HELSINKI – GAC Public Safety Working Group Meeting
Tuesday, June 28, 2016 – 08:15 to 09:15 EEST
ICANN56 | Helsinki, Finland

ALICE MUNYUA: Good morning: Good morning, everyone. Thank you very much for coming this early to this GAC working group session, the Public Safety Working Group.

We have an agenda set up, which is going to be a quick update on a few of the activities that the Public Safety Working Group has been following up on. And then we're going to spend a little bit of time to prepare for the privacy -- proxy/privacy services accreditation issue in preparation for the GAC session and also in preparation for our joint session with the GNSO and the ICANN Board.

I will quickly introduce members of the Public Safety Working Group who are actually the subject matter experts, and I will start perhaps with Wanawit at the end, who is my co-chair. Introduce yourself, please.

WANAWIT AHKUPUTRA: Good morning.

CATHRIN BAUER-BULST: Good morning, Cathrin Bauer-Bulst from the European Commission.

GREGORY MOUNIER: Good morning. I'm Gregory Mounier from the European Cybercrime Center at EUROPOL.

LAUREEN KAPIN: Laureen Kapin from the U.S. Federal Trade Commission.

BOBBY FLAIM: And Bobby Flaim from the FBI.

ALICE MUNYUA: Thank you. And I'm Alice Munyua, chair of the Public Safety Working Group, from the African Union Commission.

So we're going straight to the first update that's looking on the next generation gTLD registration directory services.

GAC liaison has been EUROPOL, Greg Mounier, so I'll hand over the microphone to you, Greg.

GREGORY MOUNIER: Thank you, Alice. For those who were not there yesterday for the PDP RDS cross-community session, just a very quick update on where we are at.

The reform of the WHOIS and this PDP is a long story, of course. ICANN and various working groups have been working on it a long time, so a lot of work has been done already.

We had -- The working group has spent -- have spent the last three months mapping out all the key inputs on that topic, and now we are in the second phase where we are identifying out of those key inputs all the possible requirements that next generation RDS could have.

We haven't started any deliberation yet on those requirements. Yesterday we had that public session where all attendees could met with new requirements, just to give you an idea. We have now a document about 110 pages with about 750 different requirements that the next generation RDS could have. And so at the end of this ICANN meeting, we will start dividing those requirements in groups and then another task that the leadership of the PDP next generation RDS has now is to try to find a compromise on a way to decide and to define consensus on those requirements. They're working on the working method of how we're going to discuss about those requirements and how are we going to decide on which requirements are relevant

or not. And then once we have done that work, that will be by the end of 2016, there will be a first report that will be an initial report that will be presented to the community. So that's where we are at. It's a long-term endeavor but for the Public Safety Working Group this is very important to be sure that the GAC and the Public Safety Working Group views are represented in this PDP.

And, yeah, I will keep you informed regularly.

ALICE MUNYUA: Thank you, Greg. Any questions or comments?

Switzerland.

SWITZERLAND: Hello, good morning, and thank you very much for this update.

Just a very quick question. Do you see any need for GAC input on this moment of time?

Thank you.

GREGORY MOUNIER: Yes, absolutely. That's important. The working group has already issued a second informal request on possible requirements that are not already on the list. And so we are

working now on -- at the -- me and the commission and the Public Safety Working Group on trying to commit with new requirements that might be suitable for the GAC. And the plan is to send is to send you in July a draft list of requirements that are not in the initial list, and then for you to endorse it or not and then potentially by the end of July we'll submit it to the full working group.

But the way the working group is working is that they want to issue a number of outreach requests, sometimes formal, sometimes inform ma'am. There's no obligation to respond. And sometimes the deadlines are fairly short and this one was issued mid-June and we had more or less informally to come back to them by today. So it's very short. So for the GAC structure, it's -- you know, we told them and had discussion with the leadership team of the Public Safety Working Group that we are engaged. We want to contribute, but we'll probably need a bit more flexibility in terms of the time we'll have to get back to them. But that's okay, I think.

ALICE MUNYUA: And just to be clear, I sent an email just before we came to Helsinki, I think last week, just warning GAC colleagues to expect this second informal outreach request. And I did let you know that we've informed the working group that it's going to be near

impossible to have the GAC comments on time and to receive a response for them to say it's okay, they would expect a GAC response by the end of July.

This is an informal request. Most of the documents already exist so basically all we're going to be doing is providing a list of documents that already exist from the GAC. But we do have to come pack to the GAC for the usual, you know, process of endorsement and additional comments.

Any more comments?

Okay. If there are no other comments, I think I'll hand over the mic to Bobby Flaim to give us an update on the previous GAC advice on the Registrar Accreditation Agreement. Bobby.

BOBBY FLAIM: Okay. Thank you, Alice.

One of the things that we're aiming to do is have some follow-up to GAC advice which has yet to be implemented. There's three areas. The number one area concerns the WHOIS specification of the 2013 RAA. More specifically, and the WHOIS specification is the cross-validation of the address. That was something that should have been implemented within about six months of the RAA being signed back in January of 2014.

So we've been following it over the years, but this is something that I think we want the GAC to formally look at and make a request for concerning the implementation.

So I think what we envision at this point is discussing this here or at least mentioning this, and then actually drafting a document maybe with very specific questions.

And more particularly, with the GAC advice session yesterday, conforming what we do write with what was discussed yesterday, I believe by Manal, insofar as the implementation, what the vision is, the rationale, so on, so forth.

Some of the things with the cross-validation that we're going to ask about is what has been done so far by ICANN to fulfill this recommendation. Is there a timeline with specific milestones, things of that nature.

So that is something that we would like to maybe have the GAC look into a little bit more.

Another thing that we are looking into pursuant to GAC advice from Beijing on the new gTLDs, specifically the six general safeguards, one of the things was providing statistics on abuse such as phishing and malware. So we're going to see where we are with that and make a request from ICANN insofar as if there's being any statistics provided.

I know we had a session yesterday with the registrars, registries, Bruce Tonkin from the Board had called the session yesterday, and one of the things that the ICANN security department said that within a few days they would start to release some statistics. So that is something that we would like to follow and look into; again, pursuant to Beijing GAC advice concerning the new gTLDs.

So these are some of the things. I think there may be other areas as well, but these are the two big things that we are looking for to kind of follow the advice that the GAC has given previously to see what the status is; if it hasn't been implemented, when can we look for that implementation; how will it be implemented, so on and so forth.

So there may be a few other things but like I said at the beginning, what we do plan on doing as the PSWG is writing a document and going to the GAC for review and endorsement and then bringing it to ICANN.

So that's all I had for myself.

I do also have Mason Cole here. I guess we can go to questions first, but I do want to give Mason Cole the opportunity to give us an update on the Healthy Domains Initiative.

Mason, if you know, is the GNSO representative to the GAC, and he also is the chair of the Healthy Domains Initiative. So I had asked him to be here to give us an update on that. The PSWG sits in on that and we look to be a partner in that. Any way we can foster good behavior, good practices, security and stability, we always want to be a part of.

So Mason has done that through Healthy Domains Initiative. At the last meeting in Marrakech, they had a meeting. This meeting being different, there's no meeting, but there is constant movement on that initiative.

So, Alice, do you want to -- If there's any questions, should I take them and give it to Mason or what do you think is best?

ALICE MUNYUA: We can have questions on the Registrar Accreditation Agreement first and any follow-up.

Any questions?

Iran, please. Thank you.

IRAN: Thank you. Good morning. Once the statistics of abuses of safety are identified and available, what follow-up action is required? Does it have any impact on the advice itself, or what is

the actions? Just providing the statistics is just what has happened. What will be the follow-up actions?

Thank you.

BOBBY FLAIM: I think what we want is first to have the transparency to actually get a vision of what's going on. And then take appropriate steps from there to see if there's any contractual obligations, to see if there's any enforcement mechanisms at that point.

But I think what we're trying to do at this point maybe is shed some sunshine on the issue, see where things are going right and things where things may not be going right, and to see how we would work as a community to correct some problems.

ALICE MUNYUA: Okay. There are no other questions, so, Mason, please.

MASON COLE: Thank you, Alice. Good morning, everyone. As Bobby mentioned, my name is Mason Cole. Some of you know me as the GNSO liaison to the GAC, which I'm pleased to continue serving in that role. I also chair the Healthy Domains Initiative committee, which is under the umbrella of the Domain Name Association. The Domain Name Association is the trade

organization for registries and registrars that represent those bodies' interests in various form.

Bobby asked me to give a brief update on the Healthy Domains Initiative, which I'm pleased to do. I'll do so quickly and if anyone has any questions I'm happy to answer them now or later on in the day, whatever is convenient.

So let me just give you a quick overview of the purpose of the Healthy Domains Initiative. There are three objectives. One is to establish a network of industry partners that communicate and collaborate with one another in order to present a healthier and continually evolving domain name space.

The second is to identify or develop industry accepted best practices that registries and registrars can employ in a way to promote standards for healthy domains.

And the third objective, then, is to demonstrate to the community contracted parties' desire to implement those practices and otherwise fulfill the stewardship obligations we have to the domain name space.

So the Healthy Domains Initiative started about a year ago, and in the process of developing the initiative, we collected lots of feedback from registries, registrars, and other parties who have an interest in the domain name space.

We held a summit in Seattle in February of this year where we had 77 participants, and we collected lots of ideas about how to promote a healthy domain name space, both operationally and otherwise representing what a healthy domain name space would look like.

As Bobby mentioned, we met again in Marrakech and we synthesized those ideas down to a few that we thought we could reasonably implement in a productive way, and that -- excuse me, that's evolving into a best practices document which we're now refining as the first output of the Healthy Domains Initiative.

So as Bobby mentioned, I'm here to give you a brief update on what that -- what the status is of that best practices document and what you might expect in terms of the next steps.

So the document then is organized into -- oh, I'm sorry, there's one other thing I want to mention. We conducted a survey of registries and registrars to ascertain what they already are employing in terms of operational best practices that promote a healthy domain name space. These are things like -- and we wanted to find out what contracted parties are already doing. And we found that in a pleasing way there were lots of things that were already underway. Things like monitoring for phishing and malware, pre-registration validation for certain high security TLDs, publication of easy ways to report abuse

complaints, tools for automating abuse complaints, things of this nature.

So with that as a baseline then, we wanted to find out where we want to go. So we've categorized the best practices into three areas. The first is operational best practices that could be immediately recommended. And there are maybe a dozen of those, and these are things such as making sure there's a priority focus on proactive recognition and action on abuse, you know, maintaining an environment among all parties that's quickly able to react to best practices and principles. Abuse reporting requirements that are clear and documented to end users and to contracted parties. And I'm happy to share some other ideas with you as well, but I'm conscious of our time.

Our next category then is aspirational best practices. And by aspirational I mean these are things that are not currently in place but can be put into place over time. And we have -- some of these are operationally complex and they'll need to be implemented over time, but they include things such as making sure that there's a timely response to domain name takedown requests by various authorities or law enforcement. And I know that contracted parties are interested in enhancing their relationship with law enforcement for various reasons, but this is one of them that can be productively put to use.

Another is sharing information among contracted parties as we're able to do so legally about fraudulent domain name registration. That includes things like credit card information, company names and other available data such as that. We're thinking of collaborating with child abuse authorities as a way to combat online child abuse, establishing a reporting system for what's known as badware which is software that disregards user's choices about how their computers are used. These are examples of aspirational practices that we would like to employ over time.

And then the third category then is additional practices that would be ideas for future consideration. These are things such as third-party validators which would be a validator that has expertise, credibility to evaluate complaints, and then form a trusted relationship between that party and registries and registrars so that abuse can be handled in an expedited way.

Another example would be the trusted notifier program. You might have read that there are registries in the industry who have recently established relationships with experts in content and they have established ways that those trusted notifiers can let a registry or registrar know about clear and pervasive uses of copyright infringement and then there's a process for taking down those domain names or otherwise mitigating that abuse.

So in terms of next steps then, we're here in Helsinki. There will be a brief meeting tomorrow of the contracted parties for the healthy domains initiative. We're going to review these ideas, refine them further, and then the next idea or the next step would be to assign subgroups to develop the concepts and then find out how to put them into operational practice with registries and registrars. We'll probably also plan another summit sometime in 2017 where all interested parties, not just registries and registrars but anyone with a stake in a healthy domain name environment, can gather and talk about how to further put some of these practices into place.

So I realize this is a very short update. There's plenty more in here. So I encourage questions, and I'm happy to answer them as I'm able.

MASON COLE: Thank you, Bobby. Alice.

ALICE MUNYUA: Thank you, Mason. Any questions or comments? Yes, Council of Europe.

COUNCIL OF EUROPE: Thank you very much, Madam President. Just a quick comment to -- yeah. Gianluca Esposito from the Council of Europe. I just wanted to thank very much the speaker for the presentation and I was particularly watching the reference to these aspirational practices that he described on preventing child abuse. That's an area where recently our membership has been really focusing on working not just to take down content of course but also to deal with the issue of domain names that explicitly advertise child abuse and child pornography material. So I just wanted to welcome that development. I think that's actually a very welcomed step. Thank you.

ALICE MUNYUA: Thank you. Ah, yes, Thailand.

THAILAND: Yes. Wanawit, for the record. Mason, thank you. And I have some question regarding the trusted notifier because you have mentioned about the registry and registrar coordinations. And if we -- and that might be related to the issues that are dealing with this, IPs and that kind of content, but when it come to this kind of hate speech or things that led to the platform provider, will the trust notifier includes in that scopes of discussion as well with this? Thank you.

MASON COLE: Thank you for the question. At present, no, the trusted notifier program does not include hate speech. It's specifically devoted to copyright infringement. So contracted parties want to be careful to also protect free speech rights and balance that out with dealing with clear and pervasive infringement of copyright. Hate speech may be an area that we address. It's not currently on the agenda. But I appreciate that, and I'm happy to bring it up with the committee.

ALICE MUNYUA: Thank you. Oh, yes, U.K., please.

UNITED KINGDOM: Good morning. My name is Nick. I'm from the U.K. Mason, thank you very much for coming along. A quick question on a sort of slightly divergent topic. As part of your best practice within the HDI, are you also looking at best practice deployment of protocols that can facilitate security, things like DNSSEC and DMARC? Is that feature in as part of this study or likely to feature as part of future additional studies?

MASON COLE: Thank you, Nick, for the question. We have looked at DNSSEC and other security issues. Those are -- some of those issues are already, as you know, baked into operations with registries and registrars, so it's not an operational focus of HDI. But we do consult with security authorities to make sure that anything relevant to security is represented by best practice ideas. So I'm happy to take that concept forward as well. And I thank you for the input.

ALICE MUNYUA: Thank you. If there are no other questions, I think we'll spend the next half hour discussing quite an important issue for the GAC, privacy/proxy accreditation issues. I think this has been a sensitive topic for the GAC and for the public service working group, especially taking into consideration there's a final report that's supposed to be considered by the board. The GAC has a few concerns that were presented to the working group prior to finalization of the final report that was submitted to the -- to the board. So this -- we decided to take this opportunity to start discussing some of the concerns that were raised by several GAC members regarding some of the issues. In preparation for the two sessions we have, one that's going to be a GAC-only session starting at 11:00 to 11:30, and the objective of this session is going to be looking at those questions again, discussing them with the GAC members, and discussing the various approaches

by the PSWG and identifying some of the questions. And we are also going to try and come -- and come up with ways of approaching the joint session. But for now, I think I will let Laureen Kapin and Cathrin from the European Commission to present on -- on the issues. And we can have a discussion in preparation for the next session. So Laureen, please.

LAUREEN KAPIN: Good morning. So this is Laureen Kapin from the Federal Trade Commission wearing my public safety working group hat. For context, what I briefly want to do is give a little bit of background and then identify the key issues that we hope to focus on.

So I think as a preliminary statement, what I want to make clear is that the public safety working group welcomes the work of the privacy/proxy services accreditation issues PDP because it establishes a framework for accreditation of privacy/proxy service providers where none existed before, and there are many, many positive, positive developments contained in the recommendations of the working group. And the fact that we have some concerns should not take away from the overall very positive impact of the working group and their efforts to really grapple with a lot of difficult questions.

That said, I want to lay a little bit of foundational information for the discussion. The working group came out with an initial report and in response to that initial report the public safety working group submitted some comments that were subsequently approved by the GAC that set forth some concerns. By the time of the final report there was a final result by the working group that in some places did not accept some of the concerns that were expressed by the GAC-endorsed public safety working group comments. And the comments in the first instance reflected some public policy concerns. And so now we're here at the point where -- where these recommendations are before the board to be accepted and now is really the -- the moment where if the GAC has concerns that they want to be addressed, now is the time to set forth those concerns as advice. And the real issue is what would be the best way to handle those concerns.

So what are the concerns specifically? Within the GAC we had an excellent briefing document prepared on this issue that's labeled privacy/proxy services accreditation issues, not surprisingly, and it's agenda item nine. If folks haven't already looked at it, I would commend them to look at it because it gives a great summary of all the background and the issues. But specifically there were three issues that were identified as raising public policy concerns. The first one deals with the

confidentiality of law enforcement requests for information. When law enforcement or consumer protection authorities are engaging in investigations of criminal conduct, deceptive conduct, they may seek information regarding who is behind a domain name. And in order for those investigations to go forward, it's quite important that those requests not be conveyed, relayed, revealed, disclosed to the very target of the information. So that is -- is quite important. Because if the target of your information knows that you as a law enforcement authority are looking at them, that may have lots of negative impacts for your investigation. Evidence may be destroyed, and that could be the least harmful consequence.

Money can disappear. People can get harmed. There can be very significant consequences. And that is something that was not made a requirement in the final recommendations.

Now, on sort of a way-forward path, there is a protocol that is contained in the working group report on an analogous issue that deals with how information in the I.P. context may be handled. And there's a specific protocol for when investigations regarding infringement are going to be handled. So certainly there is a model in place that can be looked to and serve as an analogy for how law enforcement requests can be treated as well. And so this may be something that can be dealt with during implementation phase of the privacy/proxy services

accreditation issues' recommendations. There could be work done to develop a protocol to deal with law enforcement requests as well and to keep them confidential. So, that is the first topic.

Second, there's the issue of how law enforcement is defined jurisdictionally. And right now, as it stands, the working group suggests that to the extent the law requires, there could be an obligation to respond to law enforcement requests within the service provider's own jurisdiction.

The issue there, the challenge there is that we live in a world where our frauds, where our criminal behavior doesn't just take place within the confines of one jurisdiction. Often there are frauds and deceptions and criminal behavior that is taking place all over the world. You may have a bad actor in one jurisdiction who is sending money to another jurisdiction and communicating with associates in four different jurisdictions. And you may have law enforcement and consumer protection authorities who are also operating in many jurisdictions, sometimes cooperatively, to deal with these issues.

So if you have a scenario or a protocol where the service provider is only obligated to deal with the law enforcement in their own jurisdiction, that can effectively hobble the ability of law enforcement to act collectively, effectively to deal with

criminal or deceptive behavior. So that would be the second issue that we see, that that raises some problems for effective consumer protection and law enforcement action.

And then, finally, we have our third issue which deals with the question -- the somewhat many-differences-of-opinion question of whether privacy/proxy services should be permitted for domains that collect money for goods or services. And the GAC-endorsed public safety working group recommendations had advocated that public -- privacy/proxy services should not be allowed in that context.

And the rationale is that when the public provides their sensitive financial information like a credit card or a bank account number, the public has a right to know who they are doing business with. And the entity or individual behind those domains should not be permitted to be anonymous, to hide their identities behind a privacy or proxy services provider.

And that was an issue that was the subject of much debate and reflection by the working group. Indeed, in the initial report, there was no consensus on this issue. And in the final report, there was a decision that there would not be a distinction between entities that are engaged in commercial services and entities that weren't; that everyone would be permitted to use

these privacy/proxy services. So that is inconsistent with the GAC-endorsed public safety working group recommendations.

And, again, the issue on the table is what would be the way forward because as I started -- and I'm now coming full circle -- there are many, many positive developments in the working group recommendations. And I think our work here is to try and find a path forward to balance the public policy concerns of the GAC and figure out a path forward for the good work that has been done by the PDP working group to go forward and figure out is there a way to handle this that balances these interests.

And I also want to turn the microphone over to my colleague Catherin to amplify on these issues as well.

CATHRIN BAUER-BULST: Thank you, Laureen.

I think you have given a very comprehensive overview of the issues. Let me just add two points. First of all, while the three issues that Laureen has raised in this public safety working group would recommend to the GAC to further discuss are key from a public safety perspective, they are in their nature -- they do not necessitate a reopening of the process of the policy development but rather could be addressed in the implementation of the GNSO recommendations. So we think

that this is an important point. It's not going back on the process that has already taken place but, rather, can be addressed during the implementation of that process.

And, secondly, they do not -- and I think Laureen has already raised this point also. They do not call into question the really excellent service to privacy that the proxy/privacy services provide. So the general principle of affording the greatest possible privacy to the users who wish to not have any public information in the WHOIS is not called into question by these recommendations. Rather, we're calling for specific modifications to address the concerns of law enforcement for the purposes of individual investigations in criminal cases.

But now I'll turn it over to Alice because I think there will be a lot of discussion on this also. Thank you.

ALICE MUNYUA: Thank you, Catherin and Laureen. There was a question -- several questions, Switzerland and others who asked whether the PPSAI PDP, the GNSO working group, what rationale they provided in not taking into consideration GAC advice.

Perhaps we can put that slide up. I think it's titled "The rationale provided by" -- Julia -- so that everyone is able to see it. Perhaps I can start talking about it while that is coming up.

So, it says that the privacy/proxy service providers are not required to keep law enforcement agent requests confidential. According to them, this reflected comments they've received, over 1,000 comments they've received from the community. The working group, again, did not develop a disclosure framework due to authorization and confidentiality issues. That was the rationale provided.

And, also, we tend to think there was a lack of law enforcement agent expertise within, perhaps, the working group.

Then the issue of definition, which I think Catherin and Laureen has touched on. And we tend to think if the law enforcement agent definition in the 2013 RAA is revised, then the definition of the accreditation agreement would also have to be revised. And we know that this could take a while. And perhaps that's not what the PSWG is recommending at the moment. So I think we accept that rationale.

They also mentioned that they thoroughly considered the policy decisions to allow the use of commercial domain transactions to continue. And what this stressed specifically is, again, the issue of definition of "commercial activity" and "online financial transaction." And, again, mentioning that opinion reflected a large majority of the public comments, specifically focusing on

the privacy risks and the need to protect small businesses and to enable political speech.

Those are some of the rationale that were provided by the PDP working group for those GAC members who requested.

Perhaps I want to encourage a little bit of discussion here before we go to the next session. So any -- anyone with questions or additional comments, this is the time. Thank you.

Yes, Council of Europe.

COUNCIL OF EUROPE: Yes, thank you very much. Peter Kimpian from Council of Europe. I'm representing the Data Protection Committee of the Council of Europe. Just a quick reaction -- though I'm not a member of this working group, however, those topics are quite familiar also to us -- to share our views on that.

On confidentiality, I think it's less problematic than it seems for the first time because if we -- if we are referring to data protection regulation all over the world -- and currently we have 108 countries which are applying data protection regulation -- basically in all this regulation, there is an exemption for law enforcement to notify the data subject when it may bring a negative effect on investigation and so on and so forth.

So I would recommend maybe to have reference to privacy -- privacy acts and privacy and data protection international legislation which allows this kind of confidentiality if it's founded and if it's well-based.

The second issue, as we also experience, it's a bit more problematic. We come across to the same problem. The cloud evidence group, which is a group set within the framework of Council of Europe in dealing with the implementation of the Budapest Convention, the convention on cybercrime, and the sharing evidence between law enforcement authority.

Here I would like to bring your attention to make also reference to, again, international legal instruments and national ones because there is the Budapest Convention which allows to a certain extent that kind of sharing of evidence between law enforcement authority.

But, for example, to give you a very basic example that if a French authority -- law enforcement authority would like to have some evidence from a Finnish service provider under European law, it would be impossible. So before -- and I know in other jurisdictions, this problem exists.

What we are encouraging in our -- in the framework of Budapest Convention is to have a better and a smoother cooperation within law enforcement but is within law enforcement players to

share information by using existing tools among each other. So these are the reflections I have and I wanted to share with you at this stage. Thank you.

ALICE MUNYUA: Thank you. Any other comments? Yes, Indonesia and then Spain.

INDONESIA: Thank you. Just curious to know more about the scope of the PDP working group studies. Do you also include public personal data that was submitted to the operators? And what if the law enforcement agencies would like to get that kind of information?

For example, I mean, Google Maps, for example. My mobile, when I buy it, there's already Google Map inside. I just activate it when I want. And the operator certainly knows where I am, where I'm located at the particular time.

Does the law enforcement agencies have the access to that more or less public information data like that? Because by doing -- by getting this data, the Google operator, for example, can even know whether I'm moving very fast or slow and whether that road is red or is -- what you call it -- jammed or not, you know, things like that.

How can the LEA, like my friend Bob, can have access to that, for example?

And of course others. That also applies to others, you see.

At least we have now high-resolution satellites that can see my house. We have many others. We have stratosphere-based apps being discussed now in the ITU, and tomorrow it will fly above my house and see whether I'm taking a bath or not.

[Laughter]

INDONESIA: So I just want to -- curious to know, this will -- this will happen in three or four years' time, and I would like to know that stratosphere-based access that will be located in -- you know, above my home. Thank you.

ALICE MUNYUA: Bobby?

BOBBY FLAIM: Hello, my good friend. No, I think what we're talking about here is totally separate. This is just proxy/privacy services for domain names, so this is the very strict and limited scope that we're talking about. When you're registering a domain name, whether you want that information to be public or private, and if you

want it to be private or proxied, you know, you would pay the additional fees that would hide your information.

ALICE MUNYUA: Spain, please.

SPAIN: Thank you and good morning. I have three points to make.

As regards the confidentiality requirements, I would like to support what my colleague from the Council of Europe has stated. At least in European jurisdictions, data protection laws provides for an exception to the consent of the data holder to -- for authorities and prosecutors and public administrations to demand data from third parties without having to get prior consent from the individual.

And the reason why I think is the individual will have an opportunity to see all the evidence gathered and to say something in -- to defend himself later in the process, so he won't be defenseless.

The only thing we try to avoid is that person destroying evidence and all of that.

My second point concerns one of the rationales given by the working group for not disclosing data, for not -- for not

prohibiting commercial activities from using privacy services. They say, "Well, if courts require the data, we will hand them over."

I would like to recall that in some national legal traditions like the ones in France and Spain and other countries, administrative authorities have authority to pursue public -- public policies and to enforce laws. This is especially in the area of consumer protection. Consumer fraud and consumer protection are mostly dealt with by administrative authorities, not courts, and they have all the powers to enforce legislation.

So when we say "courts" here, we should be aware that some public authorities couldn't have the chance to have recourse to courts because their national legal traditions don't provide for that.

And my third point is to recall that the GAC engaged early in the work of the working group. The GAC provided comments at an earlier stage and they haven't been taken into account by the working group. They have provided rationale, but in the end the result is that they were not taken into account.

So there is a chance that in the implementation phase, they are turned down again.

For that reason, I think that if the GAC is going to provide that kind of advice to tackle GAC recommendations in the implementation phase, there should be incentive for the GNSO, or whoever is working in the implementation phase, to really take them seriously now, and for that reason I think what has been specified in the draft advice for GAC is good, is fair to tell the board, "You should order or kind of give an order to the implementers to take this seriously and find a way to accommodate those recommendations." And if they are not incorporated in the implementation phase, then the relevant recommendations, the ones that relate to these, have to go back to the board.

Thank you.

ALICE MUNYUA: Thank you very much, Spain.

I have the U.K. and then Canada. U.K., please.

UNITED KINGDOM: Thank you, Alice.

A couple of points.

I'd like to sort of welcome the comments that Laureen made earlier. We don't want to hold this thing up. We also recognize

that it's important to get the accreditation in this area. I was interested by Cathrin's comment about some kind of review during the implementation phase of these recommendations.

Has there been any sort of further consideration of what form such review might take, and have we received any informal feedback from members of the GNSO to that idea or have the GNSO -- this is one for Mason -- have the GNSO also sort of considered how they might collaborate with the GAC in such a review?

Thank you.

ALICE MUNYUA: Thank you, U.K. If you'll notice, one -- the advice we've proposed here is for some of the GAC considerations and concerns to be taken into consideration during the review, but I'll let Mason speak to the issue on whether or not the GNSO has considered how they may approach some of the concerns that have already been raised by the GAC. Mason?

MASON COLE: Thank you, Alice.

The GNSO is aware of the GAC -- of the GAC's desire to re-review this issue. There's a meeting between the GNSO and the GAC -- I

believe it's tomorrow -- where I think this is going to be addressed. I don't think the GNSO has fully formed how it's going to approach the GAC's ongoing desire to address this issue, but I know it's a matter of consideration right now.

ALICE MUNYUA: And we do have a joint session with them to discuss these issues further.

Cathrin, you want to respond to the Council of Europe?

And then Canada.

CATHRIN BAUER-BULST: Yes. Thank you, Alice.

Just to avoid misunderstandings, first of all, I fully support what Gema already has said and what the Council of Europe has correctly stated, that the data protection framework is no obstacle to our first recommendation to the GAC.

And then on the second recommendation, the concept of responding to requests not just from a law enforcement agency that is established in the same territory as the privacy/proxy service, I would just like to remind participants that we are talking about two very different categories of legal frameworks here.

The one that you refer to, the Budapest Convention, is implemented through criminal procedural laws and has an impact on the enforceability of such requests.

What we're talking about here is to avoid that in a protocol, such requests are already excluded in the protocol to the implementation of a contract.

So such requests, as you're probably aware, are already being made for all other sorts of information that can be provided on a voluntary basis, and I'm speaking from the perspective of the 28 E.U. member states here, where -- to the -- to the understanding that we have on the basis of the transparency reports of major providers, such requests are being made on a voluntary basis for all sorts of evidence such as subscriber information and the question then is whether or not those requests are enforceable through authoritative means.

So really, we are talking about two different categories here and I want to be very clear that there is no legal obstacle, per se, to the recommendation that we are making on the procedural implementation of contractual arrangements. Thank you.

ALICE MUNYUA: Thank you, Cathrin.

Canada and then Switzerland. Then I'm afraid we'll have to close.

Canada, please.

CANADA: Thank you very much, Alice. And thank you, Laureen and Cathrin, for your presentation.

We certainly recognize that law enforcement needs to have access to effective mechanisms in place to obtain lawful access to WHOIS information, and we also appreciate how important accurate and reliable WHOIS information is to fluid ongoing investigations.

The work on privacy and proxy accreditation services received an unprecedented amount of interest, with over 10,000 comments being filed, and the final report is the conclusion of a rigorous multistakeholder discussion over a two-year period on a complex and multifaceted issue. It was informed by a diversity of perspectives, including privacy, small and medium-size businesses, intellectual property, law enforcement, and consumer protection, and I think there is a sense of urgency here in allowing this work to move forward.

We understand that specific -- we understand that there is a specification in the registrar accreditation agreement that deals

with the collection of WHOIS information and that this is set to expire in January of next year, and the work undertaken wasn't done to serve as the basis for replacing this specification. However, this is contingent on it being implemented.

So in light of these various considerations, Canada supports the report moving forward. We agree, certainly, that if -- if there is an opportunity to address the most pressing concerns of the GAC public safety working group, we should explore this during implementation, provided that, as Cathrin has mentioned and as the U.K. has also mentioned, that it builds on and does not undo the work to date.

However, we would not want this to serve as grounds for the GAC public safety working group to sort of indefinitely hold the report until we're satisfied with the implementation.

Thank you very much.

ALICE MUNYUA: We have Switzerland and then there's a remote participant. Switzerland, please.

SWITZERLAND: Thank you very much, Alice.

I think that the --

Well, first of all, thank you for the very good brief with -- in its final form with the rationales. I think that gives a very good overview about the history of the question.

I just want to secure clarification because I've heard some expressions which perhaps might be not completely consistent, or I'm not sure whether I've understood everything well, because in presenting the issues, there was mention that some of the recommendations are inconsistent with GAC advice and then as -- on the possibilities of finding a compromise in the implementation, there was a mention that there might be difficulties or more difficulties in some of the issues.

So what I would like to know is whether you have more information, especially on the side of ICANN, ICANN staff, or the GNSO people who might be in the implementation review -- implementation team, whether they -- what's their assessment on how our recommendations might be reconciled during the implementation phase with their recommendations.

So that's, I think, very important in order to be sure that we are going down that path of focusing on reconciling everything in the implementation, but only if that's feasible, to a certain extent, because if there's no willingness to really reconcile that, we would end up with an implementation work which is inconsistent with our recommendations and this would be

counterproductive to the common understanding that we want this work to move forward as fast as possible.

So -- And related to this, I've seen in the draft advice that we would be recommending the Board that the GAC and the Public Safety Working Group is consulted, but I wonder whether we even could recommend them, suggest them that somebody from the Public Safety Working Group -- and I know this is more work -- is included in that review team because that would smooth things a lot.

Thank you.

ALICE MUNYUA: Thank you very much. And just to respond to Canada and the concerns, the Public Safety Working Group is not in any way advising that we hold up the process of the Board considering the final report. I think what we want to consider during the joint session to respond to the question from Switzerland, we have a joint session with the GNSO and the ICANN Board to discuss the way forward and how some of the GAC concerns could be addressed during the implementation phase. Whether or not and how they can be addressed.

Now, I have the U.S., United States, and then Australia, and then I think Mary Wong. And then I do think we need to look at the GAC advice of the PSWG to see if we are okay with it.

So United States first.

UNITED STATES: Yes, thank you very much. I just wanted to concur with the comments that were made previously by our Canadian colleagues as well as some comments made by our Swiss colleague in that I think there's so much positive coming out of what the PDP has recommended already, it would really be a shame to in any way hold up that kind of progress.

So when it comes to, I think, having a constructive dialogue with the GNSO to the extent possible of trying to find ways to address the outstanding concerns to implementation is a great way forward. The concept of somehow sending back any recommendations, and my interpretation of that is that could somehow potentially hold up the approval of the recommendations. I see as an alternative to that having a continued dialogue with the GNSO to perhaps, in the future, if there's opportunities to enhance the accreditation process for privacy/proxy services, that's a more, I think, productive, constructive avenue moving forward.

Thank you.

ALICE MUNYUA: Thank you, United States.

Australia.

AUSTRALIA: Thank you, Chair. I'll be very brief.

I see tomorrow we have another Public Safety Working Group session that is a closed meeting. I just wanted to make the general observation that GAC working group -- or the other GAC working groups are all open. All GAC sessions are open, and even our communique drafting sessions are now open to other members of the community. And just as a general principle, I think the Public Safety Working Group meetings should be open as well.

ALICE MUNYUA: Well noted. Thank you.

Yes. Remote, please.

UNKNOWN SPEAKER: Thank you, Alice. I just wanted to note in response to Jorge's comment about whether the recommendations from the GAC

and the PPSAI working group were consistent or inconsistent; that out of the three issues, issue areas, there's one for which the GAC advice is inconsistent with the recommendations of the working group, and, therefore, that one could not be implemented as the GAC recommended. So there would need to be work-around.

So this issue is the -- is the issue of whether or not commercial providers providing financial services can or cannot use privacy and proxy services. So there could -- They started to discuss possible ways to address, rather than to address the underlying issues that the GAC has, which is that these providers could be hiding criminals and not responding to law enforcement requests. So by developing a de-accreditation system for those providers.

ALICE MUNYUA: Thank you, Julia. I think we may want to consider -- if we could put up the slide on GAC advice, proposed GAC advice, so we could consider that as a....

Okay. As you can see, the Public Safety Working Group has proposed language here that will probably need to be considered. The first one being I think what Julia has mentioned here, the possibility of....

Yes, we have very little time.

The idea of framework, the framework for law enforcement, continue dialogue, as has been mentioned by quite a number of colleagues. And then the possibility of exploring how some of the GAC concerns could be addressed during the implementation review, and feedback sought out as the implementation process continues.

So some of these other recommendations, I'm sure we'll have time to discuss this during the communique drafting session. We now have to go to the next session, and I think -- I would like to close this and hand over to the GAC chair to take us through the next session.

Thank you, everybody. Thank you very much for the very constructive discussions.

OLOF NORDLING: And this is Olof Nordling. ICANN staff, in support of the GAC.

And I would like to remind those of you at the table who are not GAC member representatives or GAC observers to please give priority to the GAC member representative so they have access to the mics for the upcoming plenary session which is due to start in a few minutes.

[END OF TRANSCRIPTION]