ICANN68 | Virtual Policy Forum – GAC: DNS Abuse Mitigation (with PSWG) (2/2)
Tuesday, June 23, 2020 – 16:30 to 17:30 MYT

GULTEN TEPE: May I ask our technical team to start the recording, please? Good morning, good afternoon and good evening everyone. This is Gultan Tepe from ICANN GAC support and I'm the remote participation manager of this session. Welcome to the ICANN68 virtual meeting with the GAC DNS abuse mitigation with Public Safety Working Group on Tuesday, 23rd of June at 8:30UTC. Due to unfortunate Zoom bombing incidents which happened on the first day of the meeting ICANN68 is sessions will be switching to webinar Zoom rooms and not regular ones for the remainder of the meeting. In a Zoom webinar in order for a GAC member to speak you need to be identified as a panelist. In order for Zoom to do this automatically GAC members need to either log in the Zoom room with their GAC mailing list e-mail address, or join the Zoom room with an individual link sent to them via e-mail from ICANN RP. Therefore, please check your inboxes and refer to the e-mail already shared with you by ICANN RP with the title panelists for ICANN68 GAC sessions. Please attend the GAC sessions via the click here to join tab to enter the Zoom on room as a panelist directly. Julia Charvolen is displaying to e-mail on the screen. You all received by now. In case a GAC member does not have the ability to raise hand or see the names of other panelists, he or she may need to leave the room and join again using this individual link sent via e-mail. When recognized as a panelist in the Zoom room GAC members will experience much of the information and functionality they have seen in a regular Zoom room with the ability to rename themselves for attendance records by entering their name surname country or delegation. If you have used a different e-mail address, you will not be promoted and be able to speak. If you would like to ask a question or make a comment, please type it in the Q and A pod starting and ending your sentence with question, or comment to allow all participants to see your request. And please keep them short if possible. Interpretation for GAC sessions which will include all 6 U.N. languages and Portuguese, and will be conducted using both Zoom and the remote simultaneous interpretation platform operated by Congress Rental Network. Attendees are encouraged to download the application following instructions in the Zoom chat, or from the meeting details document available on GAC agenda website page. Your microphone will be muted for the duration of the session unless you get into the queue to speak. If you wish to speak, please raise your hand in the Zoom room, when called upon by the session lead you will be given permission to unmute your microphone. Kindly unmute your microphone at this time and take the floor. When speaking make sure to mute all your other devices, including the Kang rental network application. State your name for the record, and the language you will speak if speaking a language other than English. Please also speak clearly at a reasonable pace to allow for accurate interpretation. This session includes realtime transcription, to read the realtime transcription click on closed caption button on the Zoom tool bar. Finally this session like all other ICANN activities is governed by the ICANN expected standards of behavior. You will find the link in your chat for your reference. Er with that I will leave the floor to the GAC chair, chair, Manal Ismail.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Gulten, and hello everyone and welcome back. I hope you have enjoyed your break. This is our second session on DNS abuse, we had already one yesterday and this is the second and last one on DNS abuse mitigation discussion scheduled also for an hour, and the section will be led by the PSWG co-chairs and colleagues, to also recap after the cross-community plenary of yesterday, so with that allow me to hand over to Laureen KAPIN and Chris. And Cathrin are you going to start, I'm judging by the slide.

CATHRIN BAUER-BULST: Thank you, Manal. Thank you and thanks to all of you for joining. I see we already have 190 participants so it's a topic that continues to motivate people. My name is Cathrin Bauer-Bulst and I'm with the European Commission I'm one of the 2 co-chairs of the GAC Public Safety Working Group, and as Manal has announced it will be Laureen and Chris leading the session with me today. And let me start by briefly walking you through the agenda. So first of all as Manal just mentioned we want to briefly follow up on yesterday's very successful cross-community session on DNS abuse, share some selective highlights with you for further discussion, then we want to continue from Monday's discussion to share a little bit more on the DNS abuse experience during COVID-19, and one of the points we would then like to turn to is the possible response to DNS abuse during COVID-19 but also to DNS abuse more generally, and also share a little bit of information about existing government's contributions to educating consumers and to making sure that authorities are also in the position to play their role in the overall ecosystem in preventing and combating DNS abuse. And then we would like to leave as much time as possible for a discussion with the GAC. There are already some very pertinent questions yesterday and we are hoping for a little bit more time to go into this because there are a number of points where the GAC needs to deliberate on the next steps it wants to undertake and then finally we will have our usual public service announcement on further relevant ICANN68 sessions on DNS abuse. Next slide please. So yesterday we had a great cross-community session on DNS abuse, which was split into 2 separate parts. The first part were -- was dedicated to the developments since the ICANN66 meeting in Montreal. The last physical meeting we had and, of course, to the experience during the COVID-19 crisis, and the second part was dedicated to possible next steps for the ICANN community in addressing the phenomenon of DNS abuse. I'm going to share some selective highlights and thoughts on this, and then turn over the floor to Christopher Lewis-Evans who will also share his feedback on this session. So first of all we heard a lot of very helpful information from the contracted parties who reported on their work on agreeing on a definition of DNS abuse to create a base-line for further efforts. We already had a chance to preview this yesterday, so the definition is basically encompassing mall bare botnets, phishing, farming and SPAM where it is related to malware delivery so that's a base-line definition that could be used as a starting point for further discussions, which is already helpful because as we know there are a lot of definitions of DNS abuse floating around, and knowing that the contracted parties have now agreed on one is a very helpful, is a very helpful starting point. The registries and registrars also reported on their efforts to mitigate DNS abuse in particular the registrars DNS abuse best practices, and there was guidance on the specific efforts undertaken to mitigate COVID-19 related abuse that was provided by a group of registrars that have formed to more effect IFL combat DNS abuse. Another positive development. Let me just preview the DNS abuse best practices were turned into a forum for law enforcement and we will get into that. We heard from the commercial stakeholder group and from ALAC about their experience of COVID-19 related abuse, which was quite striking amongst other things, there were -- there was a statistic cited that COVID-related domains are 50% more likely to be abusive than normal registered domains and mason coal from the commercial stakeholder group highlighted the issue of abusers riding on the shirt tails of events be it natural disasters, civil unrest and now COVID-19. There is a pervasive phenomenon of any situation of civil unrest or natural disasters being exploited to further increase the harm to citizens, which is quite disturbing. And then Laureen shared some of the Federal Trade Commission's experience, which Chris will speak to in a minute so I will skip over that here. And turn to the possible next steps for the ICANN community that was also a very interesting session. One of the main highlights that everyone shared was that there was a need more more reliable data. The registrar highlighted now there was a definition there was a possibility to collect data, and Jeff BESER from ASAC raised the issue of the evidentiary standards at what point is there sufficient data at what point is the abuse sufficiently documented to support action by the contracted parties? Another issue that was flagged was the need to build relationships so both the registries and the registrars shared their experience with authorities during the crisis, which they largely viewed as positive, and Van Ross shared the importance of good co-operation with the authorities when it came to the ccTLD space. Everyone highlighted the need to identify and share best practices information and there were a number of efforts already under way to share such best practice including by ICANN itself which is launching a system to try and collect and disseminate best practice for registries and registrars. A lot of people highlighted the fact that we are not starting from 0 like PIR, Brian ... referred to a lot of good work that had already been done over the last 5 years including on the security framework and Peter highlighted the successful approach that the ccTLD employed in terms of checking upon registration and making sure that data is accurate and verified upon registration, which had proven helpful in combating abuse. And the SSAC shared that they had created a new working group on abuse dedicated to identifying best practice and providing more guidance. One of the challenges that was highlighted by a lot of people was the need for sound rules implementable and enforcement and I took particular note of the statement by ICANN that the abuse rules as they stand have proven very difficult to enforce, which of course is not good news and something that we as the GAC have to look into. And there were also there was a heated discussion going on in the comments with some,

some commenters arguing that it was not worth even investing in rules as bad actors would be able to ignore these and the worst thing that could ever happen to them was that they would just be kicked out of the ICANN ecosystem possibly lose accreditation as registrars which we know is very challenging to get to in the first place -- and then continue doing their evil deeds as resellers, and, of course, that is something that is also of great concern to the GAC that at the moment it seems to be quite easy to remove your self from all consequence by removing yourself from the ICANN ecosystem and that is something that is worth looking into further. There were some great new initiatives such as the PIR new system of incentives for registrars -- excuse my typo on the slide here -- it's for registrars of course that they have created performance quality index and Michaela is sharing that in the chat does -- so please read registrars for registries here -- and also the two new project that is ICANN itself has set out a targeted threat intelligence system, and I'm being told I'm speaking too quickly for the interpreters. My apologies. ICANN created targeted threat intelligence system to monitor threats coming from COVID-related domains, that's I understood could also be used more widely in the future, and then I come back to the new efforts to collect and disseminate best practice that's I already mentioned earlier that ICANN OCTO is also setting out and again one of the key issues here was flagged by David Conrad very clearly unless the obligations are clearly written and understood they will be unenforceable so in terms of thoughts on this it was wonderful to see all these new efforts which are very promising and to see that there was movement going on and off abuse mitigation, at the same time we of course should not forget we have already identified as good solutions in the past. Such as verifying data registration data that is, the ASDAG studied in 2017 had already showed the link between this and abuse, and 4 consecutive review teams identified this as a priority. The WHOIS one the CCT the... and the SSR review team in its draft report and nonetheless it's still not happening. I also wanted to just come back to one statistic that Gabriel already shared yesterday that 65% of abusive registrations were hidden behind privacy proxy services. And also my personal experience from registering domains recently is that it's, in fact, difficult to opt out of privacy proxy services which are very actively flagged and promoted. And here we still don't have the policy in place despite it now becoming clear that EPDP will not address this issue. So that is creating challenges for investigations because it takes weeks and extra judicial proceeding to get to the data behind the privacy proxy which very much delays any action that can be taken on this. So we should welcome the new idea, but as Brian symbolic already said a lot of work has already happened and that should not be dropped. Rather we should include that and build on it going forward. Now we will have a chance to discuss this in a minute and now I would like to turn over the floor to Chris for his thoughts on the cross-community session before we go to some more information about the DNS abuse experience.

MANAL ISMAIL, GAC CHAIR: Cathrin, and Laureen and Chris, I'm sorry to interrupt, just to ask how would you like to take questions? Would this be at the end of the presentation? I can see a question in the Q and A pod, but I'm sure -- I am a not sure whether.

SPEAKER: If I may suggest.

MANAL ISMAIL, GAC CHAIR: Wait okay.

CATHRIN BAUER-BULST: And take the questions during the discussion.

MANAL ISMAIL, GAC CHAIR: Fair enough. Just checking. Thank you.

CHRISTOPHER LEWIS-EVANS: Thank you. And with that I think I'll take over and go to the next slides please. And it's Christopher Lewis-Evans for the report from the U.K. national crime agency. So what I'd laboring like to go is just go over some of the highlights from the cross-community session and really flag the impacts on the public and consumers and users of the DNS system. And some of the sort of scare little things we are seeing from a public service sort of protection perspective. So, Laureen shared in the cross-community session a series of really good slides and I think if you haven't seen it I would recommend going back and looking through all of those, but one of the things I would probably caveat this with at the start is you know in the vast number of countries around the world cybercrime is one of the most under reported crimes in general that we have. So during COVID-19 we've obviously seen a large number of statistics, and some of these are quite hard to draw upon, you know, comparisons against previous years because of the possible under reporting and also obviously the effects of the pandemic. So the first slide here really does show you know, date period from the beginning of January pretty much to the current date, collection of complaints received into the FTC and as you can see from the graph in the top right-hand corner, you know towards the middle of March once the pandemic started to hit, the number of complaints certainly rose significantly and a massive up-tick in complaints coming into the FTC. Majority of these reports were around on-line shopping so very very relevant, and then probably the next 6 -- and as you can imagine the around sort of vaccination and travel requirements and then use sort of a number of fraud types, so from this one I think really the take away for me is just the amount of reporting that happened, and obviously we're not clear yet on whether this is people just starting to actually report some cybercrime whereas they maybe wouldn't have before because there was a lot of effort across all the government bodies to really flag how to report issues that the people were seeing, and you know there was a lot of education which we will come onto later around you know, what bad looks like in the sort of DNS space and how to report it. See if we can go to the next slide please. So one of the things that I think was mentioned in the cross-community session and in a number of pre ICANN68 webinars was the fact that the sort of COVID-19 domain space that were registered during this time, although was a very large scale, a very small proportion of this was seen to be abusive. However, I think there's -- the slide before and this slide will show you know there still is a lot of impact and a lot of harm being cause today people by DNS abuse during this time, so it really shows that this is you know, as the community I think identified in sort of ICANN66 and 67 and before you know sort of DNS abuse is really an issue that needs to be -- have some solutions applied to it to stop some of this harm. So the numbers or the items circled in the top half of the slide are the sort of methods utilized around some of the complaint data, and you see the sort of second and third item in relation to the number of contact methods both relate to DNS, so whether it's a website related or email related. But I think what's significant around that is although they are second and third, they are almost exactly the same in value, but you know far outweighing the other sort of contact methods in the actual sort of monetary loss. And from the U.K. side, we've obviously been collecting numbers and I think since the 23rd of March we have a total of over 16 million of fraud caused by sort of on-line shopping and I think one of the interesting stats around that is nearly 1/4 of the victims were in the age of 18 to 26. And normally when you're you know, describing sort of on-line shopping type problems you generally assume it's people that aren't used to the technology, and probably you know the smallest age range you would put is 18 to 26 so that's interesting thing and you know certainly highlights the need for continued education across all age ranges. And so obviously that 16 million is just fraud to on-line shopping so has nothing necessarily to do with COVID-19 or obviously some of them will have been. But focussing on COVID-19 there was over 2000 victims that reported losses due to COVID related scams, and those losses for the U.K. this is obviously up to the 12th of June stands at over 7 million. So I think for me what this really highlights is that whilst you know the abuse during COVID-19 might not have been focussed on the actual COVID domains or around you know, vaccine and everything like that DNS abuse was still going on and the actual impact to the public is really high, and obviously during the pandemic that harm is felt even more. So I think it really is for us to look at ways that we can improve the situation and reduce the amount of DNS abuse and the harm being caused by that. With that I think I would like to turn back over to I think it's Laureen next, and go over some of the ways that we can actually effect some change for the better.

LAUREEN KAPIN: Thanks, Chris. Can we go to the next slide? So I wanted to I wanted to emphasize that in dealing with DNS abuse there is certainly things we can do within the ICANN universe particularly in making sure that there are strong obligations to prevent these malicious activities from exploiting the DNS. We can engage in co-operation as governments, with the private parties like our registrars and registries to co-operate when bad conduct is identified, but another very vital tool is consumer education, and certainly in our role as governments there's a huge role to be played in educating the public so that the public themselves, the end users, the folks who use the Internet as a way to conduct transactions and communicate with one another, and increasingly during the pandemic this is something that is becoming a vital tool for communication, so we, as governments can try and cut DNS abuse off at the possible so to speak by educating the public on how they themselves can protect themselves against these malicious activities. So I wanted to share with you a little bit to give you an little taste, the least what the United States government is engaging in terms of consumer education and more specifically -- because there are many agencies in the U.S. that perform this vital mission but more specifically what my agency the Federal Trade Commission which is the leading consumer protection agency in the U.S. does -- so in terms of coronavirus materials, which of course are very topical issues these days, and scams that seek to exploit the public's interest and concerns about this issue, the FTC has a dedicated part of its website that is particularly focussed on the coronavirus issues, and you can find it yourselves at FTC.GOV/coronavirus and you will see many different tabs that you can go to in terms of what you might be interested in and you'll see the very first tab is for consumers, and when we think of the FTC we think for the consumer. The second tab is focussed on businesses and businesses too need guidance in this area about how they can protect themselves from scams and also how they can deal honestly with the public and if you're interested about what the FTC is doing in terms of enforcement, there's a tab for that too and I will point out that the FTC has been quite active in sending out warning letters to companies particularly companies that are advertising via the Internet in terms of making claims that aren't supported.

Particularly claims about products that purport to be able to effectively cure COVID-19 or protect you from the virus. There's resources and I am I will talk about those in a moment and also importantly the slide that Chris showed you about complaints, those relate to the FTC's efforts to gather complaints from the consumers all around the world, and in our website, if you just go to our regular landing page FTC.GOV one the first things you see is how you can report a scam. So next slide please. So these are some resources that are available on our coronavirus -- on Mike site, how do to avoid scams and that's available as a visual, and there are also many videos which we will see a slide about in a moment, the financial impact of the coronavirus, because we know that many people are no longer able to do their jobs and get a pay check, and also this is all public information. And not only is it available for informational purposes, but if you are a government or an agency or any organization that is interested in using this material, we also make it easy for you to use this material and put your own logo on it. So we don't have proprietary interest in saying we are the only one that is can use this material. What we actually want to do is share it on pass it on. Next slide please? So this is just focussing in on one of our consumer education materials. Keep calm and avoid coronavirus scams, and we break the message down into 5 very easy to understand messages about ignoring offers for vaccinations and home test kits because there is no effective vaccination and there are no home testing kits. Hanging up on robo calls because that's a common method for scammers and along with e-mail and along with websites so watch out for phishing e-mails and text messages from people you don't know. Also bogus charities popped up trying to part people from funds they would like to donate to real organizations as opposed to fake ones. Next slide please. And then for folks who prefer to get their messages via video, we also have videos prepared, so you see we try and cover the bases in terms of how we can communicate these messages and how the public can protect themselves. And I will pass the baton, but also urge any one who's interested in to topic visit the FTC.website and pass this useful information onto whoever you think might benefit from it, which I hope is everyone.

CATHRIN BAUER-BULST: Thank you, Laureen. This is Cathrin taking over again just to flag that similar efforts are going on in in the European Union and all of the member states. And we just wanted to share the Europe example here and with you of the many good examples of what authorities are doing to support consumers and businesses in protecting themselves. So you see at the bottom of the slide the link to the Europol sites which selects information both for consumers but also for law enforcement and policy makers and governments. So Europol during the COVID crisis undertook 2 work streams to support consumers and businesses but also policy makers and law enforcement in dealing with this crisis so on the first work treatment Europol prepared a series of reports on the impact that the pandemic had on crime. Of course that he was not just limited to DNS abuse, rather it covered all forms of crime, we've seen significant developments also in other areas such as the fight against child sexual abuse. Domestic violence or organized crime and

and outflow those Europol prepared reports for general public consumption that provided a basic level of information for law enforcement containing data that is important for operational purposes and strategic ... for the member states and other partners. And finally for policy makers and governments to inform them on the strategic consideration that is governments need to be aware of when making choices about how to deal with this crisis. In a second WorkStream Europol prepared educational materials for the public and for businesses, and our basic consideration there is the commission in asking them to do so was that Europol like the FTC has a reputation for reliable and honest information and one of the challenges that we saw was most pronounced during this crisis was that a whole host of authorities, or purported authorities sprung up with their own sources of information or disinformation, which made it extremely challenging for the average person to find reliable information, so we thought it was even more important to use existing recognized trusted platforms to share reliable information for everyone. So, Europol made available these materials and if we go to the next slide, I won't go into all the details here. The slide is quite similar to that of the FTC just to highlight a number of the topics that are more relevant to this audience where Europol provided easy to understand information with attractive graphics to try and inform the consumers, and a lot of that was also made available in several languages as you know in the European Union we have 22 official languages, and, of course, it should be available for everyone. If we go to the next slide I want to just briefly mention another WorkStream that Europol engaged with together with the commission, I had mentioned earlier that Europol -- that the registrars had made available a document describing best practices for abuse reporting, and had made available targeted information on possibility to deal with COVID related abuse more specifically, and so what we did together with Europol was we transformed this information into a form that law enforcement could use in reporting abuse to registrars to make sure that those reports to registrars contained all the necessary information for registrars to take action. And that is something that is on going, we also had some very helpful calls with the registrar DNS abuse group to discuss how co-operation can be facilitated not just during this crisis, but also more generally going forward on DNS abuse, because the points that were highlighted in the cross-community session on bidding relationships and increasing the quality of requests are of course also shared by law enforcement and one of the things that we are looking into also is the creation of single points of contact to basically centralize expertise also on the law enforcement side and make sure that there are competent partners dealing with the private sector not just with the DNS industry but particularly also with them where the contracted parties are the single best option for the way forward. So, this was our effort to explain a little bit about the whole of ecosystem approach that authorities take, so -- and to reassure you also that we don't just rely on ICANN and its community for solving the DNS abuse problem. We are committed to doing our part also in our governments and organizations to make sure that as somebody was saying in the chat people don't just walk and the street but also are aware of traffic. At the same time of course we need to make sure that there are proper traffic rules in place and that brings us back to the ICANN ecosystem so maybe if we go to the next slide we can now turn to, to having some space for a discussion and deliberation and possible next steps for the GAC. Just to highlight once again a couple of the existing efforts and challenges that have come up, I've listed a couple in the -- in the next steps report from the cross-community session but also to showcase once again the tool that we think is extremely important, the domain abuse activity reporting tool, which continues to deliver information and could possibly in the future look at more granular information being made available, I also want to flag again something that came up during an ALAC session and also was shared in a letter that ICANN wrote about the enforceability of public interest... and abuse requirements more generally which is very challenging to enforce for the ICANN contractual staff. And then finally just to flag that of course this is an ongoing project for the Public Safety Working Group where we have some specific work streams under the DNS abuse mitigation work led by Gabriel Andrews and other colleagues that will continue to work on these issues. But more specifically for today, we would invite the GAC to seize this opportunity also to discuss the GAC's next steps on a number of efforts where we also have questions for the Board, in the upcoming session tomorrow, namely on 3 issues, on the issue of privacy and proxy services data disclosure. On proactive anti-abuse measures and specifically the CCT review recommendations related to DNS abuse that's -- that's the GAC has previously held should be implemented before any subsequent round of new gTLDs is considered. And then finally on the WHOIS accuracy reporting system where the same considerations apply. And on this, I would, if I may give the floor to Laureen and Chris for any final comments before we open the floor for discussion.

LAUREEN KAPIN: This is Laureen. I would just add that this is a topic which we, which we are most effective in dealing with, with partners, and, of course,, our partners include, our colleagues in registries and registrars. Our partners include ICANN including the out standing staff they have on their security and technical staff and all the staff supporting the work of the Public Safety Working Group, and, of course, it includes all other GAC colleagues in governments around the world who have relationships with their law enforcement and consumer protection authorities. It's really only by working together that we can be at our most effective in protecting the public from all the different forms of DNS abuse, particularly those that flourish during challenging times like the ones we are in now.

CHRISTOPHER LEWIS-EVANS: Thank you, Laureen. And just for me I think I'd just like to highlight our PSWG Work Plan that's been published and is available and you know in there obviously we highlight you know DNS abuse is definitely is one of the key issues but then there's you know a number of other items that sort of touch on and around I think as we mentioned in the chat around DOH and DOT, you know there's all different aspects around the DNS and how it may be abused that we are looking at and I think yeah, for certainly for the GAC representatives attending it's worthwhile look at what items that we are looking at that really effects us and how we are getting on with those. Thank you.

CATHRIN BAUER-BULST: Thank you, Laureen, and Chris, and with that we can possibly turn to the questions unless Manal you would like to share some more general comments before we go into those?

MANAL ISMAIL, GAC CHAIR: Thank you very much Cathrin. I think we have like 15 minutes remaining, and we have Kavouss's hand up, and quite a few questions in the Q and A pod so Kavouss please go ahead.

IRAN: Hello, do you hear me.

MANAL ISMAIL, GAC CHAIR: Yes, now I hear you.

IRAN: Thank you very much.

MANAL ISMAIL, GAC CHAIR: If you can speak closer.

IRAN: Closer thanks. Cathrin as usual provide us mega bits of information in few minutes and others, and you know our brain sometimes is saturated and does not respond properly quickly but so many information. If the purpose of this 45 minutes up to now is these 3 bullets we have no problem with any of them. We have to discuss them proxy presumptive nominee surveys. Protection anti-abuse or WHOIS accuracy. We have no difficulty at all. And as less relation with coronavirus 19 and so on and so forth. Otherwise you ask Chris or others to provide the same information for the previous years to see whether the similar months we have the same thing and so on and so forth and previous events we had so many things so if the purpose of these 3 bullets you have no problem to consider them. How we could act we have to listen to the community. Thank you.

MANAL ISMAIL, GAC CHAIR: Thank you, Kavouss. Any reactions to Kavouss's comments? And again, before going to the Q and A pod I think we also have a comment from a GAC representative of India and I do apologize to those who are waiting for their questions to be answered, we normally prioritize GAC questions so allow me to take this comment first from India before going to the Q and A. PSWG should also work with ICANN consumer safeguards director to be more effectively address public interest, safeguards and DNS abuse considerations in the DNS ecosystem.

Thank you India. So now, going to the Q and A pod, and we have ten questions, or comments, and I hope I'm not an expert here, I hope I'm taking them in the right order, so I think the first question was answered by you Cathrin in the chat but let me just read it out loud ... mentioned that it was difficult to opt out of privacy proxy services in most cases WHOIS privacy is a paid service but GDPR masks of WHOIS data is not. Did she mean the data masks was difficult to opt out of or is she conflating the privacy with privacy proxy services? I believe you already answered this question Cathrin right?

CATHRIN BAUER-BULST: Yes, that is correct Manal. I see that Cristina from the Armenian GAC team would like to comment on this also if I haven't misunderstood the note in the question pod.

MANAL ISMAIL, GAC CHAIR: Yes thank you for pointing this out for me as well. So Cristina.

CRISTINA: I'm sorry, I think it's something else happened because I haven't question. I just.

MANAL ISMAIL, GAC CHAIR: Okay, never mind. We're all learning. Okay.

CATHRIN BAUER-BULST: But just for those who didn't see it in the chat I'm not conflating privacy proxy which masking of personal data pursuant to the GDPR requirements. I am, in fact, talking about -- I was, in fact, talking about a privacy proxy service that was very convincingly offered at least 3 times during the domain name registration process. And just on the comment in the chat about engaging with the ICANN consumer safeguards director, indeed we did a lot of that engagement when Brian was still around and the position still existed but as Michaela already mentioned in the chat, he has left and has not been replaced so we don't know what the plans are but we did engage whether there was a possibility and, of course, we would engage again if again there was the possibility. Thank you.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Cathrin. And we have another question, I'm not sure why is it coming from anonymous a ten de, and whether we should take this question, but it reads, ICANN addresses DNS abuse within the framework of its mission, with a slightly broadened view but that is not enough TOISM that end be it a business user or an individual user the form of abuse that hurts most is what may be defined as the abuse of the domain Web space to place misleading or malicious content for monetary gain or exploitation, or to lead to other form of harm, for example using a domain name to set up Web space to disseminate content that would mislead poor and unfortunate people to sign up for a job that may actually lead to a form of modern slavery. There are less intricate and more obvious content related harm that ICANN refuses to address, are there harmonious initiatives external separate or private outside the formal ICANN process that goes into the class of DNS abuse that the ICANN may be able to address?

CATHRIN BAUER-BULST: I can take a first stab at that Manal but I'm sure others will want to come in. Yes, I think it's excellent question, and that remind me of one of the great graphics of yesterday's cross-community session where somebody had set out the domain name ecosystem versus the consent management ecosystem into two parallel boxes on the consent management side you had website owner the host of the website and the registrant as 3 separate entities that would be approached for issues with the content of a website. Whereas on the DNS side you had the registrar, the registry, and the name serve if I remember correctly. And one of the things that struck me is that for somebody -- for a perpetrator out for a monetary gain or exploitation you will often find that the 3 entities listed on the one site of the graphic the on the host and the register start are, in fact, one single criminal entity and then there is no direct action that can be taken. Rather the registrar is your first point of entry for any swift and effective action to take action against abuse. And there indeed the question remains how we deal with abuse that is considered by the new definition of the contracted parties to be outside the ICANN ecosystem and that's where I also really appreciated the comments from the contracted parties that that was seen as a base-line definition to be further explored and one of the big opportunities that the general excitement around COVID-19 might afford us is that everybody was paying a lot of attention to their systems and we should have a lot of data to analyze assess precisely what types of abuse look place and what can be done about them and at what point so we can draw lessons how it tackle abuse within the ICANN system and potentially beyond and a more philosophical questions that begs to ask in the context is what is beyond the ICANN ecosystem? And is that left to the realm of national governments to legislate on and how would do we manage the interaction wean the necessarily national frameworks and the international ecosystem of the ICANN developed policy? That's my 2 cents toon and maybe Laureen and Chris or others want to come in on this.

MANAL ISMAIL, GAC CHAIR: Thank you very much Cathrin. If there are no additions from Laureen or Chris, then maybe we can take Russia I see a hand up from Russia so Russia please.

RUSSIA: Do you hear me? We discuss a lot COVID issue but we should remember other as well and my question related to another hot issues and important issues. The... and the DNS HTTPS now with technologies promoted as improving security for DNS as during previous session for example DNS and IOT, however, DOT and DOH carries some risk for the public interest, for example child and land protection, and I would like to know if our group the... group conducted any research on these issues made some sort of risk analysis, and so on and so forth. And what does the position offer as a global DNS operator on these issues. Thank you.

MANAL ISMAIL, GAC CHAIR: Thank you very much Russia. Any comments from the presenters? Yeah, I see Chris's hand up so Chris employees go ahead.

CHRISTOPHER LEWIS-EVANS: Thank you, and thank you for the question. We've highlighted in our PSWG Work Plan that DOH and DOT definitely are issues that could cause some risks to the public safety, and that this is something that we are currently working on, you know per everyone and unfortunately, recent events have probably over taken some that have work and the other thing that we have at the moment is the sort of DOT, DOH aspects a lot of the assessments risks are still within sort of IATF and a little bit outside of the PSW remit so we do have a plan to look at those, and that is certainly something that we will be focussing on during this next year. And as Fabian has helpfully shared in the chat there, there's also an impact assessment risk around DOH and DOT as carried out by ICANN. So I think that's certainly a piece of work that we are going to be utilizing to support the PSWG's work going forward. Thank you.

MANAL ISMAIL, GAC CHAIR: Thank you, Chris. Following is a question from James Bladel. It would be helpful to present these separately so we understand what portion of those is occurring and Facebook.com or twitter or similar domain names which a registrar will never suspended for individual incidents of DNS abuse. So, let me move on if there are no immediate reactions to this. There is not a question, in the Q and A pod and I think it has to do with a technical issue so I invite those responsible to read it. Another question again from anonymous, how does abuse education help? IE to what extent this is a world with a variety of abuse, some abuse intricate, some abuse high tech, all of which are way above the ability of 80% of the world's population to comprehend and understand. Even if the resources deployed and the funding available for education is unlimited. Abuse requires some form of consultant well deliberated top down measures and technical back end DNS SSAC and measures and in other words some form of anti-abuse coding in the DNS abuse prevention may have to be built into the DNS with or without education. Why is there an emphasis on educating consumers or -- on abuse? Would that safeguard all consumers all the time against all forms of abuse?

LAUREEN KAPIN: This is Laureen, and I'm happy to respond. The we see consumer education as an important tool but certainly not the only tool, and I certainly think that more work could be done on studies to attempt to measure the impact of course it -- is somewhat challenging to actually conduct research in this area, as you would really need some control groups who were educated and those are who are not and follow them through time to see what sort of impact the education held. But we do know that knowledge is power in this area, and that if you are giving people youths useful information, particularly in an area that is dependant upon science, like COVID-19 is, that education can be a useful resource to help the public interpret what is valid, and useful, and what is not. So I think it's an important tool. I think it's something to add to our arsenal along with strong enforcement, along with robust obligations under contract and along with the voluntary co-operation that we get from the folks who are conducting business in this area, and I'll add that this co-operation has been very good, and everyone is struggling to respond to the threats that have emerged that are specific to this crisis.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Laureen, and I do apologize for the remaining questions, John Nigel, FABRISIO, and I hope I didn't miss anyone. Unfortunately, we have exceeded our time by one minute, and we need to conclude. So anything final from our presenters before we close the session? If not then this concludes our meeting today, and many thanks for everyone, the GAC leadership, as you may know will make themselves available from 1600UTC to 16:30 for GAC colleagues who were challenged by the time zone and would like to catch up on any of the sessions they missed. Tomorrow, we will start at our normal time, at 10:00 Kuala Lumpur time 200 UTC with a communique drafting session. Thanks everybody. Have a good rest of the day, and thanks to our presenters. The meeting is adjourned. Thank you.

[END OF TRANSCRIPTION]