ABU DHABI – GAC Public Safety Working Group Meeting
Tuesday, October 31, 2017 – 08:30 to 09:30 GST
ICANN60 | Abu Dhabi, United Arab Emirates

UNKNOWN SPEAKER: Good morning. ICANN60, October 31st, this is the GAC Public Safety Working Group Meeting.

CATHRIN BAUER-BULST: Good morning, everyone. My name is Cathrin Bauer-Bulst, I'm one of the cochairs of the Public Safety Working Group. I'm here with a couple other members of the group and Fabien Betremieux, from ICANN Support Staff, and I'll just let my fellow members introduce themselves, please.

LAUREEN KAPIN: I'm Laureen Kapin, from the United States Federal Trade Commission where I focus on consumer protection issues.

IRANGA KAHANGAMA: My name is Iranga Kahangama, with the US Federal Bureau of Investigation.

GREGORY MOUNIER: Good morning, everyone, my name is Gregory Mounier. I'm working for EUROPOL, the European Police Agency and it's the European Cybercrime Centre, the cyber division of EUROPOL.

CATHRIN BAUER-BULST: Thank you all, and thank you for coming out early this morning. I hope you all enjoyed the gala yesterday and glad to see that you still made it here in time. People are still trickling in, but we're going to get started. We have one hour and we have four points that we would like to discuss with you this morning. So, as you may be aware, our Co-Chair, Alice Munyua, stepped down and we need to look at identifying a new co-chair for the group in cooperation with the GAC and the GAC leadership.

We also want to take a look at the Public Safety Working Group strategy and update its work plan for the upcoming time period. Then we want to give you a brief summary of yesterday's Cross Community Session on abuse reporting. And finally, we want to spend a couple minutes on the impact of privacy laws and the GDPR, the General Data Protection Regulation of the EU, and in particular on the registry directory services and what that might mean for law enforcement.

And we're going to start with the co-chair selection criteria. So, as I was saying, Alice has stepped down and we're now looking at

identifying a new co-chair, rather looking at identifying the criteria to apply. So there was work going on within the GAC already on defining the processes for working groups of the GAC, because there is of course an advantage in having a horizontal set of rules that apply to all working groups of the GAC equally in order for the GAC to have a consistent approach to the way it works in these sum groups.

And one point on these processes for the working groups that is defined sort of in minimalist terms and needs further fleshing out is the selection and appointment of chairs, or co-chairs, or vice chairs for working groups. As you know, we had an informal meeting yesterday afternoon of this group. Not all of you in the room were present, so I want to take a minute just to update you on the thinking that went on in that meeting where we first discussed what might apply in terms of criteria.

Now, the Public Safety Working Group, we're going to get to that in a minute, has a pretty significant workload in terms of processes that it's looking at, that have an impact on public safety issues. And so what we thought to reflect in the criteria for the co-chair is a bit akin to the way the GAC has been practicing this in the past where we try to first of all reflect a bit of geographic diversity in the membership of the group, but also in the Chairmanship of the group or chairpersonship of the group.

We also thought that it was important to have a significant amount of experience, both in the area that we work in, and specifically in working with ICANN and the multistakeholder community in order to be able to lead this work in an impactful manner. We also thought it would be helpful to think of criteria for how the selection process would be operated to further complement the operating principles for a working group that the GAC is currently building.

And then we finally need to see how we can best communicate on this and liaise with the GAC on this and enable the GAC to take the final decision on these matters. And that's where we sort of left the discussion yesterday. Now there's a lot more people in the room today. So, I would be grateful for any views that any of you might wish to share on these criteria from your experience with the GAC or with other parts of this community. So I'll just wait a minute to see whether -- yes, Iran, please.

IRAN: Thank you, madam. [Inaudible], everybody. I hope that as to your question, you did lead with some views on how we replace or fill up the posts which are vacant. Is that what you're asking? If that is the case, yes, we fully agree that within the community we are discussing the diversity, [inaudible] CCWG [inaudible] in

two, one of the [inaudible] diversity groups and that was also discussed in the CCWG meeting.

But our view with respect to those, all the elements of diversity are very well welcome. But to have somebody to work within those diversity in our view, there are two important which are more to be focused. One is expertise and the other is devotion. You can meet all the criteria, but somebody may not have I will say the necessary expertise about the subject or may not have time to devote to that. When you see yourself so enthusiastically following all these things, this is a good example.

So, these are the things that we have no problem with other criteria, all of them are very well studied and relevant and so on and so forth. What I said at the meeting, I just repeated here. All of these criteria written in diversity are good, but their implementation sometimes is difficult. So, if you are successful or we are successful [inaudible] diversity criteria including the devotion and skill or vice versa skill or devotion, we would have more fruitful results. Thank you.

CATHRIN BAUER-BULST: Thank you, Kavouss, for that helpful input. Is there anybody else who want to weigh in on this criteria? I'm not seeing any hands at the moment. This is something that we will be discussing with

the GAC and the GAC leadership in the weeks to come, so we're not aiming to take a decision on any of this at this meeting. I'll send you the changes that are going on with the GAC leadership at the moment.

So we're hoping to get our criteria, our proposals for criteria circulated to the GAC after another comment period for the Public Safety Working Group to the GAC as a whole for their eventual comments and then to have them be approved possibly in one bundle with our new strategy and work plan which will be the second point on the agenda this morning. So I'll turn to that point if there's no further comments on the criteria at this point.

So, I already mentioned the significant workload of the Public Safety Working Group in its work on supporting the GAC on issues related to public safety. And one of the endeavors that we've been undertaking is to look at how, in view of our mandate, we can define our strategy as a group for the time period to come, and in a more permanent manner. And then on that basis, derive a work plan for the upcoming two-year period.

And to do that, we departed from or we're starting with what's -- on the base of the terms of reference and the interactions with the GAC we have identified as the Public Safety Working Group's responsibilities and objectives.

Now, we have identified four main responsibilities that we have as a group in supporting the GAC and its work. The first is to support the GAC's role in considering and providing advice on the activities of ICANN within the mandates of the Public Safety Working Group. The second is to identify policy issues and process opportunities in support of the operational needs of public safety agencies. The third is to participate in relevant ICANN and ICANN community processes to promote public safety policies. And the fourth responsibility is to develop the representativeness and the effectiveness of the Public Safety Working Group.

And here we get back to the issue that we just discussed on diversity and on making sure that the wide spectrum of views is represented in the Public Safety Working Group. On that basis, we identified a number of strategic goals for the next three year period to first of all develop the capabilities of ICANN and law enforcement communities to prevent and mitigate abuse involving the DNS as a key resource. And that's something we will get to in a bit more detail in a minute when we'll talk about the Cross Community Session.

We want to ensure continued accessibility and improved accuracy of domain registration information that is consistent with the applicable frameworks, including privacy laws. We want

to build stable and resilient Public Safety Working Group operations, so that's more of an internat objective. In order to do our work well, we need to be able to be resilient and effective.

And the fourth strategic goal is to increase participation and volunteering in the Public Safety Working Group work by 50%. And it's important to note that while we have a large list of members and while we have a lot of members following work on the mailing list and even attending the face to face meetings here, there's a small contingent that is doing the actual work of participating in different parts of communities processes, that is participating in drafting briefings or advice to the GAC on certain issues, that is participating in identifying where else we should be involved and we're trying to increase that contingent.

Because, as like most of you, we are also doing this alongside a normal day job and the workload is quite immense, which is I think a problem for all of the GAC and not something that the Public Safety Working Group is alone in. But that's one that we also face and we're trying to find ways of dealing with it.

Now, those responsibilities and objectives were circulated together with a bit more explanation on the mailing list a few days ago for your review before the meeting. And I just want to pause here and give you a moment to comment on this, and while you

reflect on any comments you might wish to make, let me just talk briefly about the process.

So what we're hoping to do is to basically, on this basis, draft a specific work plan that we would be sharing for review with the Public Safety Working Group list and then with the GAC as a whole, with a view to securing its endorsement by the time of the ICANN61 meeting in March of next year. So that's the process that we're trying to follow. With that in mind, would anybody like to comment on this document on the priorities, on the responsibilities, or the strategic goals? Yes please, the US.

US: Thank you very much, Cathrin. I apologize if I've just overlooked it, but I actually don't seem to have this document if it was circulated to the PSWG. But I'm just curious with respect to how it was developed and what are the expectations, it sounds like you're seeking feedback now on what's being presented.

But, I think just one thing to note in terms of increasing participation I think that's a great and wonderful idea, but just, you know, one thing to note and flag, it's not always clear when, you know, the PSWG is meeting informally or formally. I think it would be really helpful if perhaps the way the PSWG meeting is

more formalized so those who would like to participate have the opportunity to do so. Thank you.

CATHRIN BAUER-BULST: Thank you, Ashley. We circulated it on the 25th of October. We're going to recirculate it and there will be further opportunities to comment, so if people have not had time to review this, we're not closing the discussion today by any means. This is just the first step to socialize these ideas and get your first inputs for those of you who have had an opportunity to review.

And yesterday's informal meeting was on the schedule. We had to meet in parallel with the GAC and this was discussed with the GAC because it's very difficult to find time to actually do the work in the face to face meetings which sometimes means that we have to have smaller meetings in different rooms. But it was shared, and in terms of how this came about, the basic starting point is the need to have a work plan for the upcoming time period and we already have a mandate. So on the basis of that mandate, a small team of us sat down and came up with the responsibilities based on that mandate and based on the input we have received from the GAC in terms of priorities that you see for the Public Safety Working Group goals. We have tried to elaborate some strategic goals.

But just to go back to the procedure also for those of you -- because I'm sure there's others who haven't had time to review in particular in the last couple days before the meeting, it gets difficult for everyone. We will have a first discussion here but we will also continue this on the Public Safety Working Group list and on the GAC list, then once the Public Safety Working Group has had a chance to weigh in. Who else would like to comment on this document? Yes, please.

THAILAND: [Inaudible] from Thailand. I actually have a question. It seems that this covers the attack using DNS as a resourceful tool. Does it also cover the attack to the DNS infrastructures? Like the DDOS attack to DNS servers?

CATHRIN BAUER-BULST: So, in the past we've interpreted DNS abuse to be a broad term for any misuse of DNS resources. So that would include to my limited technical understanding both the attacks on the infrastructure and the attacks using the infrastructure. Yes. Am I correct in this?

IRANGA KAHANGAMA: Yeah, I would agree with that, and I think it's safe to say from the Public Safety Working Group perspective that we are always open to hearing about any other challenges or issues within the DNS space related to security that we can help tackle or clarify. If that's anything of interest or something you want to work on. Please let us know.

CATHRIN BAUER-BULST: Yes, and that of course is something that we could clarify in the strategic goals to make sure that that is clear in the document itself. Thank you for that. [AUDIO BREAK]

Okay, if there's no other comments on this, then we will proceed as described. So we're going to send around this document once more. There were some comments on it already on the list and in yesterday's meeting. So we will send around an updated version to the list of the GAC Public Safety Working Group for possible further comments, and then share it with the GAC as a whole with a view to drafting a work plan for the upcoming period on this basis, which also will be circulated and and with a view to possibly adopting this then at ICANN61.

So this being said, let's move to the third point which is the feedback on the Cross Community Session on DNS Abuse. We saw many of you there; for those of you who weren't able to

participate, we're going to give a quick debrief and I'll pass this over to Iranga.

IRANGA KAHANGAMA: Thank you, Cathrin. So we had a Cross Community Session on the reporting of DNS Abuse data for mitigation and it was well attended. I will start by thanking Mia. I know that when the prioritization list came out, a number of you listed DNS Abuse mitigation as one of the top priorities which enabled us to hold a session.

The Cross Community Session was well attended. We had panelists from throughout the community come to interpret their -- or give their perspective on DNS Abuse mitigation and the use of data. The stakeholders included representatives from the registrar community, registries, SSAC, the business constituency, NCUC and IPS, as well as and the ICANN organization, specifically the CTO's office, so we had a number of those panelists on board as experts giving their advice.

The session began with presentations by David Conrad of the ICANN CTO office where he described the DAR project, the Domian Abuse Reporting tool that he's working on with the security team, which is a tool that aggregates a number of different data feeds and block lists to identify abuse online. And

I believe there's a session later this week where that's going to be outlined a little bit more specifically, but he gave a more specific presentation on the sources of the data that's used in that reporting system and how it is used in many other or different contexts.

And so, he went into some depth to describe that, you know, the email services, the browsers, the other things that we use on a daily basis on the internet are receiving this data and using it to block malicious activity from going on. And so it made sense to start to try to use some of this data within the ICANN space. And so he highlighted the sources of data and some of the methodology behind that.

Then we went on to a second presentation from Drew Bagley who is on the CCT review team, and he described some of the policy solutions that they were recommending and just provided examples of how there is a clear gap between the existence of DNS Abuse data and the policies because not all of the issues are being addressed. So that was a nice bridge that he provided.

And then it went into a discussion of the three buckets that we used to categorize how we should be looking at DNS Abuse data. These would be the key questions that are available on the screen. So how do we identify DNS Abuse? How do we create effective and transparent reporting, and how can abuse reporting

supports registries. Again, it was these three themes of identification, reporting and then usage of DNS Abuse data.

The reason we came and posed the session the way we did is because in the run up to the event, the Public Safety Working Group tried to draw up some proposed principles that should guide the way the DNS Abuse data is used within ICANN, and we drafted up a potential document and shared it with the nine panelists in the Cross Community Session who agreed to work on this.

And we had three working calls in the run up to this ICANN meeting but it became clear after about the second one that there was a disagreement over some of those principles that relate to those three buckets that I just mentioned: identification, reporting and usage. So then we turned the Cross Community Session itself into the debate that kind of needed to be started in order to close the gap on some of the differences. And I think that was relatively successful. I think it became very clear from the session that there's a very high demand for the transparency of data that ICANN is sitting on that should be reported publicly and be made transparent from different community members.

I think it also became clear that there's a lot of common or well known bad actors in this DNS space that the data can clearly point to rather definitively while still admitting that there can be

others that are more ambiguous. But I think what became clear is that it's important to narrow the gap of the scope because if you have a very high level of more, for lack of a better term, obvious abusers, and then some more undefined activity happening, there should be a mechanism to try and look at some of those obvious abusers.

And I think what the Public Safety Working Group is going to try to work on is to kind of hone down on those principles with the Cross Community and try to find more specific criteria to close the gap between perceived DNS Abuse that exists in this space.

So the slides are, I believe, up and available if anyone needs to follow the presentations that Dave Conrad did or Drew Bagley, and then the recording does exist to get into some of the discussion. But it's something that I think we take a lot of pride in in the PSWG in shepherding through and keeping the conversation alive on how to combat DNS Abuse and how DNS Abuse data, as part of Open Data Initiative, and all the new efforts that ICANN is trying to do remains really important, so we'd like to keep putting the light on that issue, keep it alive and keep making DNS Abuse mitigation a high priority for the organization.

Happy to entertain any questions as well as any other comments from the people on the stage that may have anything to add. Thank you.

CATHRIN BAUER-BULST: Thank you very much, Iranga, and thank you very much also for all your work in making this happen, and Fabien's excellent support in doing that; that was really essential. Just to say that I also felt it was a quite successful session and that there was a high degree of consensus in terms of the identification and the transparency around the reporting of abuse. And that one sort of gap that emerged was between the kind of data that the DAR tool in particular makes available on trends, and what might be needed to get individual action from registries and registrars to actually address abuse on that basis.

And I think we heard an interesting statement also yesterday from one of the registrars who said yes they have the legal tools in place to take action based on their terms and conditions pretty much on any basis, including possibly on the basis of abuse feeds. But of course, they have a responsibility not to do this on a whim, as they said. And I think now we will need to determine what it takes to make this abuse feed data not look like they're acting on a whim.

And I think that's a gap we can probably bridge in the time to come. We will have to identify what exactly it would take to also enable specific action, but it's already I think a very big step forward if we manage to have transparency around the abuse

data for input to policy processes. Because that will enable us to have evidence based policy making on how we tackle abuse and then also to track how our policy affects that abuse because that same tool should in principle show us improvements or setbacks depending on the policy that we adopt.

And I think one aspect that was tackled in the CCT review team's analysis report on DNS Abuse, was the impact of the safeguards, the new gTLD safeguards on mitigating abuse on which the report was very short. So it wasn't able to go into the necessary depth of analysis and those are some of the issues that we would also like to bring up with the GAC for a possible follow up. So to see whether there is an opportunity for the organization to follow up with a more in depth study on how safeguards affect abuse because that's something that was actually criticized by a number of the public comments to the report to the CCT as needing further research.

And then also to see how we can come back to this idea of the principles, and see whether akin to what the GAC has already done for example with the new gTLD Whois principles in 2007 or in other areas, whether there are basic bottom lines that the GAC could set out in terms of what we want abuse data to look like. So what should be the scope? How should it be identified? How should we create transparent reporting around it? And then what

types of action could be taken on that basis ideally? Which principles should apply to these 3 or 4 categories if you want to have scope as a separate one?

And that's what we would propose to take back to the GAC in our session on DNS Abuse reporting and on this Cross Community Session feedback. I'll pause here for any questions, comments or feedback on the session. We will take -- sorry, Kavous, there was one speaker before you, and then Iran.

UNKNOWN SPEAKER: Thank you very much. Last time, the CCT review team for ICANN presented a segway regarding the DNS Abuse. There was the view that DNS Abuse for new gTLDs, vulnerability is higher than the existing gTLDs. Then we asked a question, what are the reasons that the new gTLD program is more vulnerable in terms of DNS Abuse. They were of the view that it may be due to weaken SOP implementations, maybe have less compliance to the agreement with ICANN and there is a possibility that they have lack of professional HR and minimal experience.

In this regard my question is that, what are your views, comments on this issue, particularly the DNS Abuse and new gTLDs, and what do you suggest, what is the strategy to mitigate these

challenges, especially in the new gTLDs and ICANN is also in the process of a new gTLD for the second round as well. Thank you.

LAUREEN KAPIN: I just want to put on my different hat as a member of the CCT review team and clarify some of the data on abuse in the new gTLDs. Some of the high level findings of the study were overall since the expansion of new gTLDs, abuse has not gone up. But what we have seen is that there is a trend towards DNS Abuse in the new gTLD program on the rise and needing the same level of DNS Abuse as in the legacy gTLDs. In one particular area, spam, we did see in terms of the snapshot in time that the DNS Abuse study looked at, there was a much higher rate of spam in new gTLDs over the period of time that the study looked at. So that warrants some concern.

The other area that Cathrin has identified is that there wasn't a lot of information that we were able to glean in the study as to why this was happening. Because of course the new gTLD program had many additional safeguards that the contracts applicable to the legacy gTLDs did not have. So there's this uncertainty.

That said, I do want to emphasize that this study was a snapshot that really looked at the beginning of the program, and one of the

recommendations our review team is making is that we should be studying this more and thinking about what is the most effective way to measure it so we can really hone in on what would be the most effective safeguards. Were these effective? Were we not measuring the right thing? How can we improve our policies so that in an ideal scenario we're going to have additional different safeguards that actually result in a decrease in DNS Abuse? That is the aim.

But to loop back to your question which is, what can we do to improve the status quo, I think really the DNS Abuse panel started laying the ground work for that sort of work which is that one, make the data transparent, and what we see even now from the snapshot that the DNS Abuse study took is that in certain cases DNS Abuse can be very concentrated among a small group of players, whether it's a registry or a registrar, that show levels of abuse that are higher, much higher than the rest of the space.

So, if we make that information transparent, then the next step would be what action can be taken to make sure that at the very least we are creating an enforcement environment within ICANN and also within, you know, law enforcement as a whole that can take action against players that are identified as having very high levels of DNS Abuse.

CATHRIN BAUER-BULST: So I have Iran, then the US, and then you. Kavous, please.

IRAN: Thank you. There's some questions, important. I think I have a few small comments. One comment is that when you look into the abuse we are grosso modo wrongly using something for which the objective was different than it was used. Has there been any study whether this abuse or intentional, willful, or there has been unintentional by lack of necessity elements or support this abuse has been done? This is the first question.

The second question that mitigation is good. This is mentioned that the malicious stopped or blocked and has there been thorough identifications. Because if you continue to try to identify the wrong things but not really looking into the source of that and try to eliminate it in a more permanent manner, we continue to have this flow of problems. So these are the things.

And then the statistics, whether it is abuse from a particular DNS groups or there is something which does have very unidentified patterns in -- so all of these questions remain to be answered. Thank you.

IRANGA KAHANGAMA: Thanks. So I think your questions are good and kind of speak to what we are trying to aim, is that there is a lot of confusion over what the trends show, and I think what the CTO's office is trying to do is through this DAR initiative gather a lot of data and statistics. Specifically, maintaining historical records. So once this program, the stats collection is up and running, ICANN will have a number of different data feeds that will aggregate data over historical time line so that you could see the trends of how the DNS Abuse is going, and specifically identifying it so we will be able to do that kind of analysis and then go towards more of the root causes in combination with action as well as policy.

Because, I think one thing that also came up in the session was the importance of being reactive but also proactive, and that the availability of data and statistics will better enable us as a community to be proactive in identifying and inserting policies that will minimize bad actors, increase the cost for bad actors and reduce the burden of all the legitimate actors who are here at ICANN and participating in the policy making process and the business process of the DNS, so kind of balancing the need of being proactive and reactive.

But overall, yes, I think at the end of the day the data is going to be needed and the very smart people here at ICANN can conduct the proper analyses to look at that kind of abuse.

CATHRIN BAUER-BULST: Thank you. I have the US, and then the gentleman over here. Ashley, please.

US: Thanks, Cathrin. I just wanted to take the opportunity to say that these Cross Community Sessions on DNS Abuse have been very, I think, helpful and interesting. And any opportunity to encourage the use of abuse data to inform policy and decision making at ICANN I think is a really good idea, and these sessions have been very worthwhile.

Also programs such as the DAR I think are also positive steps in the right direction and effort should be made to share this data, is needed to enforce contractual obligations, so thank you for continuing to hold these sessions. I think they've been of great interest to the broader community. So thank you.

CATHRIN BAUER-BULST: Thank you, Ashley. Please.

INDONESIA: Yes. Thank you. I speak from Indonesia. I'm asking because of my curiosity. In every meeting about safety, security, and so on,

there's always people from FBI. My question is, is all ICANN safety problem is always taken care of by FBI and not the local police? I'm not talking if someone stole a computer in your office [inaudible] local police.

But I mean, if there's DNS Abuse in, I don't know, Los Angeles, always taken care of by FBI and nothing to do with the local police department? That's number 1. Because I would like also to go further. If I have a problem with ICANN, do I have to go to the California court or to the federal court? Thank you.

LAUREEN KAPIN: So, I'm going to answer your first question first. The Public Safety Working Group actually has a diverse range of players which include members from local police. For example, during this meeting, we have folks from the Royal Canadian Mounted Police and [inaudible] to Quebec.

I'm from the Federal Trade Commission which is a civil law enforcement agency that focuses on combating deceptive and fraudulent behavior. I have my colleagues from the EUROPOL and the EU Commission, so we really run the range of the huge variety of law enforcement and public safety folks that are interested in making sure that ICANN policies promote a safe online environment.

In terms of whatever legal issues folks may have regarding ICANN, that's very fact specific and I wouldn't be able to give you a one size fits all answer on that.

CATHRIN BAUER-BULST: Ineed. And of course, just to pick you up on that, we always welcome new membership. I mean the challenge for us is also that we have to convince countries to invest in this group, and to see an added value for their police in participating and for their other public safety organizations and participating.

So we have a number of states who have nominated also representatives of nongovernmental organizations dealing for example with the fight against child sexual abuse, and we really encourage you to consider bringing people to complement our membership and to increase our diversity. It's something that we're actively seeking.

As you know, we've run a number of Capacity Building Workshops also in the areas where ICANN meetings take place to try and increase the diversity and to equip law enforcement and public safety organizations in the local region with the necessary tools to benefit from the work that's going on here and to actively participate in it. If there's no further questions on this, I would like to spend -- oh yes, Jason, please.

JASON PLOMP: Hi, good morning. My name is Jason Plomp. I work for the Royal Canadian Mounted Police. I do not work for the FBI. As Cathrin said, we certainly encourage all members to join the Public Safety Working Group. We have two members from Canada that work in two different organizations. One from a provincial law enforcement standpoint and one from the federal law enforcement standpoint; and although the Public Safety Working Group certainly works on international causes such as DNS Abuse and the Whois database and things like that, we certainly do discuss operational issues and the contacts that we make within the Public Safety Working Group certainly do help us on an operational basis, and the connections that you do make.

So we do encourage people throughout the world to come out and join the Public Safety Working Group because it certainly does encourage that networking and a face to face communication. So it will help operationally as well. So by all means, if you need help with something, please approach one of us. Thank you.

CATHRIN BAUER-BULST: Thank you, Jason. So we have about nine minutes for our last agenda point on the continued availability of the Whois and

possible impact of privacy laws to prepare a session which we will have with the GAC in a little while. So we're going to have a half hour on that at 11:00.

And we don't want to do a full run down of the half hour, but we thought we would give you a snapshot of what's been going on and then go into one particularly a bit more technical issue on the RDAP pilot program. First maybe, I'll turn to Laureen for a quick update of where we currently stand, and then Greg will say something about how we plan to approach things at 11:00. Please, Laureen.

LAUREEN KAPIN: So a lot of people probably have heard the phrase GDPR being mentioned along with Whois. And the GDPR is a complex wide-reaching set of privacy laws that are going to be implemented later this year in May. And ICANN has been grappling with what impact this will have on registry directory services also known as Whois, and this is has been an issue of considerable concern to many stakeholders in the community.

But what I want to focus on from a Public Safety Working Group perspective and a GAC perspective is that this group is the stakeholder that will ultimately speak for the public interest, and

for civil and criminal law enforcement interests and consumer protection interests in keeping the public safe.

And where ICANN has many representatives from other stakeholder groups, registries, registrars, commercial and noncommercial interests among others, we are the group that is going to have to give voice to the public interest in why the Whois is important for law enforcement and consumer protection concerns. And we are the group that's also going to have to speak for the public interest in terms of the individual gathering information for a safe online experience.

So, for our session later on, we're really going to be focusing on one, what the Whois is, to be a little repetitive, and why it's important. And just as a preview, we are going to be discussing briefly real live case examples where step one is going to the Whois database to find out information about what entity is behind a particular website that may be involved in misconduct. Whether that misconduct is invading people's privacy or exploiting children or just trying to rip people off.

Step one, step one in investigations is often going to that database and gathering information. And right now, that step one is rather simple and quick. And when you are engaged in trying to save people's lives or trying to stop serious misconduct, something that is simple, quick and effective is crucial. So we're

going to be previewing these issues in this later session. But what I want to really emphasize is that things are moving along quickly because the law is going to be implemented, and naturally, ICANN as an organization is very interested in being compliant with laws that apply to it.

But the other thing I want to emphasize is that there's also a period of uncertainty when laws come into effect. There are disagreements about what the law is and what the requirements are. And the process that is going on now is really trying to seek clarity, get legal perspectives on what's going to work best to comply with this law, which in and of itself balances privacy interests and other public interests such as the interest in preventing crime and fraud.

So, this is the time where we're going to be weighing in, and a big ask that the Public Safety Working Group is going to be making is for you as governmental advisory committee members to reach out to your consumer protection and law enforcement agencies and find out how important the Whois is to them so that you can weigh in on this decision making. Because ICANN is going to be asking you to weigh in.

In fact, ICANN has already asked all different stakeholder groups to weigh in. So I just want to emphasize that it's a crucial time and we're going to be providing some further information in our

longer session on what the equities are here in terms of the public interest.

CATHRIN BAUER-BULST: Thank you very much, Laureen. And I think in view of the time, we just have one minute left. I want to take this minute just to inform you that the key goal for us now is to move from basically getting excited about the problem to working towards practical solutions that we can put into place within a reasonable time period. And that's a big challenge at the moment, and there will be a Cross Community Session on Thursday, one of whose goals is also that. So to move towards more practical solutions, and I would encourage you all to attend.

And in parallel, in July there was a pilot program launched of the RDAP protocol, which is a possible protocol to replace the current Whois protocol which has a number of additional features, including for example the possibility for layered access. Now, that protocol is test driving a number of different implementations, and is also open to our input in terms of what we would like to test.

So if we can come up with options that could be compliant with privacy laws, and at the same time maintain the kind of access that we need to see from a public policy perspective, for the needs

of law enforcement but also for the needs of consumers and the cybersecurity researchers industry and authorities, there's an opportunity to basically test drive these solutions now during the pilot project and to try and impact assess, what that would mean for an investigation, what would that mean for cybersecurity researchers, or what that would mean for a consumer and how we might think of solving the challenges that we now face in terms of updating Whois policy in a practical and pragmatic way.

And we'll stop here, and I'm sorry we can't take any questions on this, but we will come back to this at 11:00 today, so there will be another opportunity to discuss this in just a few short hours; and now we need to leave this space for the full GAC to resume its work. Thank you all very much for coming to this session so early in the morning and we look forward to continuing the conversation throughout the week. Thank you.

[END OF TRANSCRIPTION]