ICANN83 | PF – GNSO: ISPCP Membership Work Session
Tuesday, June 10, 2025 – 10:45 to 12:15 CEST

BRENDA BREWER: Thank you. Hello and welcome to the ISPCP Membership Work Session on Tuesday, the 10th of June, 2025. My name is Brenda and I am the participation manager for this session. Please note this session is being recorded and is governed by the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy.

If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom, and the on-site participants will use a physical microphone to speak. Please state your name for the record and speak at a reasonable pace, and I will now hand the floor over to Philippe Fouquart, ISPCP Chair.

PHILIPPE FOUQUART: Thank you very much, Brenda. Good morning, everyone. This is Philippe Fouquart, speaking as the chair of the constituency. I think we all appreciate that this is going to be small team today just to give you a bit of background. So today is traditionally Constituency Day, but given the four-day format of the meeting, we have two conflicts.

There's an ongoing GAC-GNSO Council meeting at the moment, which the councilors have to attend, and this afternoon during the informal council meeting, we have the ICP-2 bilateral with our ASO/AC colleagues, so it means that in practice, we can't discuss much policy issues today. So, just as an introduction to the meeting, but hopefully next time we'll make sure that this doesn't happen again.

This being said, welcome everyone to our ISPCP session today. We've got a couple of interesting and important topics on our agenda. I just want to make sure that, as usual, the statements of interest are up to date. Any update that people would like to make? Okay, seeing none, any update to the agenda or notes as additions to the AOB? Christian.

CHRISTIAN DAWSON Thank you, Christian Dawson, for the record. I'm looking to put in AOB a note about a session that I am helping to facilitate today at 5:15 around the newly forming Coalition on Digital Inclusion.

PHILIPPE FOUQUART Thank you very much, Christian. Anything else? Christian again.

CHRISTIAN DAWSON A second thing, when we do talk about DNS abuse, I thought we should surface the NetBeacon Institute's recent white paper, Proposals for DNS Abuse.

PHILIPPE FOUQUART

Absolutely. Thank you. Thank you, Christian. There are indeed several parallel, somewhat overlapping threads in the discussion about DNS abuse. We'll say a word about that. There's been a lot of talk within the CSG on this. There's somewhat of a proposal as well. I don't know how much backing there is on those respective approaches.

Most of them, they're not incompatible, there are differences, but we can have that discussion later on, it's an important one. And coming back to my initial point, that is one of the hot tops for discussion on the policy side of things at council, and unfortunately, it's on the informal council meeting this afternoon, and our councilors are not here. There we go. Anyway, as I put in the email, there's always so much we can do.

And just as a note on the agenda as well, you do not see anything on the SSAC paper on DNS blocking, which we referenced. I think, last time I asked for a speaker, no one was available for that same reason because of the other conflicts. I would encourage you to have a look at the latest version of the paper. Maybe we can have an introduction to it at one of our next calls, that would be a good idea. We'll see. But as you all know, that's an important topic for ISPs and telecoms operators as well. Yeah.

CHRISTIAN DAWSON: Apologies, I have something to interject here as well. I would also like to, and I'm going to put this in the chat, to call to attention a recent campaign that my organization started. We are attempting to be an organizer around U.S. Pushes for DNS blocking.

And to do so, we are trying to document cases of DNS blocking around the world and specifically where they have resulted in overblocking. So we wrote a 50-page report with 13 case studies on overblocking in different countries around the world, including the United States, and launched a website called dnsatrisk.org. So I encourage people to take a look it.

PHILIPPE FOUQUART: Thanks, Christian. And maybe in addition, maybe in addition to the chat, would you mind posting this on the list just for people to have the reference?

CHRISTIAN DAWSON: I would absolutely be happy to. And I'm also looking forward to talking to you about France later.

PHILIPPE FOUQUART: Sure, and other countries as well, I'm sure. But it is indeed in France and in Europe, under the, say, the lawmaker's scrutiny on certain types of content. This being said, I think we can go through the first item, which will be very quick, not only because we don't have our counsellors today, for the reason, I said, but also because this is one

of the council meetings where, given the nature of the issues at hand, council devotes their time to discussion and not votes with the exception of the consent agenda, if there were opposition, to what's proposed here, obviously we'll just send a note to our councilors.

I just want to make sure that regarding item 3, people are comfortable with the deferral of the WHOIS Implementation Advisory Group moving forward. This is normally an uncontentious issue. This has been on the table for a while. At this point, and let's say by default, councilors would not oppose it, as we see as council, given that it's a consent agenda item. But I just want to make sure that people are happy with this. Okay, I see people nodding.

On the other items, and notably, on DNS abuse, we'll say we have, I think, it's not an item, but on the CSG and CPH update, we can have a discussion about that particular item. Beyond the question of how, in terms of form rather than substance, how procedurally we approach this, which is the issue that council will be discussing. There is a small team, you would remember at council. There's been a small team for a while since at least recently to 2020, which has been reinitiated a few months ago.

So with this, I think we can go to item three. That's the presentation on DNS for you from colleagues from Whalebone. Thanks very much for joining us. This is a project that has been of interest to a number of ICANN participants. I seem to remember that there was one presentation at some point. I forget what that was, but was

that three, four meetings ago, which led to an interesting discussion?

As an employee of a European operator, I am somewhat familiar with that, but I'll leave you to give the context and assume that people here would not remember the funding, et cetera. So that'd be great if you could remind people you have. We said 15 minutes, but given that we had items which we could not fill, feel free to use 20 or 25. I think people will want to go out of this session with as much information as possible. So don't feel limited by the timing here. With this, the floor is yours, and we'll go to questions after that.

VILIAM PELI

Thank you so much. Viliam Peli, for the record. I'm from Whalebone, and I'm here for the first time. Okay, next slide, please. Okay, so I believe every one of us, at least for once, have received ever a suspicion link via SMS, email, messenger or any application. Or you have felt unsafe to visit a new website that you haven't seen before. Or scanning a QR code that you are never sure what is behind the QR code. Or you have suspected that your devices is slowing down for some reason, or you don't know where the data are going.

Next slide, please. Well, in Whalebone, we have a solution for that. We can protect any device that is connected to the internet. It can be your car, it can be your mobile phone, your fridge, anything that is connected to the internet, and we make sure your device is

protected without needing to install or maintain anything on the device. This is because our solution is being run on the DNS resolution. This is why you don't have to download anything.

And from the threats that you can see or you have on the DNS resolution, we block all the types such as scam websites, malware, trojans, malicious con miners, fake phishing apps, fake messages of phishing links, the botnets, command and control, which is quite popular these days, DGAs, compromised websites, and everything like that. Next slide, please.

My name is Viliam Peli, I'm threat intelligence lead at Whalebone, and today, I'm going to talk about the threat landscape and threat intelligence that we do at Whalebone to protect our users, ISPs, and everyone. In today's landscape, what I like to say always, the speed is everything in this world. It's not just about identifying threats, but also stopping them before they can do any harm. And thanks to the regional intelligence, that we are focusing on these days, it gives us the edge to stop them before they can harm anyone.

Next slide, please. So, who is Whalebone? We are a company based in Brno, Czech Republic, and we are creating a DNS security solution for telecommunications, ISPs, CSPs, governments, and any enterprises, critical sectors, and also for the public with our project DNS4EU that I have been speaking the last time, and I'm going to talk about the updates later on. Across the globe, we are a trusted cybersecurity partner, and we have also one of the best DNS security solutions on the market. And why am I saying that?

Next slide, please. It's because AV-Test, which is Independent Security Research Institute in Germany, every year, it is comparing us against other DNS security solutions for telcos. And every year, we have the best detection rate of malicious websites and threats, and we have the lowest false positive rates of benign domains that we actually don't block. Next slide, please.

And I'm going to deep dive a bit into the thread intelligence. How do we do the thread intelligence at Whalebone? Well, we combine multiple pipelines, our own in-house malware research and analysis, where we have multiple algorithms, machine learning models, our own techniques to find new threats. Then we have the DNS traffic from the customers, which we evaluate and we go through.

We can see multiple new threats on the DNS traffic of the internet as well. And we have multiple external sources, thanks to the cooperations that we have, such as the National CERTs that are providing us the regional threat intelligence within their country or region. We have multiple cybersecurity research vendors that are helping us, university institutes, cybersecurity experts, antivirus vendors, and multiple other sources that are helping us creating the best cybersecurity solution for DNS security solution.

And we gather all these, we collect them, we parse them, and we process them. We enhance the data with all the tags or every data that we can find for such threat or IOC. We enhance the IOC, and then we evaluate it with our multiple scoring systems to evaluate if

such threat is actually a threat or it's a benign domain. For example, we have a traffic analyzer, our own white list bot that has the records of benign domains, we check the name convention of a domain.

We have a really great DGA detector, which is currently a really huge topic because of the enhancement of AI. The threats are becoming much more hard to detect, they have really short lifetime, and you have to detect them before they even emerge to the Internet. And we also have our own domain intelligence for multiple domains, either if they are benign or malicious. And then after we evaluate it and we say it's a malicious domain, we quickly send it to all the resolvers for the DNS resolvers so all the customers and everyone can be saved from such threat.

And, of course, we iterate all over it, we re-evaluate it all the time so we have the most recent updates for each threat or domain. And also, we collect feedback from our customers if they think there is something, some false positive, or they think we should block something. Okay, next slide, please. And just to quickly overview from the high level, how are we on the global scale of threat intelligence, over the past month, we have blocked 3.8 billion accesses to malicious domains across the whole globe, which saved so many customers and people all over the globe.

And we currently hold over 27 million, currently, as I checked yesterday, unique malicious domains, which are active. We have much more that are inactive currently because they are not

malicious anymore. And our database is growing every day, with over 350,000 new domains that we add to the database. Next slide, please. And for the case study, for our telco customers and ISP customers, we create custom reports, what is going on inside their network, what can we see, what kind of threats?

Recently, we have been doing a report for one ISP. This is pretty common scheme that is pretty popular these days, and those are the free movies or the copies of, let's say, Netflix, Amazon, or whatever movie vendor you watch. And the streaming website, this one, exactly had an issue where if you wanted to check or watch the movie, it actually had the movie. But behind it, when you clicked on it, it redirected you to advertisement, which started 13,000-line Javascript from a Russian domain.

And the script itself was monitoring the HTML forms, it was identifying passwords, your personal data, financial data, and it was sending them straight to their domains, to their databases, which was really cool from the point of thread intelligence and the malware, this script could also work with multiple languages, alphabets, which is not normally usual within the threats. Thanks to our solution, we have blocked thousands of accesses within that exact ISP to this streaming website, so our customers, the people using the ISP network, were safe from such a threat of such a malware advertisement, and we protected their data.

Next slide, please. I was talking in the beginning about the regional threat intelligence. Why is it popular? Why do we think we should

be talking more about it? It's because the landscape is quickly evolving, it's shaping every year, and currently, we can see the trend of the APTs and threat actors to regionally focus their malware, their threats, where it's more sophisticated, it's harder to recognize it, it's almost the same as the valid domain, and we had to combat this as well.

For this, we have a special regional threat intelligence team within the Whalebone and, for example, the pipeline, how the process works is at the beginning. For example, this is USA example, where we did example for United States Postal Service. We have gathered all the information about the USPS, then we even gathered the information about previously known malicious attacks for such provider. We have checked all the detections for the USPS, the phishing campaigns.

Next slide, please. We collected all this data, we processed it as we usually do. It should be the 11th slide. No problem. We collected all this data, we processed it, we enhanced the data with our own domain intelligence, and we also analyzed the metadata that we could see for each domain. We checked the context of such domain and also the behavioral analysis of each domain, each regional threat. And then we decide if it's either malicious or benign.

So for each region, we create a custom thread intelligence of such region, what are the most popular vendor's websites, and we create a special domain intelligence just purely for the vendor in

each region. Okay, next slide, please. About the DNS4EU, I've been speaking about it--

PHILIPPER FOUQUART I'm sorry to interrupt, but maybe before we get there, since there are sort of two parts in your presentation. Do you mind if we stop here and see whether people have questions?

VILIAM PELI Of course, yes.

PHILIPPE FOUQUART I might have a couple of questions, but any questions from the room? Yes, Anil.

ANIL JAIN Anil for the record. Thank you, Philippe. Very good presentation, and I find that the software which you have is a combination of several solutions, which people are looking especially for the DNS abuse. My question is, as an ISP, when we use the traffic analyzer, in my term, taken from you, how it helped to identify whether a particular customer or a particular domain is becoming malicious, or there are some external DNS threat which is happening to that?

So this is my first question, which I want to get it clarified. Second, you said that you are identifying malicious domains through your system. Now, suppose I have a domain, I am a customer of a ISP

and I have taken a domain, and my domain is now categorized as a malicious domain. Now it is not, because I am not doing anything wrong.

So how your system informs the ISP and how ISP inform the end customer that this kind of report is coming and how to correct these kind of things so that end customer do not get harassed without any reason. Thank you.

VILIAM PELI

Okay. Again, Viliam Peli for the record. So first question was, if I understood it, how do we know within each client, or within each customer, if what kind of threats are there, right? That was the question. Well, we have, for each customer, we have the admin portal, which is their front end, where they can see all the traffic that is going through their resolver, all the logs, all the malicious data that are currently going through the resolver, which is also anonymized.

They cannot see the customer, they can only see the traffic going on there. And for each customer, we create a custom report where we look at the data that is going there, we look at the what kind of threats are going there, and then we compare it with our domain intelligence that we have, and we make more in-depth report for them. And for the second question, can you please repeat it, I sorry?

ANIL JAIN

My second question is that suppose your system identifies a particular domain as a malicious domain, right, how you inform ISP and how ISP informs the end user? And what kind of conversation, or what kind of resolution which can be brought to make that malicious domain into a good domain?

VILIAM PELI

Okay, thank you. Well, if we identify maybe a benign domain or your website, we decide it's malicious, usually it's because it's running on WordPress, on really old, let's say, updates, and we can see some malicious data in there with the URL. In case we actually have a false positive, what we have is our ticketing system, where the customers, okay, the customer opens the website, it says this domain was blocked because it was malicious, we even state what kind of threat type was it.

But what can they do is they can actually skip it, and they can still visit the website always if they decide to, and they can also click on the report button. So they can report it as a false positive, and it immediately goes to our ticketing system, and our colleagues are resolving that within a day. So we check it manually, we evaluate manually the website.

If it's actually benign, if it's not malicious, we deactivate it and we send the message to the customer. And we usually even state why we thought it's malicious. Usually it's because previously it was

malicious, currently it's parked, but the evaluation process didn't start yet for the current update of the domain.

ANIL JAIN

Yeah, thank you. Before I go, just one more question. When you are using traffic analyzer as a ISP, how your traffic analyzer is helpful in upgrading or downgrading or modifying the infrastructure which an ISP has based on the results of the traffic analyzer as a whole?

VILIAM PELI

So about the end customer portal and the graphs? This goes to our technical consultants. I don't work with them. Maybe, Lorenzo, do you have any comment on this?

LORENZO BRACCI

Can you hear me? So the deployment of Whalebone for ISPs is very easy and fast. It is a hybrid solution which is leveraging one part, which can be deployed into the ISP premises, and there is also the cloud part. 90% of our customers like to deploy it on their premises, of course, because they get full IP visibility, faster connection, lower latency, and they're independent from the cloud.

And it is very easy, it's just matter of doing Piston copy one script, having one VM where they can launch it, and that's about it. And in case some customers don't have a VM or bare metal, they can just use the cloud resolver. So it is a very easy and fast way to protect

people and their infrastructure at the DNS level, and it can be integrated with other solutions they are using, firewall and so on. I hope I answered the question.

PHILIPPE FOUQUART: Thank you. Thank you, Anil. Did you have, if you would, just state your name? It's an open session, so you're very welcome to ask questions.

UNKNOWN SPEAKER: My name is [00:31:01 – inaudible], I am from At-Large. You made some very strong claims here. You said, for instance, that you will protect devices or customers from any threat, which will happen possibly, and you react very quickly, and you can react to overblocking or a wrong claim. If I see our customers, I'm working for an ISP, there are some enterprises who have the problem with their cyber insurance and they said, do something.

It looks like your solution might be a good idea to add, but next question I have, or they have, is, if something goes wrong, can I sue you? If I get ransomware in the enterprise and I had a protection, the cybersecurity insurance will go and say, oh, you had a protection claim that there will be no threat anymore and now we have a threat, can insurance come to you and get the money back? The next point from the ISP question.

PHILIPPE FOUQUART Let's just take the question, if you don't mind, one by one. I would just add that, just to frame the context of your question, I think the first part of this presentation is the service to an ISP, it's not the Open resolver. So the assumption is that there's a contract between the ISP, which will not be the case for the second part. I just want to make sure that people have that at the back of their mind, but it has an impact on, I think, on the answer. So would you?

VILIAM PELI Yes, so basically what I mentioned at the beginning were that we detect all threat types, not all threats. Because in the real world, there cannot be a product that can detect all the threats in real life. So for the record, we detect all types of threats, we do not detect all the threats on the internet.

But, as I said, the AV tests, which is independent research, are mentioning every year that our product, compared to other DNS security solutions, has the best blocking rate of actual threats on the internet. And I'm not sure what was the second question.

PHILIPPE FOUQUART Yeah, the liability question. Can the customer, the enterprise, actually "sue you," given that there's a contract between you and the ISP, if, say, a domain was not blocked, whereas it may have been known as being a spot for botnets or something?

VILIAM PELI

Yeah, in case we have detected such ransomware, we even have a custom threat intelligence within the resolver. The customer can set from which score they can set the blocking. So in case they set it too high and they don't block enough malware, which we can see in some customers, they didn't want to be more strict, they want it to be more free, then, yes, we wouldn't block it on their resolver.

But we can actually show them that if you would, usually the sales or CSM experts from our company show them that if you would just lower the score of which you will block, then you would block actually much more threats that are coming. And about the law, I'm not really sure if somebody has ever sued us before, and I'm not the contract guy, so I'm not sure.

PHILIPPE FOUQUART

But that's an interesting question. The liability question is a good one. Ultimately, my personal take is that it's going to be like a legal dispute. But it's a good question, say, for example, if that domain name is so well known that most, if not all, public resolvers and DNS resolver providers actually block that domain name, whereas you wouldn't, for example, just for the sake of the argument, and then that enterprise is harmed for that reason. Are they in a position to sue you, I guess? You have a liability issue, certainly, you're a provider, the DNS operations is outsourced to you by the ISP, so you're responsible.

But ultimately, I guess that's going to be a legal dispute coming back to your note about the rates. Whether the responsibility lies

with the ISP because the rate or the threshold was too low, or whether that was your responsibility because the sources of your blocked lists were not those that most of the others would rely on, and it was so obvious that such a domain was a source of botnets, whereas you didn't block it.

So that would have been your responsibility. I guess, ultimately, I'm not a lawyer, bear with me, but I've seen those things. Ultimately, that's a legal dispute, and you'll be probably between you and the ISP sort of try to swing the responsibility on one side or the other. But that's a fair point.

VILIAM PELI

If I can add one more thing. With our customers, we are constantly speaking, our CSM experts are visiting them, and we usually create best solution for them because we also check what kind of other solution, security solutions they have, what do they actually are seeking, how can we ideally set it for them to be like the best practice? And we usually show them within the reports what they have missed, what kind of threats they had.

And if they have any issues, then we can also check on it, we can focus on some special threat that is coming straight from their country, we can focus more on it, we can also change the threshold anytime. So everything is here about the customization, what the customer wants, and also we try to tell them how to make it better. So if the customer says, I want the threshold to be set much higher,

I don't want too many blockings, it's not really our problem if there is a ransomware or something that we would actually block.

PHILIPPE FOUQUART Thank you very much. You had another question, maybe?

UNKNOWN SPEAKER Yeah, a lot of technical questions, but we can postpone them. I have a question for my At-Large community. How about privacy? You get the deep insight into the communication details and metadata of each customer of the ISP. You claim that it will be unannounced, but you have the possibility to select it out. So, let me rephrase the question to, how many requests from a lawful agency do you have regarding hand me out something about this guy, I want to know more about them.

LORENZO BRACCI Yeah, so the Whalebone and the product we make is fully JDPR compliant, and JDPR is this one of the strictest law about data protection and privacy that are there in the world? Later on, I can also share with you, like the legal things we have regarding data privacy. And from what I know and recall, we are not data processors, so we don't work with the data whatsoever.

And we had several cases of ISPs that were concerned about the topic. I remember one ISP in Norway and a couple of customers in Italy, and in that case, we have the possibility to anonymize the IP

addresses because that's what we can see from the portal, for instance, in order to enable this higher level of respect. So it is general answer, but I can provide you later on more information to clarify any issue.

PHILIPPE FOUQUART

Thank you. I suggest we go to the second. I have a couple of questions, but one of them is arguably equally related to the second part. So let's move on to the next slide.

VILIAM PELI

Please. So the DNS4EU part will be pretty short because I have two small news, but they are actually like two short news, but they are actually huge. So about the introduction of DNS4EU, in case somebody wasn't here the last time. So, DNS4EU is an initiative by the European Commission with the goal of providing private, safe, independent DNS resolution for European citizens within the whole European Union, and also for the governments and institutions as well.

So, DNS4EU aligns with the European Union vision and the digital independence by providing alternative to the existing public DNS service. Usually, they are offered by major non-EU tech companies, and European Union doesn't know where the data goes. So they usually go abroad, usually to America, but we don't know what do they do with the data. Some tech companies are even stating that

they are reselling the data that they get from the citizens by providing the free DNS resolution and the security.

What makes DNS4EU special is that the data will always stay within the European Union, and it's also strict under the EU law regulations. And we ensure the privacy, that the data are not misused, and everything is also anonymized. So we are the consortium leader of this project as Whalebone, and we have multiple universities, law companies, also some DNS companies, so many other huge companies within the consortium that are helping us developing this project to bring safe browsing for the European citizens.

And for the news that I have for the DNS4EU, next slide, is that I have the map of 14 resolvers that are being deployed within the European Union. This will be the starting resolvers, maybe in future we will have much more. We will be collecting all the feedback that the people will send us. We already heard some feedback they wanted to have it in a specific country. So this will be shaping in future, but for now, this will be the first 14 free DNS security resolvers, publicly free for everyone within the European Union.

And I also have a date of the public launch for everyone, which is actually tomorrow. So tomorrow, we are launching all of these 14 resolvers to be publicly open for everyone to test them, try them. We also have a special ticketing system for DNS4EU. So feel free to try it, give us your feedback, and we will happily shape it to be

better and better in the future. So that's it, from my side, from the DNS4EU.

Next slide, please, also. If you want to check the DNS4EU, if you want to try it yourself, use joindns4.eu, and you can see more information how to connect to the resolvers and be protected. And that's also everything from my side. Next slide. Feel free to connect with me if you have any questions related outside, feel free to talk. Thank you so much for being here and listening. Thanks.

PHILIPPE FOUQUART: Thank you. Thank you for coming. That's very useful. Just a very simple question. If you would put, I think you're on the Zoom room, if you could put the public IP address for the countries in the chat, that would be great.

VILIAM PELI: I'm not really sure about the correct IP address. So, Lorenzo, do you have it?

PHILIPPE FOUQUART: You probably have it.

LORANZO BRACCI: Yes, we do. So we have several IPS for several blocking. So, if I recall correctly, there is one IP just for security, so threats will be

blocked. There is one just for pure resolution. There is one IP for child protection and maybe one for ID blocking. But I can share it.

PHILIPPE FOUQUART If you could put the URL, if not the public IP addresses, but the URL in the chat, that would be great.

VILIAM PELI And also one thing to mention, we also have an IP address for advertisement blocking, which was already tested by the beta testers and the people that were joining the DNS4EU. We so far collected really great responses and feedback for the advertisement detecting and blocking of advertisements.

PHILIPPE FOUQUART Okay, thank you. Thanks very much. Any other questions on this part? I have a couple of questions. One is very simple. In terms of blocking, the sort of technical blocking, there's a paper from SSAC that discusses the various ways, good ways and bad ways to implement blocking, like lying, as we say, sending back NX domains, which is the bad way to do it, well, sort of.

I was just wondering how the way you do it actually maps onto the various options that are in that, I think it's 127 or something, that report on DNS blocking, whether you had given some thoughts on the consequences of the way you actually do DNS blocking.

VILIAM PELI

Yes, so it's actually the same solution as Whalebone, but also to clarify, this is customized. The main part of the DNS4EU is to also connect all the regions, all the cybersecurity National Certs to cooperate together. Because currently, me personally, I was in contact with every National Cert within the European Union, and we can see the huge differences within each of them.

And there are some cooperation with some countries that they have, but some countries do not share or have a cooperation with anyone. And thanks to the project, we are shaping the collective threat intelligence of European Union, where we take all the national threats, bring them together to be put into the DNS4EU so they can also cooperate together, they can send us the regional data that they have, so we can protect from every regional emerging threat that the threats have so we can protect every European citizen from it.

PHILIPPE FOUQUART

Thank you. Well, we can take that offline. My question is more about sort of the technical DNS protocol standpoint, but that's fine, we can talk about that offline. I have a more overarching question, if I may. Coming back to Christian's note very early during this session, there are legislations in Europe regarding DNS blocking and content blocking in general.

Just for argument's sake, and only recently, there was a decision in France, for instance, to block pornographic content material for kids, which will probably end up being implemented on DNS resolvers for ISPs. And for the record, we abide, as I usually say here, we're good law-abiding people, that's what we do. But you have a sort of a different approach since you're sort of pan-European.

So say, for argument's sake, if there is a ruling in one country regarding blocking for a certain purpose, whether that's CSAM or anything else, how would you approach this? Would you just abide and block access from that country, given the distribution that you described earlier? Would you not do this for the other countries, for the customers in the other countries? Or may you challenge this with the European Court of Justice, for example, just on the principle of blocking?

VILIAM PELI

Yeah, so when it comes to, let's say, regulations, and each country has different regulations, different regulatory lists, we deploy it like custom for each either customer or each resolver within that country. So let's say, if we deploy it, I don't know, in Germany, we are in contact with German regulatory. We have the regulatory list which is constantly being updated.

We have the most recent one and we deploy it as one of our features to have a custom, we call them the regulatory list and also custom feed list. So we can put something extra there, and for each

country, we put their regulatory list that they have within that country. And as you mentioned, the adult content, also the DNS4EU has one IP address assigned to also blocking the categories of adult content. So that would be the answer.

PHILIPPE FOUQUART

Thank you. And we'll start with this because it's an endless topic. For adult content, the sort of scenario I had in mind is a bit more complicated in a way because it's not only adult. It is adult content, but it is subject to a certain decision at some point in a country. So beyond what the content is, it's a legal obligation in one country not to access certain contents. In the sort of scenarios, I had in mind, was that even if it's adult content, the decision by the authorities was to simply block the access, because in that case, the provider did not abide with the regulation of making sure that only adults could access to that content.

VILIAM PELI

Okay, I understand it now. So, within the DNS4EU resolvers, we are aligning with European Union law. So we do not just take like one… let's say in one country it's completely forbidden to access it, and in other countries it's okay.

We do not decide like we will do it just for this or this. We are complying with the European Union laws. So in case European Union decides tomorrow, let's block all the adult content for

everyone within the European Union, then we will block it for everyone.

PHILIPPE FOUQUART Okay, thank you.

LORENZO BRACCI Regarding ISPs, not the DNS4EU project, we give the tools to ISP to be compliant. So, for instance, in Italy, there are many different authorities that they ask ISPS to block a specific domain. So, we cooperate with ISP to be compliant, and in the portal, there is one little click where they can enable it.

But it is at the end of the day their choice, and we don't even charge any additional money for this part because our main part and focus is the security part. So for ISP, sometimes it's good to have also this regulatory part enabled and we help them to do so, but then it's on them to decide to if they want to do it or not. We give the tools.

PHILIPPE FOUQUART Okay, thank you. That's interesting. I had expected a different answer on the DNS4EU part. What you're saying is that you rely on sort of the overarching European regulations. So if I'm an internet user in France, if there's a law in France that prohibits access to certain content, whatever the reason, then if I use DNS4EU, and if it's only France, if it's only Italy, if it's only Germany, then if I use DNS4EU, I could get around national regulation.

VILIAM PELI Honestly, I'm not really sure how it is handled currently from the regulatory restrictions, because it's another team that is working with this. By myself, I'm focusing just on the global threats. I'm not really sure. I might be wrong currently, but if I understood it correctly, DNS4EU is aligning with European Union law.

PHILIPPE FOUQUART Well, only, I'm not. Don't get me wrong. It's a really crucial regulation, anyway.

LORENZO BRACCI The project has several other steps, this is just the first one, and regarding the regulatory part, maybe it will come later on.

PHILIPPE FOUQUART Thank you. Thanks very much for the presentation, appreciate. I think, as you can tell, this was really useful. Thank you. We've seen that in the chat. So with this, I think we can go back to our agenda, Brenda, if you would, and we'll go to the next item, which is the Pilot Holistic Review, and we'll take the issue of reviews of reviews. Maybe I'll turn to Tony, and then we'll have a discussion. Tony.

TONY HOLMES Okay, thank you, Philippe. I think most people are aware of the recent announcement from the Board. It's rather a sorry story

because certainly as a constituency and as a stakeholder group, we've been asking for a review for many years. And certainly, the work that Osvaldo was involved in, the IRT work pointed towards having a review, and we fully supported that.

And I think most people are aware, we even did some work in the constituency at one stage, trying to urge some action on this. And then the review turned into a pilot holistic review, rather than a review, and certainly the discussions within that group that we were involved in was looking to some shape around that review.

And we got into a discussion about the terms of reference for that review because the remit that had come out really didn't, to my mind, constitute a list-trip review at all. It was more a review of the existing ICANN processes and the effectiveness and the efficiency of ICANN, rather than a look ahead approach, which some of us were pushing for, rather than looking back at what needed or what lessons were learned from the past, we wanted to look ahead at what the demands were for ICANN moving forward in the future and shaping ICANN through this holistic review to be in a position to deal with all those future challenges.

Because this organization is over 20 years old, and as many of us have been through the painful steps of having these silo reviews, which didn't really change very much. And we tried various ways of doing that. We tried to have self-reflection on learning from our experiences, we also tried having independent consultants come in, and they proved one thing, and that was certainly that trying to

undertake a review of ICANN when you're not really, really involved in the processes and haven't got the experience, it is a tough ask.

And the results really exemplified that. So we felt that we needed to tackle, at least consider the structure of the organization, because otherwise it's just a case of rearranging the bits. And there was certainly not a consensus on that. I would suggest, for good reasons. Those were who wanted to look at restructuring have always felt that the structure of the organization wasn't too reflective of our aims and allowed us to operate in the manner that we should for a multi-stakeholder organization.

Whereas other parties, who have far more control over the existing organization, obviously were fearful that any structural considerations could reflect badly on those. And I think it was accepted that if we went down that path, there would have to be horse trading. Some people were fearful of that. Personally, I wasn't, because I think there has to be horse trading. If you're going to look at restructuring for any organization, there are always parts of it that we like and other parts that we don't like, and you have to learn to live with that and look at what's good for the organization.

So the decision's been taken now just to stop the pilot holistic review and to look back having a review of the whole review process. Now, what that actually means in detail is yet to be explained to me, I don't fully understand that. But it's very disappointing that even with a pilot holistic review, we couldn't get

to a situation where we were actually going to try something to see how we could shape having the holistic review. So where we go from this as a constituency is unclear, but I think it's unclear for all of us at the moment.

Certainly, it's really disappointing, and I think at some stage that point needs to be made. I would suggest this is a conversation for the stakeholder group, as much as anybody, to see if we're all in the same position. And then I would suggest it would be helpful understanding clearer some of the other stakeholder views on this as well. Because it's not only the CSG that have been in a position where they've been pushing for a review, there are other stakeholders as well.

So yeah, I think there's a session later, I'm not sure whether this was on the agenda or not. It is. And I think the way forward after that will come out of that session later this afternoon. But we're in a position now where the whole thing's been halted. And how you can actually get to a position with any organization, large organization, and not have a review of the whole operations and the structure of that organization when it's over 20 years old just doesn't make any sense to me.

If this was a commercial organization, we would just go out of business because you haven't kept up with the demands that that organization faces, and you're certainly not in a position to tackle challenges ahead. So I think it's a very serious step and that needs to be reflected back. How we reflect that back is something we can

discuss with our colleagues in the CSG and then maybe see where others are situated as well.

But it's a really significant situation and a very sad reflection on this organization that trying to effectively make the organization better and do that through having a review, that we're in a position where they can just say, stop. And after 20 years, I can't see this happening in the next five years now, because even having a review isn't going to be a quick exercise, it's going to be painful, it's going to be long.

So how old is ICANN going to be before it actually stands back? And maybe we should change a few things here. It's beyond me. So it's not a good story and I'd welcome any other comments on that.

PHILIPPE FOUQUART

Thank you, it isn't, but we certainly would appreciate your inputs, well, yours and Osvaldo's inputs to those discussions. I have one trivial comment and one question. But indeed, it's on the agenda, or it will be. I've asked that it'd be on the agenda or the CSG session later today. But the comment is just to add to what you said on the relevance of the organization.

The organization of the GNSO and the position of the ISPS have always been such that, well, we are in the GNSO, but as you could tell from our inputs to the issues at hand, they are, I wouldn't say marginally within the GNSO, but they're certainly just as much outside of the GNSO. And to some extent outside of ICANN, so it's

not as if the structure… I'm not arguing for a total revamp, but just for the sake of the argument, it's not that the structure had been relevant for 25 years already.

There were questions in the first place within the GNSO at the time, of the position of the structure we had altogether and of the position of the ISP. So it's yet another argument to what you just said. And my question was more on the… so the discussion that we will have with the Board is just as much on the form as on the substance. There are complaints about ATRT4 being deferred. To me, that is essentially a placeholder, I've used the term.

When you look at the bylaws, it's open-ended. It could be very restricted or it could be very broad. My sense is that it's just a medium, it's just a way of approaching this. And the question I have is, should there be a structural review of sorts or some thinking around that? Would ATRT4 with a certain remit, which would be very limited? Could it be given that some other constituencies and advisor groups argue for continuing for embarking with ATRT4, would that be the right medium to do that structural thinking moving forward?

TONY HOLMES Well, the ATRT3 exercise was, I think, fraught with difficulties on restructuring, anyway. And what came out of the pilot holistic review was somewhat reflective of that. I'm not sure that that is the vehicle to take this forward. You made some very good points as well, because we have particular problems with the GNSO, and

we're all aware of those, they've gone on for years. And I can't remember when the meeting, ICANN held the meeting in Paris, maybe you can. It was years ago. But at that meeting, it was the last GNSO.

PHILIPPE FOUQUART I would have said 10, but you know better because I was there. It was the only meeting I attended at the time, because it was Paris. Okay, it was before mine as well. Long before, with all due respect.

TONY HOLMES So at that meeting, there was a proposal to change the GNSO that nobody liked. And what the Board said to us was, okay, form a group, go away, and work for two weeks and come up with an alternative. And if you can't do that, this is what you're going to get. So we went away and we came up with an alternative, it was the bicameral system, which wasn't ideal, but it was better than what was on offer.

And the Board said, okay, we'll try this for two years, see how it works. It's never been reviewed. So it's that long ago since it was looked at. And what happened in the years past that was that we found the schedule of reviews we couldn't keep up with. So the reviews were getting delayed, delayed, delayed, and they suddenly said, stop, let's have this total review, a holistic review, to get over that.

And now they've said stop the holistic review and let's look at reviews. So it's a mess, the whole thing is a mess, and we've got to find a way to tackle it. The other thing with ATRT I find quite frustrating, I think they did some good work, and maybe you want to comment on this as well Osvaldo, but a lot of the recommendations that went from the ATRT to the Board have never been implemented.

So I'm not sure how successful that route is either. And this is a problem. We can't keep ducking it if ICANN is going to survive as an organization, and there are many challenges out there. Certainly, WSIS could be quite a challenge in itself, then we need to face up to the fact that we've got to improve things. And one way of doing that is to have a look at the whole business of ICANN, and that must include structure, because otherwise, you're just moving the chairs around. It doesn't work.

PHILIPPE FOUQUART Thank you, Tony. Thomas first and Christian.

THOMAS RICKERT Yeah, thanks so much. I joined the conversation a little later, so forgive me if I'm asking things that you've touched upon. When we last met, I pretty strongly advocated for actually going with reducing the burden of reviews. I think your point is well made that in commercial organizations, you would be out of business if you don't review how you're set up for 20 plus years.

At the same time, I've seen organizations that changed management every two years, and every management changed the organization and thereby drove the entire organization crazy. And ICANN is a special beast, and what I think we have to discuss is whether the shortcomings of the current setup are so severe that we want things to be changed. Let's say we want the bicameral structure to be revisited or something.

But then I think we should have concrete ideas on what we would like to see and then advocate for the reviews taking place or other reviews, or whatever the format might be. As far as I'm concerned, we have accountability-related things that are still not implemented almost 10 years after we did the transition. So the Workstream 2 topics that also have to do with making the organization better, haven't yet been implemented.

So I would say, unless we have something very urgent that we want to see fixed, let's try to help make ICANN more efficient in the outcomes. Because, yes, we start the bylaw provisions in the course of the IANA stewardship transition to make sure that the outside world sees ICANN to be accountable and to be looking at itself and improving things, but I think we're also seen as an organization that's very light on tangible outcomes.

And what I want to avoid is an impression by the outside world, specifically in the light of WSIS+20, whereby the organization is very good at reviewing itself and trying to make organizational changes by being very delayed, but not really coming up with substance.

And I think we need to focus on enabling the organization to produce substance. We were late today because we had the meeting with the GAC, but they were pushing for us to do policy quickly, to find other ways, innovative ways to make rules, to tackle DNS abuse that don't take years or something like that.

So I would try to focus our attention on that and shine through good results of what we're doing and not to be seen as an organization that is totally tied up in terms of volunteer resources and doing reviews and stuff like that. So you get my point. So my question to you is, and this was a long way of introducing that, do you see the urgent need, apart from the principle, that we need to review ourselves and the bylaw requirement to do so, do you see an urgent need of us pushing for the organization to be reformed in a certain way?

TONY HOLMES

Yes, it's a good question. My answer, short answer to that is yes, I do see that. But that does not in any way take away the points that you raised, Thomas. I think that working to improve things with the organization as it is, and certainly related to the transition is something we have to do. We should be doing that anyway. But the nature of ICANN is changing, and for us, I think, as ISPs, many people think, oh, they've just got a problem with GNSO.

I don't view it that way at all, because I think the fit of ISPS within the GNSO itself raises some questions. And certainly, I think some of the things that we've done as a constituency over the last five or

so years reflect the need to have a fresh view. Because I think a lot of our interests as ISPs, purely as ISPs, lie outside of the GNSO. I think there are other parts of ICANN that we should work closely with on infrastructure, ISP issues as well.

And I think having a holistic review of the organization actually helps facilitate that. So the part that you raise concerns about, I share your concerns, and I think that is an ongoing work stream, to put it in a different way. But I also think it's just as important, as I said at the start, I'm not sure when you came in, Thomas, but looking ahead with ICANN, the challenge is coming down, you can't just do that with an organization that was formed 20 years ago.

And I was around at those times, and they were all trade-offs, we weren't really sure how ICANN was going to work, how successful it was going to be, what its real scope was in those days. And what has come out of that is an organization that was actually bred, I would say, within the first three to four years of ICANN. It has never, ever changed.

Now, certainly, its responsibilities have increased and we do need to work on that, and I think the transition was a vital part of that with ICANN coming to age, so that needs to happen. But there is absolutely no argument in my mind that says, restrict it to that, because you're not looking ahead to what ICANN needs to do in the future. And that's where the split came within the Holistic Review Team. There were people that had that sort of vision.

I would say most of those that have that vision were probably fearful of an impact the review could have on them because they're quite comfortable with the organization as is, for reasons that we all understand. So I think both elements of those are things that we need to work on. But as for just saying, okay, let's not bother with that, let's just focus on what we've been doing for the last 20 years, for me, that doesn't stuck up as an argument. It is important and let's do it, but we need to do the other side of the equation as well.

PHILIPPE FOUQUART Thanks, Tony. Just for people to be aware, we're running out of time, but deliberately, I think it's important that we spend some time on this, the other items essentially for information. I'll go to Christian and Susan, and we'll take a few seconds to go through the other items. I think we need, as you said, Tony, we need to continue this discussion within the CSG, possibly within the house, to see what others would think about that and how they approach the topic in general.

CHRISTIAN DAWSON I think I'll try and be really brief. Definitely, share your overarching concerns. We need to do policy faster, especially in light of the WSIS+20 review. A lot of that does come down to scoping issues and implementation issues, but nonetheless, we need to make sure that those make those progress.

But we've also got, like Tony said, some sort of incumbent power structures that have maybe led to some roadblocks that we could end up breaking should we actually go through with the process of addressing the real circumstance of having an anachronistic system. And so I do think that it is important to address this, and it may actually help us advance policy outcomes if we do, particularly.

Because there are a couple of areas, particularly in the non-contracted side of the house, where the CSG is a clear example of this sort of disempowered structure that's existed for a long time. There's also a lot of sort of homeless constituents without a clear constituency, and that needs to be talked about at some point, too.

And that's going to help representation in an ultimate future review, if not addressed in the WSIS+20 in the next one. So I think it's really important. We can't shy away from it. I also think that there are a lot of areas where we can't get CSG agreement to put a common position on paper. But we may be able to on this, and it could be useful to do so.

PHILIPPE FOUQUART Thanks, Christian. I'll give you a minute, Tony. But I think to both of your points, I think that's a good idea to lay out a ideas on either the limitations of the current structure. I wouldn't say flesh out a new proposal in terms of what's next, but if we can, that would be good. But just to push the ball forward, that would be great. Who's

next? I guess it's on this point, but who would like to… Susan, you were next?

SUSAN MOHR

Thanks. This is Susan Mohr, for the record. I was just going to say, I thought that both commented, so I'm going to pile on a little bit with what Christian said and how Tony followed up. It seems like the two issues are interconnected. I'm not sure that we can get to a better policy process without having some structural review and the ability to come together as an organization on issues. So it seems like they're very much tied together.

And the challenge that I see is that it's one that we're mentioning yesterday that, if you have a board who's tasked with the job of doing these reviews on a regular basis, we've heard that in the last ICANN meeting, the question that was presented to us from the Board was, how do we overcome these challenges of having multiple implementation schedules and tasks that we've got to perform, and we're not able to do it, which I think reflects the decision to stop the IRT.

So if the Board is asking us for help, I think we're in trouble because it's really their role to try to do this. But it may be incumbent on us, to Christian's point, to come together as a group and help them with that to come up with a recommendation that we think the CSG could get behind and then go to them with that recommendation, which is a tall order, I think.

PHILIPPE FOUQUART Thanks, Susan. Thomas.

THOMAS RICKERT I did not mean to suggest that we shouldn't, at some point, do a holistic review, right? So I think the organization needs to be looked at, but we have limited resources. And my question to you, and I'm going to repeat it, I mean, Christian, you mentioned the point of folks being sort of homeless, but we have the opportunity to form new constituencies under the current regime, for example.

If we're talking about other ways to find solutions, we've been moving more and more to cross-community working groups to solve issues. We're using small teams. So my question is, can't we afford to say, or to support the deferral by a couple of years so that we can focus on the immediate policy pressures? We do know that the EU is the epicenter of policymaking, at the moment they're in a regulatory pause, and I think we're losing an opportunity if we don't try to address those things full throttle, like now.

And then say, okay, let's see how far we get in the next couple of years and then do a structure or holistic review or whatever you might call that animal. So, again, what can't we solve at the moment? So why is there the urgent need to do this like now, given the limited resources?

PHILIPPE FOUQUART Thanks, Thomas. I think we have to close it down because I understand that we can't run over by 10 minutes.

TONY HOLMES Can I have two minutes?

PHILIPPE FOUQUART Sure. Well, maybe not two, seconds.

TONY HOLMES We've postponed it for 10 years, doing it another two is pointless. And my real worry, Thomas, here is that Christian raised a really good point about people who can't feel part of this organization. And yes, you can try and wedge them in to a structure that is already challenged without them coming in.

And if you bring in more constituencies, it makes the situation even worse. And we are coming up to a crunch point, and ICANN is the multi-stakeholder organization that everyone looks to see whether it's working. There are a lot of governments out there that still say, this isn't a good model, and ICANN is beginning to prove that because there are people outside the tent where there is a lot of discontent.

And if ICANN doesn't try and address that, the whole multi-stakeholder organization, I think, is challenged. Because many places, you won't hear this, but there's an awful lot of people that look at ICANN and think it's not working in the way that truly

reflects the multi-stakeholder interest. And that is a really big worry we should have, and the way to fix that is having the holistic review.

PHILIPPE FOUQUART Thanks, Tony. One sentence, if you would, Christian.

CHRISTIAN DAWSON Just an additional note. I spent two years working with David Olive, and Tony, you assisted me a number of years ago in attempting to explore the possibility of starting a new constituency for the rest of the internet's infrastructure, and that system does not work.

PHILIPPE FOUQUART Thanks, Christian, very much for what we started from. That's a good point. We'll just adjourn the session now. I think we'll take the other points, including the AOBs, if you would, Christian, to the list, and we'll continue this discussion with the CSG later today, possibly the CPH. The other points are essentially for information. We can take it to the list. Anything else that we need? Yes, Thomas.

THOMAS RICKERT I'd like to bring up one point that I think I should mention in council as well a little later. But this might also be relevant to the CSG discussion that we're going to have. As you know, I'm the council liaison to the IRT, registration data, the Registration Data Policy

IRT. And we have been tasked with looking into the question of urgent requests.

And to refresh everyone's memory, the EPDP recommendations at the time had a provision on urgent requests, but it did not specify the timeline, right? Because we couldn't agree on how many days or something, it should be. So this is haunting us. There's been some back and forth, even with the Board, and the Board then said, well, this mechanism isn't really fit for purpose. Because in really urgent cases, critical infrastructure in danger, children in danger, things like that, we shouldn't be talking about days or hours. It should be a matter of minutes.

So, in that form, the discussion is, what should the appropriate timeline for urgent requests be? Then we have the RDRS, where folks are frustrated with the RDRS not really functioning, particularly for the law enforcement community. So the question is, how do you authenticate law enforcement authorities? And then there's a question, some folks say, as soon as a law enforcement authority is authenticated, there should be automated disclosure.

Whilst in legal terms, for example, even in IS2, you have legitimate ex-seekers that can be defined by national lawmakers, but they still need to send duly substantiated disclosure requests that then need to be legally vetted. Then we have the DNS abuse discussion that's also surrounding this topic. And my thinking is that, and I've tried to get that point across for years now, even in the EPDP Phase One

era, I think we should approach this topic of how the ICANN contracted parties and ICANN deals with law enforcement requests at the global level in a different way. Otherwise, we don't get it resolved.

And my suggestion would be that we maybe have a dialogue between the GNSO, the Board, and the GAC, because we need the public sector to help with the authentication, but also with putting the safeguards in place so that contracted parties can lawfully disclose data. There's just been a guidance from the European Data Board that was issued on June 3rd that basically cautioned infrastructure provider to honor disclosure requests based on orders coming out from outside the EU.

They said, well, for law enforcement, there are different mechanisms than the GDPR. It should be law enforcement, abroad talking to law enforcement domestically. So if you get a request, the default be decline, unless there are specific mechanisms in place between the countries. And also, we know from the discussions surrounding the Budapest Convention that even law enforcement doesn't have a list of authorized authenticated law enforcement. So it looks to me like the public sector is trying to make ICANN provide a mechanism to fix a broken MLED system.

And we can't do that without their help. I'm all for disclosing in split seconds in an automated fashion. But then the public sector needs to provide the legal safeguards for that. And so I think we need to have a discussion around ICANN providing the infrastructure and

the mechanism, but we need the public sector to help with that. Because otherwise, ICANN is going to look bad, the contracted parties are seen to be just stubborn, not to be willing to cooperate. But we're facing real life legal issues in in this environment.

PHILIPPE FOUQUART: So to interrupt, Thomas. Any concern over raising this during council, the need for a try party dialogue with the GAC, the Board, and Council, policy-wise?

TONY HOLMES: So what has been the response back on that so far, then, Thomas? Is it your feeling that they just don't understand the complexity of this?

THOMAS RICKERT: Some do, some don't, some openly say, well, you can't just disclose. Don't worry, it comes from law enforcement. And I had folks from the European Commission that mentioned to me, or from the UK law enforcement arena who said, well, it's all legally sound. And there's just such a discrepancy.

Gabe Andrews is working with the FBI to help with this, and they might have tools to exempt operators from liability if they disclose. But we're talking about a global system, nobody's talking about nuance. I think you really need to be specific and say, if A discloses to B, that's okay if A is in this jurisdiction and B is in that jurisdiction.

But I think we really need to have a thorough analysis and we need the governments for that.

TONY HOLMES So you're saying ICANN can't solve the problem anyway, really?

THOMAS RICKERT ICANN can't, no. And ICANN doesn't want to take responsibility for that. Joran has asked the European Administration to just provide a blanket exemption from liability, which is crazy. I have suggested that we translate the SSAD idea into a code of conduct and get that approved by the authorities.

That would be a way to make it legally viable if that code of conduct is approved, but folks didn't want to hear those things. And so I think we really need to… if we want to take this discussion further, that could be a way to get traction.

PHILIPPE FOUQUART Thank you, Thomas. I think we do want, and we're looking forward to some feedback and we'll discuss substance later on. Again, apologies for running over. That's just the result of where we're starting from. That's poor scheduling as far as we are concerned.

We've just had our counsellors showing up, which is fair enough. No, no, I'm not, that's just the fact of life. You had the dialogue with the GAC, so you're not magicians, not more than I am, so we're managing this. So thanks very much, we're going back to the list.

And we've got our ICP-2 session in a moment later today, as well as the CSG. Thanks very much, everyone. Have a nice rest of your day and see you later.

THOMAS RICKERT You too. Thank you.

[END OF TRANSCRIPTION]