICANN decides on content with those applicants for the domain names. Because for the applicants for domain names they have the registry and they have taken the responsibility to take policies or safeguard for domain names. For example, maybe it is one of the ideas of how the domain names related to -- should be on. That's why the responsibility will come to the applicants of the domain names and the one who ICANN, ICANN, the operators of the Internet on the domain names and also IP. So I will see in this way. So yes. Someone should take responsibility on.

>> MARIE-LAURE LEMINEUR: Thank you. Bindu, do you want to say something because we are almost -- we need to wrap up.

>> BINDU SHARMA: Yes, I want to add two comments on the photo DNA and project VIC site because I know we have been working closely on. Photo DNA I am sure that Celeste will have a good idea. The photo DNA hash database that NICMEC hosts, so they -- what NICMEC has done they have hash values of what they call the worst of the worst images. What the lady of Nepal asked it could be really subjective. What the photo DNA is flagging it is known child abuse images. If you or I upload an image with that photo DNA hashtag and it is in the NICMEC

database that is confirmed illegal content. So there is no gray area there. That was one comment.

And on the project VIC site what project VIC does it is a database of videos. So if law enforcement and increasingly we hear from law enforcement saying and I think it is ECPAT Taiwan who made the point that when we say we have only got a 100 or 200 reports, each report has thousands of images. So the same thing when police apprehend huge databases or hard drives from the offenders what project VIC does it is a software that can run an entire hard drive and flag videos or images that have already been viewed by law enforcement and match up those. So those are already in some law enforcement database and they don't have to relook at those to confirm it.

>> MARIE-LAURE LEMINEUR: Excellent.

>> BINDU SHARMA: Considerably reduces the effort that law enforcement needs to put in and they can focus their efforts on new images that may not be tagged and flagged or have a DNA hash.

>> MARIE-LAURE LEMINEUR: Thank you. Those are very key points. And unfortunately we don't have more time to discuss it. But they are very key points and further to be discussed maybe IGF next year.

(Laughter).

>> MARIE-LAURE LEMINEUR: So we will have part II of the session next year. Thank you very much for attending this session. I hope it was interesting enough. It has been a pleasure being with you. And I can speak on behalf of all the speakers the questions were very interesting. Thank you to the speakers for accepting an invitation. And that would be it for the moment and have a good afternoon. Thank you very much.

(Applause.)

>> BINDU SHARMA: Thank you all.

>> MARIE-LAURE LEMINEUR: Thank you, Bindu.

>> BINDU SHARMA: You are very welcome. Bye David.

(Session concluded at 1546 p.m.)

***

***