ABU DHABI – GAC discussion on Whois/RDS and GDPR
Tuesday, October 31, 2017 – 11:00 to 11:30 GST
ICANN60 | Abu Dhabi, United Arab Emirates

THOMAS SCHNEIDER: That gives time to for the Public Safety Working Group, which is not something that needs to be in the recording. While the physical dislocation is taking place, we welcome Cathrin Bauer-Bulst here at the table and Laureen Kapin as well. And we can now start with Agenda Item 22, which is a session and an update on WHOIS and the new Registry Directory Services and GDPR, which is the European upcoming data regulation directive, which is something that has been discussed by some for quite some time. So let me not prolong the transition period any longer but hand over the floor to you. Thank you.

CATHRIN BAUER-BULST: Thank you very much, Thomas. Good morning to you all. We saw a number of you already in the Public Safety Working Group session. Thanks again. We're going to come back to this topic of the continued availability of the WHOIS and the impact of privacy laws and the new General Data Protection Regulation in particular in this session.

I'll wait for the slides to be pulled up, and while that is happening, we've tried to make it transparent in the Public Safety Working

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

Group session that this is an issue of major significance for the GAC as a whole. While the GDPR is a regional law, there are other regional laws that work towards the same aims of creating a safe space for privacy, of creating standards for data protection. And there is no such thing as a regional Internet, as we all know, so there's also as of now no such thing as a regional WHOIS. And that is something, we of course, would like to continue to see on a global level. So this topic is something whose importance for the GAC as a whole I think cannot be overstated.

What we're going to do today – the slides will be up in a minute – is to basically just take ten minutes to explain to you where we stand right now, why this is a really important issue for all of us in the GAC, and then what the next steps could be for the GAC. Those revolve in particular, to already get you thinking about that, around the possibilities that we have in terms of the conversations with the ICANN Board and the possibilities that we have in terms of providing advice, possibly based on the 2007 principles of the new gTLD WHOIS which we consider to still be valid and applicable. And thirdly, as the GAC to help working toward solutions because it's very clear that there will need to be a road towards concrete, pragmatic, effective solutions that we as the GAC have a key interest in contributing to.

It's still not there. Maybe we can start with a quick update of where we stand. Okay, there we go. Very good. So you’re going to

see the agenda which I just set out on the second slide. So we want to very quickly update you in two minutes on the developments since ICANN 59 and talk about the significance of the WHOIS and the ongoing processes to the public interest with a few examples and then take you to the next steps.

Just very quickly on the development, since we spoke about this in Johannesburg, a lot has happened. Notably ICANN convened a task force to assemble a list of cases for the WHOIS to which Laureen and I were nominated on behalf of the GAC to contribute. There were a lot of contributions from different agencies, different parts of the world around the ways in which WHOIS is used that showed that it has a very diverse range of users right now who all use it for legitimate purposes. Of course, what it doesn't show is there's also abusive uses of the WHOIS. One opportunity in this process might be to see how we can curb those abusive uses.

There was some outreach by the ICANN organization to a number of participants in the community but also to data protection authorities in the EU and to the European Commission. I can just use this opportunity as a staff member of the European Union commission to reiterate that we are fully committed to helping ICANN and the community work towards solutions and that there are tools under GDPR to run a system such as WHOIS and we need to work on how we can explore solutions on that basis.

There have been a lot of community discussions and there are a number of legal analyses that have been published that I would draw your attention to. There will be a Cross Community session on Thursday that I would warmly encourage you to attend where this will be explored in more detail.

Now let's quickly turn to the examples that we have of the significance to the public interest of the WHOIS. The first one will be from our Canadian colleague Nadine who will speak in French

CANADA: Good afternoon, everyone. I am Nadine Wilson. I come from Quebec in Canada. I am a member of the Royal Mounted Police in Canada, and I work in the Cybercrime Division.

I would like to speak about the need to use this data on WHOIS. We use this data in order to find child sexual abuse. We have started using this information in order to detect suspects. Information available on WHOIS is not always valid, but when the abusers make mistakes this information enables us to track them. We can track their valid e-mail ID and we can track different hints and read different suspects. We are able to work along these lines because of the WHOIS information.

Then we have a national center that coordinates actions against child exploitation in Canada. In 2016 and 2017, we received more

than 30,000 different information items, and we were able to read different people that were engaged in child exploitation. We're speaking about children. I do not want to overlook other victims, but I would like to draw your attention to the fact that we are dealing with victims that are children. Therefore, we need the WHOIS database in order to act expediently. Thank you for your attention.

CATHRIN BAUER-BULST: We would like to start with you from EUROPOL, our colleague Greg Mounier please.

GREG MOUNIER: Good afternoon, everyone. To continue what Nadine was saying to really put things into context. WHOIS is really the first step in cybercrime investigation. It's really essential. The investigator will use WHOIS information mainly for two purposes. First of all to find contact points for domain names. So if you find the domain names and you fine the registrar, then you can get serve legal process or [a legal just] to get more information on that.

I think it's very important to keep in mind that investigators and law enforcement are after identifications. They are trying to attribute a crime to an individual, and WHOIS has a lot of

information that can give you investigative leads to continue your investigations.

We're not saying you will find your suspect in the WHOIS because, of course, if you are a criminal, you are a little bit smart and you will not put your right information. But you will have to have at least one valid e-mail in order to communicate with your registrar. You need to pay your bill, so you have to have at least one type of information correct. And [you are] [inaudible] to find that information, cross matching other information and then leading up to the identification of somebody and to attribute crime. So it's not the silver bullet, but this is really an essential tool. Next slide.

Again, just to illustrate what we are talking about, this is the result of a WHOIS lookup. You can do the same. You take any domain name, you enter in ICANN WHOIS or any other central [ops] WHOIS, and then you get a list of information. We sift through that information, and this gives you very important leads, clues that can be cross matched with additional information and then leads you to continue your case.

For instance, you find the registrars, you find the date when the domain was created. That gives you some good information, when it was last updated, if it's still valid or not. Then you also find the address of the registrar. That can also be very useful. A phone

number, sometimes a phone number may be the only link that is linked to other malicious domain. Next slide.

That's the information on the registrant. In that case, that's the domain name [inaudible]. You see that the person or the company in charge of that name is associated with [inaudible]. You have the postal address, phone numbers, e-mail address as well. So you cross check all this information, and it leads you to more information. The case I want to show you is a botnet case fairly recently. Using WHOIS data, we were able to attribute who was behind and controlling that domain.

Basically, a botnet is a network of infected computers and they all report to one server where they are going to get their orders to do a spamming campaign, spread ransomware. If you are a victim of ransomware, you report the case to the police. We will investigate. Possibly, we will find out how the malware or the ransomware was distributed. Then you might find the domain, which is the rendezvous point for the bots to connect to the command and control server.

Once you have the domains, you do a WHOIS lookup and in that case we find one e-mail address. You do a reverse WHOIS lookup which is research on the e-mail address which gives you all the domains that were registered with the same e-mail address. Of course, if you are a smart criminal, you will use maybe ten

different e-mail addresses, but you will need to register hundreds of domains. So at some point you will be able to find one valid e-mail, and that's what we have done.

We came up with a huge list of domains that were registered with the same e-mail address. Again, you go through all the various domains. And then we were able to find an old private website which gave us some information to then order some more house searches on the person which lead to the identification of the suspect.

Again, this is not the silver bullet, but this is really an essential tool. If you remove the WHOIS, then most of the cyber investigations will be hindered severely. Thank you.

CATHRIN BAUER-BULST: Thank you, Greg. We will have one more example from Laureen Kapin, and then we we're going to actually give you time to speak in a minute.

LAUREEN KAPIN: Sure. What I also want to draw the link about is you are hearing why WHOIS is important, but what I want to underscore is the reason we are having this conversation is because the GDPR, depending upon how it is interpreted and implemented within the ICANN ecosystem, really will impact how easily law

enforcement can access the WHOIS database and also how the public can access the WHOIS database. So I just want to underscore that point. That's why we're giving you these case examples because the GDPR is going to have an impact on how this information is going to be made available.

So back to one final use example. In the United States, the Federal Trade Commission focuses on consumer protection issues, and we are also the agency that enforces privacy and data protection laws in the United States. And we actually use WHOIS information when we investigate privacy violations.

So if entities are sending out phishing e-mails luring you to click on a link that may download spyware or malware on your computer that can actually then track your keystrokes when you are putting in your credit card information or putting in passwords, when we at the FTC investigate those types of elicit behaviors, we go to WHOIS to find out who is behind those websites. We do that to protect privacy.

I just want to underscore that because the GDPR and the GAC's own 2007 principles on the WHOIS really seek to balance these law enforcement and privacy interests. And privacy interests are not just related to protecting information, people's personally identifiable information, but they are also related to how law enforcement agencies combat crimes that have to do with

invading privacy or using your private information to rip you off, to cause you financial harm, to cause you other types of harm. So that's one last use example.

And then finally, just to also emphasize the public, you and I in our online communications, in our online purchases, in our online activities where we provide sensitive financial information, sensitive health information when we may be getting prescriptions for example from pharmacies, we use this information when we want to find out, is the website I'm dealing with legitimate? Maybe that website doesn't have contact information on it, so as a user, you can go to the WHOIS.

Also, we at the FTC know that the public uses WHOIS to resolve their own disputes and to assist law enforcement because when they complain to the FTC and say, “I've been ripped off” or “someone is engaging in elicit behavior,” they refer to WHOIS information in their complaints. So this is another public interest.

And that's separate and aside from all the legitimate business interests: the cybersecurity investigators, the brands protection folks who want to make sure that folks aren't masquerading as a legitimate charity or a legitimate bank when, in fact, they're not. There's a whole host of other uses that is important to the public here.

So that's a broad array of reasons why we as the Governmental Advisory Committee need to be thinking about the public interest regarding these very important GDPR issues and how it may affect the WHOIS.

CATHRIN BAUER-BULST: Thank you very much for those powerful examples. Now I want to emphasize also, taking my commission hat here, from the perspective of the commission, the threats to the continued availability of this data and to the continued accessibility does not lie so much in the GDPR in and of itself because the GDPR offers tools and methods to run services with a functionality like WHOIS. The threat comes more from the fact that at the moment there is no coordinated process to ensure that there is one cohesive approach to how we deal with this problem and that leads to insular solutions.

Because if we are not providing that process, registries and registrars will have to draw their own conclusions about what they need to do to be compliant individually rather than us as a community. And I think GAC has an important role in this, not just the contracted parties and ICANN, because there are clauses in those contracts that are there because of the public interest in the infrastructure they provide. And there's a sort of guardianship of the GAC in terms of those clauses be brought to [life]. And that

cohesive process I think should be one focus for the GAC in terms of how we move forward on this. I think we are long past saying this is an issue. We now need to look at how we can address this issue pragmatically.

Concretely, there are three next steps we want to submit for your consideration. We could raise this with the Board. We could include this in GAC advice. We could also offer our support in contributing toward solutions. We've already done this as the European Commission, but perhaps we should also do this as the GAC.

I'll just stop here and allow for you to take the floor and share your views on all of this. We have Indonesia. We have the U.S. So Indonesia first, then the U.S., and then the gentleman in the back.

INDONESIA: Yes, thank you, Cathrin, for the PSWG information, especially about the standard GDPR. I apologize for my not too much knowledge about the GDPR standard for [Europe]. As far as I know, GDPR was set up by a nonprofit organization, the [inaudible] or something like that. And then is it adopted by the European countries? Or if it is adopted by the European countries, why would you transform that into a [EM], European [indiscernible] which is from my understanding is a European standard? Now that's number one.

Number two, is there any coordination between the standard with other big organizations like IS or IEC or whatever? Now I'm asking this because in several [different] countries, including Indonesia, standards are carried out by government, not by public or nonprofit organization. It's by government agencies. And being [inaudible] from agencies, it is easier for us to work together with organizations where we are members. Indonesia is a member of IOECE, but it is very easy for us to work with [EM] rather than non-governmental entities. Sorry asking you this.

CATHRIN BAUER-BULST: No need to apologize. So the GDPR, the General Data Protection Regulation, is a law that was adopted by the EU, the European member states and the European Parliament, that will come into application in May 2018. That basically regulates the way in which businesses and organizations handle personal data. So it's not a standard. It's legislation designed to basically further specify the fundamental right to privacy in data protection that exists under the European Charter of Fundamental Rights.

I have the U.S. up next.

U.S.: Thank you, and thank you so much for this very useful session. I think it was a very opportune time to remind us, as well as inform

us, as to how important access to WHOIS information is for a variety of uses and stakeholders, particularly governments and protecting the public as well as cybersecurity.

I'm also very glad you are focusing this conversation on the important role that GAC can play here because what I'm concerned is, I mean, it's very important that ICANN contracted parties work to be compliant with GDPR, but I'm afraid that has been the sole focus and we have almost lost a little bit of sight with respect to we make sure it's very clear how very important it is that we maintain access to this information. Not only access, but timely access. That's very important. If we go to a system that requires court orders in every single case, that's going to be very debilitating I think in our efforts to protect people.

Also, I just wanted to note and flag that this actually has a very extraterritorial aspect to it. It may not be obvious and apparent to everyone since in the case of GDPR you have to protect the privacy of European residents. But the issue is that what we are facing here, particularly in ICANN context, is that there is going to be a global solution, which is a good thing in itself. But at the end of the day, the United States for example, is going to have a harder time accessing registrants of .com. That's an issue for us. That's an issue for our law enforcement and for our consumers.

Also, it has been made apparent to us this is potentially going to put us in conflict with a number of free trade agreements we have with other countries. Where we explicitly have text that says that we have to make publicly available registration information for domain names.

I just wanted to bring that to people's attention, and I urge my GAC colleagues to please consider how you use WHOIS information and how it's important to what you do – if it is important to what you do – and consider what the impact will be if there's a day in the very near future where we do not have timely access to this information. Thank you.

LAUREEN KAPIN: Thank so much for raising that variety of really crucial issues. One thing that I wanted to underscore was this issue of timely access and access in general, particularly if you are trying to access information from another jurisdiction. Right now as a law enforcement agency in the U.S., if I am going to use WHOIS, I can access information from registrars and registrants in terms of identity from all over the world. I don't have to seek a court order. I don't have to collaborate with my colleagues in other jurisdictions. I don't have to be told, no, you are not in our jurisdiction so we don't have to give you information.

This system lets me access that information quickly to be able to conduct my law enforcement activities. And that is a benefit that is beyond measure because, as I said, that's a first step. So this is really crucial to law enforcement agencies' effectiveness. And that's not to say in appropriate situations when you need to delve deeper, that law enforcement isn't going to go through the appropriate due process procedures to obtain the information they need. But this is for basic, first step information.

CATHRIN BAUER-BULST: We've heard examples of cases where WHOIS information has been crucial, but maybe it's also interesting to look at the volume. Because we spoke to some cyber investigators in the EU and we were trying to assess the impact, and just one smaller cybercrime unit from one member state, the head of that unit told me he estimated his unit makes around 50,000 WHOIS lookups a week. If we imagine that going through a system including court orders, that's just not going to work at all.

With that point, we have Pakistan, then we have Iran, and then the gentleman in the back.

PAKISTAN: Thank you very much for the detailed explanation on your examples.

I noted from your example that you recommended that please contact with the domain name point of contact, it may via e-mail from the registrar. Generally, we see that this is a challenge for the Internet community that the WHOIS date is not up to date and the accuracy of WHOIS data is one of the key challenges.

We also note that ICANN and its Working Group and the concerned [quarters] are working since 2000 on the accuracy of data, but still it is a challenge. Of course, anybody who is facing the challenging issues, they will contact the domain names point of contact, i.e., the registrar, but the registrar is not updating the information. So it is also a challenge for the Internet community.

As you know, ICANN also launched the IDN ccTLD, and there are many IDN ccTLDs and they are in the local languages. These are also additional challenges for the WHOIS database because the handling of Unicode and conversion into ASCII code and then maintaining the WHOIS data is also a challenge.

The next one, in the new gTLD program which was successfully launched in 2012 and as per the applicant guide of the new gTLD, it is clearly mentioned about the WHOIS that applicant must provide WHOIS services for their users. However, ICANN will verify the WHOIS data is accessible. And how we see that accessibility on the WHOIS data is still a challenge.

I highlight two challenges. One is the accuracy of the rules data and the accessibility. So I want to hear from you, your recommendation and your working group. Thank you.

CATHRIN BAUER-BULST: Thank you very much. The accuracy is also a point the Public Safety Working Group is working on. For the interests of this session, I would perhaps propose that we focus for now on the availability and come back to this. There will be a another session later in the week. So I will propose we now go to Iran. Then I have Netherlands and U.K. Please.

IRAN: Thank you very much. I think the subject that you discussed this morning, earlier at the beginning, is one of the very, very important topics and subjects that all people, all governments are interested in. It was said that when a suspect or a website is followed and then you go to hundreds of e-mails, hundreds of registrars, so on and so forth, once you find the sources, do you make this information publicly available to the others? And actions you have taken not that the issue will be continued and so on? Is this information you share with other people? Particularly I'm addressing to the Interpol whether you share this information as soon as possible with your other connected

Interpol offices in other countries that they are timely aware of the situation that is being done?

And my second question is, if for one or other reason – I don't want to go into detail – is there any restriction of any country to have access to this information? Because sometimes there are restrictions or decrees that do not make the service available to particular countries for various reasons and so on and so forth. So this is a very important issue. We do not want to have any restriction to have access. It's very important information. [With humanitarian it] has a very, very important nature and not fall under these other decisions which have different reasons and so on and so forth. I would like to whether there's full access for all countries irrespective of where they are and the issue of some services and so on and so forth may not be available to some country does not apply in this case. Thank you.

GREG MOUNIER: Thank you for your questions. Very briefly, if we work on a case which is transnational, which is most cybercrime cases, if the backend infrastructure is spread in different countries, including Southeast Asia and Europe and so on, we will be [competent if their] victims are in Europe. But then afterwards if we need to take down an infrastructure and then we need the help of the local police, yes, we will go through Interpol and the international

police cooperation mechanism to have your help and the help of those competent authorities that are involved in the case to further the investigations.

I think if your questions relate to whether you have restricted access to the WHOIS, no, everyone has access to the WHOIS. I know the cyber police in Iran are using WHOIS to do their criminal investigation as well as in China or in the U.S. or in Europe. Everyone is doing the same. There is no restriction as long as you go through the normal procedure which is Interpol mostly or bilateral information [treaty].

CATHRIN BAUER-BULST: Thank you, Greg. We have the Ukraine, the Netherlands, U.K., and Palestine. After that, we have to close the list. So, Ukraine, you're next.

UKRAINE: Thank you. I have a very short question because our country is [inaudible] the European Union and according to the association agreement needs to follow their latest legislation development. I just wish to receive a very basic but very important clarification. In the Europe Union, how do you qualify encrypted data [inaudible] which is being stored in the European Union? That's this data, personal data, text, picture, which was encrypted and

doesn't appear to the administrator or law enforcement agent inside European Union jurisdiction as a personal data or it's just like technical data without any personification. Thank you.

CATHRIN BAUER-BULST: Thank you for that question. I suggest that we maybe tackle that after the session because the WHOIS as of now is openly available, at least the part that we are talking about now. So let's talk after the session. We will now go to the Netherlands and then we have the U.K. and Palestine.

NETHERLANDS: Yes, thank you, Cathrin. Just some remarks. I think first of all maybe the GDPR is maybe underestimated as if some things would be possible within the GDPR [context]. But I think GDPR is very clear about certain things, and it's not anymore something which is, for example, being dealt with the commission but all 27 countries have to really look whether some WHOIS solution is according to the GDPR.

It means they can get fines up to, I think, 4% of the revenue. This is real. I mean, we are talking about something about which will be illegal in some countries. And probably have seen the DPA letter which was sent on request of the [.frl] registry, which basically says it's illegal under Dutch law, their specific

implementation, and probably also according to GDPR because GDPR and the laws we have now are not so much different. It's only harmonized. So I think we have to really deal with the fact that GDPR will be there and [as this year's case].

Secondly, I think, of course we recognize the access needed to WHOIS data, but I think there's a kind of simplistic way of saying, okay, it will be shut down and we will have only access through court orders and lengthy processes. I don't think this is the case. I think for all kinds of access of certain data, a motivated request without a court order is possible. And to be even in the Netherlands, .NL Dutch [ccTLD] registry, has these kinds of mechanisms. This can be used. It's not only black and white. I think the representation of this problem is a little bit too simplistic. Thank you very much.

CATHRIN BAUER-BULST: You make two very important points, if you allow me to briefly react. One is that, of course, all of us are in this together. It's not the European Commission on its own and it's not just even the 27 member states. It's the entire GAC who need to look at this. We need to look at how we can comply, and it's very clear that changes are needed to ensure that compliance. We should be a key participant in creating this change and in contributing to a solution that works.

I have to apologize if we have been painting it with a simplistic picture. Given that this is an extremely complex debate and we are trying to basically transport options and status updates to you in a very short amount of time, we may have been oversimplifying things. I fully recognize that. And, indeed, what solutions could be are somewhere in between.

I think there are still parts of the community who think that things are going dark and I think for all intents and purposes if there needs to be an individual motivated request for 50,000 lookups a week, that is an issue for law enforcement. So there must be other options that we should explore, and that's where we as the GAC can contribute.

I'll go to the U.K. next, and then we have Palestine.

U.K.: Yes, thank you, Cathrin. I'm pretty much on the same track of comments, really. I'm not an legal expert and I haven't been close to the U.K.'s participation in the negotiations that have led to the GDPR. All I know is when I go into the office in London, I see a big poster: "GDPR is coming. Get ready!" It's major, no doubt about it.

But my question really is, the case examples we have heard about in this session this morning demonstrate that this is legitimate

purpose to these requests for consumer protection authorities and law enforcement agencies. And so is it actually definite that access for those legitimate purposes to advance the public interest, to protect consumers, to track criminality is somehow defeated by application of the GDPR to the WHOIS database?

Maybe this is connecting with what the Netherlands have just said, that actually, the material impact, substantive impact of GDPR might not be that great and that if you have some agreed mechanism approach, whatever it is, similar to what individual country code registries have enacted, may actually solve a lot of this problem.

In the PSWG this morning, I caught the final part of the session, when there was reference to layered access that would facilitate the kind of access for public interest purposes that we need to maintain in order to avoid the situation of registries starting to delist this kind of key data, contact details and so on, from the WHOIS database. That is the real threat to the whole integrity of the WHOIS database.

But maybe, actually, the message we could be going out with is actually the solutions might be readily available to us. It might need some quick work to actually bring about those in time for May in consultation with data protection authorities and law enforcement agencies and consumer protection agencies and so

on, but maybe there is a course ahead of us within this community to bring that about.

So that's my question really, do you think there is some prospect here actually for fixing the issue in time? In view of the legitimate purposes we have been talking about, which I understand are kind of catered for in the GDPR itself. Thank you.

LAUREEN KAPIN: You raise very excellent points and if we didn't think there was a solution, of course, we wouldn't be here talking about it. I think it's really important to emphasize that the GDPR has these pathways baked into the system. It has a balancing between protecting privacy interests and people's personal identifiable information and balancing legitimate interests for access to that information. And there are specific paths available under the GDPR to appropriately balance those interests.

I think our mission here, should you choose to accept it, would be to say, we need to focus on these public interests to make sure they are balanced in the proper way so that information is protected under the GDPR and also these other interests are taken into account. It is a balancing. There are paths there. And we want to make sure that ICANN is not only focusing on the important business interests at stake and avoiding liability, but

the paths available under the GDPR to protect these public interests as well.

CATHRIN BAUER-BULST: Thank you, Laureen. We have Palestine next.

PALESTINE: Thank you. In the past I was within a group discussing the conflicts. In the past I was working with groups that discuss the conflicts with the laws and how that conflicts the applied legislations in Europe and what can be done against to defeat the cybercrime and all the abuses. And there were so many sessions with the RIR and with enforcement law agencies.

The RIR are subjected to the laws of the country where it is. And there might be a crime that be committed in a country and in other countries that it might be not as ordinary and it might be there is a strong law that can deal with that crime. So how can we get the data from that?

In the past, we were suffering of the registrar or registries are not documenting the information and data very accurately, so when we try to get information, that will be a difficulty and there will be no sufficient information an accurate and other parties should be involved to get this accurate information.

CATHRIN BAUER-BULST: Thank you, Palestine, for raising these points and also for bringing the attention back to this accuracy point, which I think we all agree we have to tackle and which is actually one of the things that is required under data protection rules, you have to have accurate data about yourself.

I think you are also asking what can be solutions to this and how can we get to the data? And I think that brings us back to the discussion of possible next steps. So what we would suggest in terms of the avenues that the GAC might explore is, first of all, we could consider raising this and the importance of GAC involvement with the Board. We could also look at drafting GAC advice. And we could look at ways in which we can contribute to pragmatic solutions. The last two points we can, of course, come back to after the Cross Community session on Thursday when there will be a second session where GAC can discuss GDPR and WHOIS.

But maybe to already share with you, if we can go to the next slide, we have drafted a few bullets that to us seem to sum up the views that the GAC has taken in the past, in particular based on the 2007 WHOIS principles. Which we still think are an excellent source of guidance for the public interest as it is reflected in WHOIS policy.

So we could consider in GAC advice to reiterate that these principles should remain applicable and should be respected. That WHOIS should remain accessible to the public to combat abuse and fraud and engage in due diligence for online interactions and communication. That WHOIS must also remain accessible and effective for consumer protection, law enforcement investigations, and crime prevention efforts. And on the process side, that we should encourage ICANN to practice transparency in its activities related to compliance with the GDPR and to provide opportunity for a timely and meaningful GAC input.

And finally, we might wish to encourage ICANN to continue engaging with the European Commission to facilitate discussions regarding the GDPR compliance process. And as our colleague from the Netherlands points out, the European Commission is not the only actor in implementing this. Part of what we can do to support the process is that we serve as the secretariats of the Article 29 working party, which is the place where all of the EU data protection authorities from the member states come together and discuss these issues.

And in our role as the Secretariat, we can help facilitate conversations and make sure the right parties are at the table. So what we are trying to say with this point is not to say the European Commission is the source of all wisdom on GDPR. Far from that.

But that we can help in supporting a process that would allow the community to check any options it wishes to put forward with national data protection authorities.

Maybe I will close it here and leave this for your consideration and further discussion. We now will have the session on the GAC's meeting with the Board where we might at least discuss the first point of those three possible steps the GAC might wish to take. Thank you very much to all of you for your participation.

THOMAS SCHNEIDER: Thank you, Cathrin. That's the end of this session, number 22. We will move over to 23 in 30 seconds. So thank you all for having joined us. I guess we will have a slide with the so-far proposed agenda items for the meeting with the Board that's going to happen later this afternoon. Until, we wait for the slide.

[END OF TRANSCRIPTION]