ICANN71 | Virtual Policy Forum - Plenary Session: Impact of Regulatory Developments on ICANN Policy Topics
Monday, June 14, 2021 - 00:00 to 00:00 CEST

BRENDA BREWER: This session will now begin. Please start the recording.

[Recording in progress]

BRENDA BREWER: Hello and welcome to ICANN71 Plenary Session: Impact of Regulatory Developments on ICANN Policy Topics. My name is Brenda Brewer, and I am the remote participation manager for this session.

Please note that this session is being recorded and follows the ICANN Expected Standards of Behavior.

During this session, questions or comments will only be read aloud if submitted within the Q&A pod. I will read them aloud during the time set by the chair or moderator of this session.

Interpretation for this session will include English, Chinese, French, Russian, Spanish, and Arabic. Click on the interpretation icon in Zoom and select the language you will listen to during this session. If you wish to speak, please raise your hand in the Zoom room. And once the session facilitator calls your name, our technical support team will allow you to unmute your microphone. Before speaking, ensure that you have selected the language you will speak from the interpretation menu.

Please state your name for the record and the language you will speak, if speaking a language other than English. When speaking, be sure to mute all other devices and notifications. Please speak clearly and at a reasonable pace to allow for accurate interpretation.

All participants in this session may make comments in the chat. Please use the drop-down menu in the chat pod and select "respond to all panelists and attendees." This will allow everyone to view your comment.

Please note that private chats are only possible among panelists in this Zoom Webinar format. Any message sent to a panelist or a standard attendee to another standard attendee will also be seen by the session hosts, co-hosts, and other panelists.

To view real time transcription, click on the "closed caption" button on the Zoom toolbar.

And with that, I will turn the floor over to Joanna Kulesza.

JOANNA KULESZA: Thank you very much, Brenda. Welcome to the first plenary of this ICANN71, hosted in virtual Hague. Thank you for joining us on this lovely European afternoon and possibly very early in the morning or late in the night where you are. So thank you again for joining us today to discuss the impact of regulatory development on ICANN policy topics.

If I could have the following slide, I would like to explain how this session has been composed and how we plan to conduct our discussion.

In the first part of this session, we welcome two of our speakers who will give us examples of current regulatory developments and how they might impact the DNS. I will introduce them in a moment; but let me emphasize at the very beginning, we welcome this input as a sign of support for the multistakeholder policy development process within ICANN and beyond.

In part two, we will welcome brief interventions from representatives of ICANN community stakeholder groups.
This part will be formed as a panel discussion, giving representatives of each community a chance to share their

reflections on how national or regional regulatory development impact their respective communities.

And in part three, as advertised by Brenda at the beginning, we will welcome questions. Again, looking at the high participation, which is highly valued and appreciated, we will limit the input into this third part to the Q&A pod. Feel free to add your questions to the Q&A pod as we progress through this session.

I will then kindly ask staff for their support in reading out the questions and will ask our presenters and panelists to respond to these. If I could have the following slide, I would like to welcome and introduce our speakers and panelists.

My name is Joanna Kulesza. As already indicated, I have the pleasure today to moderate this session on behalf of the At-Large community. I serve as the ALAC co-vice chair responsible for capacity building. And, indeed, this session does have a capacity-building effect to it. We want to learn better how to ensure community participation into regulatory processes.

For us to be able to understand how this can be done efficiently, we welcome two introductory presentations. The first one coming from Olivier Bringer, representing the European Commission. The European Commission has recently welcomed quite a few regulatory proposals that will impact the way the ICANN community operates. We welcome the participation from the commission and a brief recap of what these processes are and where and how the community can best support them.

Let me note the European Commission has been very welcoming in explaining the way the work that is done in Brussels impacts the DNS community. So this meeting is not a chance for us to detail these efforts but rather to understand how the multistakeholder process works.

Our second speaker today is Mr. Alexander Seger who has been a guest to our ICANN meetings on numerous occasions, and we welcome his participation as he heads the work of the Council of Europe on the Budapest Convention, one that is focused on cybercrime.

One of the top topics for the ICANN community has been DNS abuse. And as Alexander has explained before -- and I very much look forward to him explaining again today -- there is a lot of common ground between the work of the Council of Europe on cybercrime and our community efforts on targeting DNS abuse.

We will then move to the second part of our session. And in alphabetical order, I welcome our panelists. Fred Baker who will speaker on behalf of the Root Server System Advisory Committee; Philippe Fouquart who will speaker on the Generic Names Supporting Organization's council and community. And I welcome Philippe as the chair of that community.

On behalf of the At-Large, I welcome the participation of my colleague, Matthias Hudobnik.

And last, but by no means least, looking at the specific legal framework the ccTLD community operates in, I welcome Alejandra Reynoso who will give us a perspective of the CC Names Supporting Organization as the chair.

Please kindly note Alejandra will be speaking in Spanish. There is interpretation provided. Do seek advice from our staff, should you encounter any issues or challenges.

With this, I would be eager to swiftly move to the first part of our session today, giving the floor to Mr. Bringer to give us an introduction to E.U. regulatory developments and the way how these may impact the DNS with the overall theme of us understanding better how we as a community can find our place to understand and support these efforts.

Without further ado, Olivier, the floor is yours. Thank you very much.

We cannot hear you, Olivier, I'm afraid. You might want to unmute. And I believe your slides are following.

Thank you.

OLIVIER BRINGER: Thank you very much, Joanna.

I have unmuted now. My name is Olivier Bringer, and I will be speaking in English.

So I will be presenting regulatory developments that have an impact on the DNS, and I hope it will serve as a good illustration and as a good basis for the follow-up discussion we'll have in the panel.

Next slide, please.

I will be presenting two proposals from the European Commission, one that links to cybersecurity in the European Union, the so-called NIS2 directive, and the other one is a proposal for regulation on the single market for digital services, which is called the Digital Services Act. I insist on the fact that I will be presenting proposals from the European Commission. I will not -- I am not in a position to comment on the legislative process that is taking place at the moment. So I will stick to our proposals.

Next slide, please.

So the first, I will start with the NIS2 directive, the proposal for NIS2, reminding that there are three essential pillars in these proposals which actually are also the pillars of the current NIS directive. The first is to have appropriate capabilities at the level of the member states to deal with cybersecurity incident. The second one is to have risk management in place, and that concerns essentially operators and companies. And the third one is to have cooperation and information exchange in particular across borders.

So what we do, what we aim to do with these two directives is to reinforce each of these pillars, reinforce the capabilities, reinforce the way risk management is being implemented, further harmonize the measures, and reinforce the level of cooperation we have in Europe.

For the DNS operators, they will be mostly concerned by the second the pillar, the pillar on risk management.

Next slide please.

So how is the DNS concerned by the NIS2 proposal? First, we recognize the criticality of the DNS. A reliable, resilient, and secure DNS we think is a key factor in maintaining the integrity of the Internet.

Because of that, we have included DNS operators among the category of essential entities, and we propose to cover in the scope of NIS2 all DNS services along with what we call the DNS resolution chain, and this includes operators of root nameservers, this includes TLD registries, operators of authoritative nameservers and recursive resolvers.

If you are aware of the current NIS directive, DNS is already covered in the current NIS directive, but the DNS operators have to be identified by individual member states, which has -- which, as a consequence, has led to different implementations, different operators being covered in different countries with different threshold, et cetera.

So to have a more harmonized implementation, we propose to put all DNS service providers and TLDs automatically in the scope of NIS2, and we propose also to have a single jurisdiction regime. So DNS operators will have to implement NIS2 in their main country of establishment in the EU. And in case operators are providing services in the EU but are not established in the EU, they will have to designate a representative in the Union.

NIS2 foresees horizontal security measures, so measures which apply across different sectors, but it will be possible to have sector-specific measures, because we cover very different -- very different sectors, of course.

And one point I wanted to mention is that NIS2 is also adding a point about the accountability of management bodies of the essential and important entities. So the management bodies of these entities will be accountable to implement appropriate cybersecurity measures.

Next slide, please.

So among the obligations that we foresee for TLD registries, we also have -- we also want to cover domain name registration data. And here our point is that maintaining accurate and complete database of domain name registration data and providing lawful access to such data is essential to ensure the security, stability, and resilience of the DNS. And we also link the availability and timely accessibility of these data to the fight against Domain Name System abuse; in particular, to prevent, detect, and respond to cybersecurity incident, cybersecurity being the scope, of course, of the NIS2 directive.

Next slide, please.

We have, based on this principle, proposed one article, which is so-called Article 23 on the domain name registration data, which foresees a number of general obligation that will apply to TLD registries and entities that are providing registration services for them. So we have obligation about collecting and maintaining accurate and complete domain name registration data; obligations about having relevant information to contact holders of domain names; obligation to publish nonpersonal data, ensure response to access request without any delay; and finally, providing access to specific personal data upon duly justified requests by legitimate access seekers.

So these obligations are rather high level. And what we ask the concerned operators is to have policies and principles in place to implement these obligations. And our idea is really that these policies and principles would be derived from the policies that are developed inside ICANN for what concerns gTLDs.

So our approach is really one which is trying to complete, to complement the effort that is already taking place in ICANN in particular in terms of WHOIS policy.

We can -- we have also foreseen the possibility to adopt guidelines, but really our idea is to point toward industry guidelines and in particular to ICANN guidelines. Of course our objective is to make sure that across a single market, there is a harmonized approach.

So that's what I would say on the NIS directive. It's very short, and I would propose to be even quicker, say a few words about the Digital Services Act. Next slide, please.

So very, very quickly. The Digital Services Act is about modernizing the rules that we have in place, eCommerce rules, to illegal content and systemic risks in the online space while taking into account the fundamental rights of our citizens. It's about having a single set of rules across the digital service -- across the digital single market which will provide legal priority to the companies concerned. And it's also about supporting crossborder cooperation among national authorities to have a better oversight; in particular, of the systemic players.

Next slide, please.

So there are different categories of services that are concerned by the -- by the DSA. And I have -- in this slide, you see these different categories.

The broader category is intermediary services. This is where the DNS operators will be located, if I may say. But then you have more specific categories, the hosting services, online platform, and the very large online platforms.

Next slide, please.

And the idea is that there is a graduated set of obligations that will apply to these different categories of operators. And the higher the capacity of the operator to tackle illegal content, the higher the impact of the category of operator, the more obligation, the more due diligence obligation we will expect them to take.

So again, the DNS would be in all the intermediary's category and subject to limited number of due diligence obligations.

Next slide, please.

So what does the DSA bring for the DNS? Essentially it brings certainty of being covered by the European legal framework. So the certainty that the liability exemption regime applies to DNS operators. A sense of proportionality when tackling illegal content online. So that's what I was explaining in the previous slide. The number of mitigation measures is lower for infrastructure operators such as DNS operators. And also, there is this notion of subsidiarity, that illegal content should first be tackled with those who disseminate the illegal content, and when it's tackled through intermediaries, with those intermediaries who have the biggest capacity to remove the content. And in this chain, I think DNS operators can -- can really last.

There will be also a harmonized framework for how member state can request intermediary services to act against illegal content, meaning that there will be legal basis, there will be a certain set of information that will be provided by the member state to be -- to ask an intermediary service provider to act or to provide information about illegal content.

So overall, we're seeing what we propose is a balanced solution as far as infrastructure service providers are concerned, and this includes the DNS operators.

And in the next slide I have simply put -- next slide, please -- I have links if you want more information. But to sum up, we propose in the DSA very balanced obligations. And in the NIS2 directive, we propose essentially high-level obligations to meet these important policy objectives for us to increase cybersecurity in the European Union. And this is very really meant to be complementary to effort being taken in ICANN in terms of defining how this obligation should be met.

And I would stop there and give you back the floor, Joanna. Thank you.

JOANNA KULESZA: Thank you very much, Olivier. I am noting the questions in the Q&A pod. Thank you for putting them into the dedicated section.

For the sake of time, I am going to give the floor straight to Alexander. I am mindful of the time we have for this session.

Just a heads up to our panelists in the second part, I'm going to kindly ask you to limit your initial remarks to five to six minutes. I believe this will allow us to stick to the originally proposed timing.

Olivier, there are some questions for you in the Q&A pod. These can be answered live in the Q&A section of this session or, should you wish to answer these in the Q&A pod directly, that is also encouraged.

Without further ado, as I already said, I'm happy to give the floor to Alexander Seger who will give us an update on the work within the Council of Europe that we, as a community, will likely find interesting for the purposes of DNS abuse policies that are being developed.

Alexander, the floor is yours, and the slides, I believe, are in the same slide deck that our wonderful staff is advancing. Thank you.

ALEXANDER SEGER: Thank you, Joanna, and everyone. A great pleasure to be here, and obviously we are very supportive as Council of Europe, but also the parties to the Budapest Convention on Cybercrime, to the multistakeholder policy development process.

What I intend to do in the next five minutes is to give you an update on the second additional protocol to the Budapest Convention on Cybercrime that was approved by the Cybercrime Convention committee just over two weeks ago.

Next slide, please.

Just a reminder of what the Budapest Convention is about. It's a criminal justice treaty about specific criminal investigations, about specific offenses against them by means of computers, substantive criminal procedural powers with safeguards to investigate cybercrime and collect electronic evidence in relation to any crime, and then international cooperation not only on cybercrime but also electronic evidence related to any type of crime.

It's complemented by a number of guidance notes to explain that the smartphone nowadays is also a computer system, which wasn't the case 20 years ago, for example, and lots of other guidance notes. And currently there is a protocol on enhanced cooperation on cybercrime and electronic evidence in preparation. I'll give you a short update on that in a second.

As of today, we have 66 parties, which means parties from Europe but also from Asia-Pacific, Caribbean, the Americas, Africa, and so on, and so a mix of countries from around the world. And the Budapest Convention is a nice little booklet and a nice treaty, but it's more than a legal text. It's a mechanism complimented by the Cybercrime Convention Committee that does follow-up and assesses the actual implementation of this treaty.

And, of course, we have a very strong capacity-building component through the Cybercrime Program Office of the Council of Europe in Bucharest. The Budapest Convention was open for signature 20 years ago in Budapest, but we have this office in Bucharest from where we can support countries from all over the world.

Next slide, please.

For many years now, it must go back almost ten years, we have been discussing how can we overcome the problem of territoriality and jurisdiction, meaning that offenders, victims, computers used to commit crimes, the evidence of crime are scattered all over the place in multiple jurisdictions, in unknown jurisdictions, in shifting jurisdictions. And how can we, therefore, obtain more efficient access to data at the same time also meet human rights and rule of law requirements. Specifically, we try to solve of how do we obtain subscriber information more efficiently, how to obtain access to WHOIS data, in particular to create a legal basis for access to or for request to and disclosure of WHOIS data; how to obtain -- how to cooperate in emergency situations, and I'll say an ongoing emergency. Almost instantly, how can you obtain content of email accounts, for example? How can you make mutual assistance more effective because we know it's slower, but we cannot do away with it. It's still an important means to obtain evidence, and we have to make it more efficient.

And if we have all sorts of interesting, new and efficient measures like direct cooperation with private-sector entities and other parties, how can we establish rule of law and, in particular, data protection standards so that we're sure that if data is transferred under this protocol, it is also protected at an appropriate level to the satisfaction of all parties and the other party. So that's what we tried to resolve, and I think we are getting there.

Next slide, please.

I will not bore you with this. But, again, as I said, this started almost ten years ago. Four years ago, in June 2017, the parties decided to launch negotiations of the protocol. And we had over 95 sessions to negotiate this. Very intense. In particular, during COVID times, we had 65 virtual meetings in recent months. We had consultation with industry, with data protection experts, with civil society. And a large number of bilateral, trilateral meetings, domestic meetings, it was very intense, very difficult topics, of course. Very difficult. But at the 28th of May, we agreed among the parties on the draft protocol. It is now going through some formal procedures. Hopefully, by November this year it will be formally adopted and then open for signature in spring next year.

Next slide.

There's also the dimension that in these negotiations we had 66 parties negotiating. So we had to make sure that what works in Europe also works in the United States, in Canada, in Argentina, in Tonga, in Ghana but also Australia and all other places.

So this protocol, as it is now, the draft -- the main part is Chapter 2. These are the measures for enhanced cooperation. And what is of particular interest possibly to this meeting here is Article 6, is about request for domain name registration information, WHOIS data, right?

Also, important is Article 14, protection of personal data. This protocol, the draft protocol, has a very detailed data protection article. It's been very difficult to negotiate because we had to make sure that what countries like Canada, Australia, U.S., Argentina can do is also meeting expectations of the European Union under the GDPR and the police directive. It's very difficult to negotiate, but we now have a draft that should work.

I must say that for the 27 European Union member states, the European Commission negotiated the protocol.

Of course, the other member states are also there; but European Commission negotiated on behalf of the E.U. member states.

So this is the content of -- next slide, please.

Again, I will not go into detail here. But, of course, I am ready to take questions.

Under Article 6, request for domain name registration information, important is that parties to this protocol will have to put a legal basis in place to empower its authorities to request an entity providing domain name registration services, a registrar, registry, okay, to make such request.

And, secondly, to commit a registrar or an entity providing domain registration services to disclose information in response to a request by another party directly without going through the domestic authorities of that state.

And then there are some details in paragraph 3 of Article 6 about what shall a request contain. And then there is also provision of consultation in case of noncooperation.

What is important is there's a lot of flexibility built in. And we kept it slim and flexible to take account of the possible future solutions that will come out of the ICANN process, okay? So it's very important.

But with this, it's a legal basis for requesting data and for disclosing data. And very important, Article 14 on data protection applies. So a registrar disclosing data can be confident that if this request comes out of the protocol, the receiving party has the obligation to protect the data under the standards according to the standards of Article 14, which is the acceptable standard to everyone. Very important.

Next slide.

Again, the question comes up, will registrars respond, or will they say we don't want to incur any liability risks. And the.

Of arguments also explained in the report in Article 83, we do believe that in the end registrars or entities will respond because there's a clear legal basis for that. There are other safeguards of Article 14 in the receiving party and so forth. So we think there's a lot of ground where eventually they will cooperate.

Maybe in the beginning this will be a bit slow. It will be a bit slow going. But over time, the routines will kick in and, in particular, depending on what happens with the systems developed by you and by ICANN and so on how that will kick in.

Next slide.

So we hope that it will work with the SSAD. We have to figure out how this will work in practice. I think we have from the Cybercrime Convention; we will have to cooperate with you in the future to see how we can make sure that this all works nicely together.

And, again, there is a specific support to the multistakeholder policy development in this protocol.

The next one.

It's my last 20 seconds. We believe that overall this protocol will provide a lot of operational value to have more effective, more efficient criminal justice in cyberspace, better rule of law. But it will also be clear that the mechanism of the Budapest Convention will continue to stand for free Internet -- free and open Internet where limitations are restricted to specific cases of criminal misuse.

And with that, back to you, Joanna.

JOANNA KULESZA: Thank you very much, Alexander. This is most informative.

I already see the questions forming in the Q&A pod.

As before, I would encourage you to look into the Q&A pod and decide whether you might want to answer these live in the dedicated timing at the end of our session or whether you would like to type your answer into the chat.

Now, again, for the sake of time, I would like us to move to part two of this session. There will be questions to all of our panelists. I am going to invite the panelists to speak in the alphabetical order as they were initially introduced.

We have a few questions formed for our panelists to try and respond. If I could ask staff to show these questions on screen, that would be wonderful.

The overall theme here is for us to better understand how individual communities tackle regulatory advancements and developments. I would like Fred to start us off giving a perspective from the technical community, the security community.

If you could limit your intervention, Fred, to five to six minutes, that would be wonderful. Thank you.

FRED BAKER: I suppose I have to go off mute for that.

So thank you for that. I'm looking for the questions. They have gone away somehow.

And let me be very clear about the point of view that I'm coming from. The root server operators don't speak for each other. We maintain internal independence in that way. And so I'm speaking from the perspective of the Internet System Consortium, which is the root server operator that I'm on the board of.

And I think the other root server operators probably have similar concerns, but they would need to comment on that for themselves.

The root service is explicitly included in the NIS2 directive, as I understand it. But I'm not at all sure that the people who formulated NIS2 understand the root service or what it is.

The root service starts with data that is available from IANA that is sent to us by the root zone maintainer. And we then distribute in response to requests from various other parties, whoever they might be.

We do not operate a registry. We do not operate as a registrar. Now, those might be other businesses that the same companies are in, but that's not true of the root service. And actually there is no money that changes hands. The root server constellations and so on and so forth, that's not how they're funded.

When I read through NIS2, I'm pretty sure that the people that wrote it are thinking of a very different system than I'm a part of. So I would like to understand when NIS2 is proposed and is supposed to be addressing registrars or registries and billing people for infractions of various kinds, who do they think that they're addressing this to? So I'll leave it there.

JOANNA KULESZA: Thank you very much.

FRED BAKER: Back to you, Joanna.

JOANNA KULESZA: Thank you very much, Fred. That is very helpful. We will have 30 minutes hopefully for further discussion. But this flag that you are raising is very important.

For the benefit of our panelists, I have inserted the questions also into the chat. And I give the floor to Philippe to give us a GNSO perspective on these issues. A broad landscape that you might wish to draw is welcome; but if you wish to address specific initiatives as they were described, that is also wonderful. Thank you.

The floor is yours.

PHILIPPE FOUQUART: Thank you, Joanna.

I hope you can hear me. This is Philippe Fouquart here from the GNSO. Thank you.

I would just in broad terms -- and with the same caveat as Fred just put initially, I will just say that -- and quoting Olivier -- those are proposals including one directive. There will be translations along the way, for example, in national remits. So many unknowns on the path, on the end result, A.

And, B, obviously the way the GNSO -- the communities and the GNSO in particular will respond is very much a work in progress.

So that being said -- I appreciate those answers will not be very solid at this point given those unknowns.
That being said, I'll just pick up on a couple words that both Olivier and Alex used, "reinforce" and "harmonization."

As far as what might impact GNSO policies, I think it's fair to say as far as accuracy, natural versus legal distinction, et cetera, data accuracy, those are not new topics. I think they should come as no surprise to the community and especially those who have been involved in phase one of the PDP. Phase two there was a reference to the SSAD and the ongoing Phase 2(a). So these are things we are already familiar with. So maybe I'm jumping ahead, but there's, indeed, room and opportunity for us and the community to participate and sort of figure out the end result, we're using the term I just used, might be. And Phase 2(a) is a good opportunity to do that.

But the question of triggers, for example, is asked in that context, in the context of NIS2 but also more broadly. So that's certainly something that the community may want to take up on all these aspects.

That being said, I should also say that with hindsight, those couple of years, those are extremely difficult issues. I think there's a learning curve also on the lawmakers' perspective. I think there's now a recognition that it's a balance between redaction and the use of those data by -- not only by legal enforcement but also the legal community.

There's also a learning curve within the community as far as the actions that we want to take.

So I'm not going to use any more of our time. Just setting out the broad landscape of what we've done and what we're looking ahead. And we're using the term "inconcrete" actions within the PDP in particular. And I will say a word on the "how" in phase 1 later on. Thank you, Joanna.

JOANNA KULESZA: Thank you very much. Thank you for setting the scene.

And I give the floor to Matthias to give us the end user perspective on this. Thank you.

MATTHIAS HUDOBNIK: Hello, everyone. Matthias Hudobnik speaking for the record.

I have the great pleasure of representing end user interest on behalf of the At-Large community in this plenary session.

Related to the question, so, first of all, the At-Large community has a strong regional focus. So meaning for the ALAC getting involved in our regulatory processes is primarily a regional effort.

We have ALSs in all regions, and one of the focal activities is understanding and reflecting the needs of individual end users. This is why advancing ALS participation is one of ALAC's key priorities as recently reflected in the ALS mobilization working party report.

And this is also an excellent example for the multistakeholder approach, integrating everybody who is interested to contribute and also living diversity.

We're also trying to work with other ICANN communities, though the At-Large makes sure to work together with other constituencies within and across regions. So this session is one of the examples where the ALAC and also people from GAC work together in streamlining the narratives and also objectives.

And the At-Large community also tries to get a citizen as an end user on board, meaning At-Large much like as the GAC expands across the globe of individual Internet end users. So while, for example, GAC interests and focuses might be more versatile and the At-Large is all about people understanding their needs and also reflecting them in the ICANN processes.

While our objectives often align, the At-Large is also focused on identifying particular needs that come with its unique mission. So it has helped us to better inform the regional and local legislative processes. And a very important point is also capacity-building to be able to better react to local, regional proposals.

We need educated members. So, therefore, one of the At-Large key priorities is end user education.

You can imagine in time of the pandemic; we saw a rise in DNS abuse. This is why also the At-Large has put focus on streamlining its DNS abuse narrative into local capacity-building activities that will inform also end users and also try to foster, like, legislative processes, executive decision and normative trends related to the end users; inform community members of the cornerstone of an effective regional policy making within the At-Large community.

And a little bit more concrete to the question of lessons learned and also how can we prepare in the future, I think the GDPR is a very good example of legislation affecting not only European countries but having an extended effect on the ICANN technical community and also negating potential risk of the ICANN multistakeholder model where we also discussed during the last ICANN meeting at the At-Large panel how we could, like, affect on these things. And we also agreed on some points like having an early warning system that could inform the community about any global changes which could affect the unique identifiers multistakeholder model.

Then there's also a need for all stakeholders to work together collectively, and for that evolution of the ICANN multistakeholder structures would also be an essential part.

Also the At-Large structure have a central role in educating and raising awareness of the public about how the Internet works and also about ICANN's important role, and the (indiscernible) potential warning system integrated in the At-Large structure's role, which might mitigate (indiscernible) risk to the ICANN multistakeholder model.

And with regards to the GDPR and the WHOIS per se, I think ALAC is very active in the EPDP processes, obviously from an end-user perspective. And, yeah, the ALAC believes that individual registrants are users, and we have also regularly worked on their behalf. So if registrants need to defer from those of the four billions Internet users who are not registrants, those latter needs take precedency. And yeah. Although the ALAC is very often agreeing with the positions taken in the GAC or the SSAC and also business or IBC statements concerning the access of those third parties who work to ensure that the Internet is still is a safe place and secure also from a user's perspective, and that means that law enforcement and cybersecurity researchers are able to combat the fraud and crimes and also to protect users from phishing, malware, fraud, DDOS attacks, you name it. So -- but all within the constraints of the GDPR, of course.

And last but not least, the At-Large community is also trying to raise awareness within the community related to GDPR. For example, we will have a session tomorrow about the GDPR as a technology where we also will talk, maybe, a bit of the data from Verisign concerning WHOIS. And we also had a very interesting DNS women panelist discussion at the last ICANN meeting where experts from Mexico, Australia, U.S., Argentina, so female -- female experts in this area discussed different data protection law. So the At-Large is very (indiscernible) contributing to these matters. I will stop here.

JOANNA KULESZA: Thank you very much, Matthias. This is truly appreciated. Even though the GDPR was not originally on our agenda, if I was keeping count, I would say that probably GDPR is the acronym that wins the popularity here, and I would assume that that would also be the acronym that Alejandra might want to use in her intervention.

The floor is straight into your hands, Alejandra. I know that the ccTLD community is facing particular challenges working closely on regional legislation and regional normative efforts, even, if they do not take the shape of law.

The floor is yours, if you could give us a brief recap, and we will move straight into the questions.

Thank you.

ALEJANDRA REYNOSO: This is Alejandra Reynoso speaking. Thank you very much. I'm going to speak in Spanish.

Definitely the ccTLD community is a very diverse community in terms of size, regulations, legal framework, registration models, administration and operations, and regarding policies, languages, customs, if you will, traditions. And of course we have to serve our local communities. Therefore, this is a challenge.

There is a challenge for ccTLDs when facing these regulatory demands, but of course they are doing it in a wonderful manner.

At the ccNSO, as a global organization, we try to find spaces for ccTLDs to share their experiences so that they can show us how things are working or going on so that they can find cooperation and so that they can help each other or other ccTLDs with similar situations.

Some weeks ago, for example, we had a session, this is a session on ccTLDs news, where two main topics were discussed. One of these topics was ccTLDs and security, cybersecurity due to regulatory demands. We had the presentation of different ccTLDs from Kenya, Japan, the UK, Canada and the U.S.

And we also had another session regarding ccTLDs' experience on DNS abuse where we had representatives from China, Botswana, Chile, and Portugal.

So this is one of the actions that we are taking at the ccNSO. And then we have groups technically supporting ccTLDs as it is the case of the TLDs ops or TLDs operations. This is a committee, the ccNSO, in charge of supporting ccTLDs in terms of security issues. There is a mailing list available so in order to, you know, send emails regarding risks or threats. And they have also developed a set of guidelines, very good guidelines, to mitigate, for example, the DDOS attacks or for ccTLDs to be able to speak about their recovery plans and disaster recovery plans in a simple manner.

There are many standards and guidelines available for these activities, but they have been developed by ccTLDs for ccTLDs in order to create simple guidelines, practical guidelines to be adopted in a quick manner. And thanks to ICANN's support, they have been translated into the U.N. languages, so they're available at a global level.

So this is how the ccNSO covers the topics, I mean seeking spaces for ccTLDs to be able to share their experiences and to learn from others.

Thank you.

JOANNA KULESZA: Thank you very much, Alejandra. Thank you for being concise and, at the same time, quite specific. And thank you for highlighting all of these challenges and initiatives that are being taken regionally to best address the concerns of the ccTLD community.

I want to thank our panelists and thank our speakers for attending to the questions in the Q&A pod. You have been tremendously efficient. Thank you for that.

There are three questions still pending. I understand they might be a live answer. So I would like to kindly ask staff to read out the three remaining questions. Then I would give the floor to our two speakers Olivier and Alexander. I understand that both of these questions are at a cross-section of your interventions. And then I would like to -- There are more questions coming up. We will see how we do on further questions, then. But I would like to ask staff to read out the three first questions and then give the floor to our speakers to try and answer.

Thank you.

BRENDA BREWER: Thank you very much, Joanna. We do have the first question from Reg Levy of Tucows: Where the current public poll -- sorry, WHOIS. Where the current public WHOIS indicates what a domain is registered outside a law enforcement's jurisdiction, what additional information do you think is necessary to be disclosed to the extra judicial law enforcement agent?

JOANNA KULESZA: Thank you, Brenda. If we could start with three questions and give our panelists an opportunity to answer.

BRENDA BREWER: Would you like me to read all three, then?

JOANNA KULESZA: Please. Thank you.

BRENDA BREWER: Thank you, Joanna.

And the next question is also from Reg Levy of Tucows: How do you propose that you will find out where a domain is hosted out of in order to determine territory -- I'm sorry, territoriality for bringing a law enforcement action?

And the third question is from -- I'm afraid I won't be able to pronounce the first name. The first name starts with V, and the last name is Erokhin, so I apologize for the name. And the question is what plan does ICANN have for the implementation of the national legislation of individual countries, not only the EU regulation?

JOANNA KULESZA: Thank you very much, Brenda. I would like to start with Olivier and then go to Alexander. I'm not sure Viacheslav's question is directed at them, but there will be a round of responses from our community reps, and I hope, Viacheslav, we can try and attend to your question.

I would like to start with Olivier, if you would like to take questions from Reg. And if Alexander would like to jump in on those as well, feel free to take the floor.

OLIVIER BRINGER: I would defer to Alexander. I mean, these are really questions about the Budapest Convention, about the law enforcement, so I will defer to Alexander.

And the question of ICANN, I think on ICANN, it's really the topic of our panel discussion.

JOANNA KULESZA: Thank you.

Alexander, go right ahead.

ALEXANDER SEGER: Thank you. I might say I had some difficulty to fully understand the first question, something about what additional information is needed when you send request outside your jurisdiction, something along those lines. As I -- when I presented the -- roughly the content of Article 6 of this future protocol, it basically says what you should include in a request to a domain name registration -- an entity providing domain name registration services in another party. So Article 6 is always to a registrar, registry in another party.

That also answers partly the second question about what do you do when you don't know. Obviously let's assume that all current 66 parties, and let's say by -- in a few months, let's say we have 70 parties to the Budapest Convention. Let's say by the time this protocol is open for signature, then let's implement, let's assume all of those 70 parties implement this protocol, of course Article 6 applies only to those parties. We cannot provide a legal grant to access data in a nonparty to this protocol. I mean, that's also clear. So it only works between those -- between the parties to this protocol.

So, therefore, if you're interested in having a legal basis for access to risk, join the Budapest Convention and later, also the protocol.

JOANNA KULESZA: Thank you, Alexander.

I'm curious if there is any of our community members who would like to pick up Viacheslav's question about how ICANN plans to implement the national legislation that comes from different countries. Viacheslav indicated this might be a question for ICANN org, whereas this session provides us with this set of panelists and participants.

If anyone wishes to speak.

I see Philippe's hand is up. Philippe, go right ahead.

PHILIPPE FOUQUART: Thank you, Joanna. I would like to speak in French, if it's possible. Thank you in advance.

Perhaps it is just common sense, but the question by Viacheslav was asked often in the PDPs. And it focused on the evolution of the European regulation.

What happens when other regulations emerge and what happens in the best of cases if they are coherent or if they are different and, in the worst of scenarios, they are incompatible with the first regulation we took into account with the PDPs; in particular, of the GNSO?

Well, the answer is there isn't any simple answer to this question. What we need to do in terms of process is to follow what happens in terms of regulation evolution throughout the world. And I think that org follows what is happening and contributes in the consultation process to those developments.

Another thing is, and we need to debate about it, but the community can submit its views to the org on the developments. I think that maybe we need to create something or recreate something in that area.

And then it is up to the PDPs or the working groups themselves to integrate the different developments. Perhaps having a team in charge of the developments of the PDPs where different parties are represented, whether it is the GNSO or others. And these organizations, these countries, in particular that plan a national development, because that was the question asked, that they submit their needs so that they are considered within the working groups themselves.

The question was general, so the answer is general. I apologize for that, but that is probably the difficulty in the future as we move forward.

As we move forward, there will be more limits, and we need to have as good of visibility as possible on the limits that will be placed upon us as we move forward.

Thank you, Joanna.

JOANNA KULESZA: Thank you very much, Philippe.

I see Olivier is picking up the question from Becky Burr live in the chat.

We have two questions for Olivier from John McCormac. I would like to move next to these two questions, again leaving time for our panelists to reflect and intervene.

Olivier, the first question from John McCormac refers to the poor definition the DNS operators seems down to the lack of a good understanding of DNS operation and the different types of DNS. The NIS2 scope is problematic, but there does seem to be some work being done on addressing the problem. The scope and definition are the problem, indicates John.

And also, Olivier, there are hundreds of thousands of single-domain DNSes. Then there are people running their own DNSes and there are web developers and hosters and registrars. The DNS ecology is quite complex.

Olivier, I'm wondering if you have any thoughts on those comments.

OLIVIER BRINGER: Thanks, Joanna. So as I said, I think what John is pointing at is the legislative process that is taking place. And, indeed, there will be changes to the proposal that we have made possibly in terms of scope, in terms of definition. But as European Commission, I would stick to our -- I would stick to our proposal. And I think we have recognized the criticality of the DNS. And because of this criticality, it is important to cover a full range of DNS -- DNS operators.

And the second question, because it does appear I have a bit forgotten what it was about, but for me it was more an information than a question. Indeed, the DNS ecosystem is -- is complex, and there are very different players. But I would like -- I remember that John mentioned hosting providers. Of course hosting are -- providers are treated differently from pure DNS providers. But it is possible that you are both a DNS provider, a hosting provider, maybe a (indiscernible) provider, and then you have the obligations from these different categories that would apply to such -- to such an entity.

JOANNA KULESZA: Thank you very much, Olivier.

I am also being flagged that there is a question from Monika in the Q&A pod that was marked as answered, but there is more information requested from Alexander Seger. Monika Ermert asks: How will the parties to the Cybercrime Convention enforce sanction with regard to Article 14, minimal data protection? How will violations be sanctioned, also considering that round about 20,000 rulings of the European Court of Human Rights in Strasbourg remain unimplemented and the non-Council of Europe members certainly do not subject to the European court anyway.

Alexander, I think that's a very general question on how the convention operates worldwide. I'm curious if you might want to reply to this question. If it would be helpful for me to copy that into the chat, I'm happy to do that as well.

Alexander.

ALEXANDER SEGER: Thank you. I actually was just responding to it, typing it. But maybe it is better to do it live. And maybe I will in addition also write something in the chat.

Under Article 23 of this protocol, the implementation of the protocol will be assessed by the parties. And that includes in particular the assessment of Article 14 on the protection of personal data. So this is one thing to keep in mind.

But equally, if not more important, is paragraph 15 of Article 14 about consultations and suspension. So if a party has information that there is a series and systematic breach of data protection obligations, it can suspend the transfer of personal data under the protocol, which de facto means basically assessment of almost all provisions of the protocol in relation to that particular party and so forth. So Article -- paragraph 15 is quite detailed.

There's also an explanation to it so that it cannot be used to unilaterally stop data transfers if there's nothing about it and so forth.

And, Monica, seriously, what does this have to do with decisions of the court of human rights and its implementation? I think that's a bit polemic. Thank you.

JOANNA KULESZA: Thank you very much, Alexander.

I think this brings us to the broader discussion on how we within the ICANN community can best understand, build capacity, and possibly impact the way that international treaties, international works. So I welcome the comment, and I welcome your precise answer.

I see there's a question from Mason Cole in the Q&A pod that Olivier seems to be typing an answer to. I don't want to give you two jobs at the same time, Olivier. If you would like to answer that question live, you are more than welcome to do so.

And then I would move to the question from Peter that is targeted to all of our panelists.

So if you would like to answer live to the question from Mason, Olivier, you are more than welcome to do so. And then I will move back to our panelists.

Go ahead.

OLIVIER BRINGER: I was typing it, indeed.

No, we have not -- as I mentioned, the obligation, the provisions that we have put in the NIS2 proposals are quite general.

But for us, accessibility is very important. It's very important to make -- provide the requests are legitimate and well-defined. It is important to make the registration data accessible to ensure a good level of cybersecurity. So we would expect that in developing the policies and procedures for accessibilities, the registries and the entities providing registration services would make sure that fees would not lead to discouraging submission.

And I know this is also discussed in the ICANN remit. And we have also made that point in the ICANN remit, that fees -- if there are fees, should remain certainly cost base and not discourage submissions.

JOANNA KULESZA: Thank you very much, Olivier.

I would like to take the opportunity to propose Peter's question to our panelists. And that is, indeed, targeted at our panelists. It does have a ccTLD and a gTLD angle to it. Please let me read it out.

What are the panelists' views on the following: National or regional regulatory initiatives typically affect both the ccTLDs and gTLDs. How can ICANN interact in legislative processes while staying within the limits of their mandate and avoid conflict with ccTLD interests or positions?

I might assume Alejandra might want to take that question on first. But if there are answers from other of our panelists, I welcome them to raise their hand.

Alejandra, would you like to start us off?

ALEJANDRA REYNOSO: Yes, thank you, Joanna, for the question.

In terms of how we, the ccTLDs, might cooperate with the gTLDs, there's always room for collaboration. We always have fluent and smooth communication in place.

In terms of the impact of the regulatory measures on ccTLDs, this clearly depends on the region where these initiatives originate. And then, of course, we need to take into account different agreements and conventions among countries that go beyond the originating region. Hence, it's complicated to seek a collective solution because every -- or each ccTLD has to adapt these initiatives to their local country's jurisdiction.

But, again, if we can share and exchange experiences and we can learn from one another, this will give rise to a space of innovation so that whoever is facing the same challenges can learn along the way. Thank you.

JOANNA KULESZA: Thank you very much, Alejandra.

I'm curious if our panelists have other replies. The question was also referencing gTLDs, if Philippe has anything to add to this question or as discussed before. Feel free to take the floor. Thank you.

Philippe, go ahead. If you are speaking, we cannot hear you. I can see your hand is up. Yeah, go ahead.

PHILIPPE FOUQUART: Thank you, Joanna. I will just -- again, the question was quite general. I would just reiterate what I said earlier about the need -- the question is about interacting with lawmakers nationally. And I think there's a need for the GNSO community, the community as a whole, to channel our inputs to those especially within Org who contribute to that evolution among many others.

And I think that's the length that we are sort of missing, even more so given the format that we're in at the moment. It's the sort of discussions we used to have in face-to-face meetings, in corridors, where those inputs would be carried across informally. We do not have that anymore, I think. And we probably want to reinstate this.

So, yeah, we need to channel our inputs to make sure that misunderstanding such as those that were flagged earlier would be corrected moving forward. I hope that's helpful.

I'm also interested in the next question, your comment to that, Joanna. Thank you.

JOANNA KULESZA: Thank you very much, Philippe.

If Matthias or Fred have anything to add at this point, feel free to raise your hand.

But I will move forward to the next question which also targets all of our panelists.

Matthias or Fred, is there anything specific you want to add at this point?

Matthias, go ahead.

MATTHIAS HUDOBNIK: I mean, just in general, it's not directly related to the ALAC, but I think it's always -- the challenge will always be to bridge the gap between, for example, as I mentioned before the GDPR which is a regulation directly applicable in all the European member states and then agreements which ICANN, for example, has with registries or registrars that they are compliant and that find their way in this ecosystem. On the one hand, the lawmakers which are adapting new laws and, on the other hand, also to find a way which is technically feasible for the community and also for the multistakeholder model.

And, yeah, serving on the one hand. And I think it will be even more complex as Philippe already said. Thank you.

JOANNA KULESZA: Thank you very much, Matthias.

Fred, if you have anything to add, feel free to chime in. If not, we can swiftly move to the next related question.

FRED BAKER: I don't have anything I want to add at this point.

JOANNA KULESZA: Great. Thank you.

I will move to the next question. There is no GDPR in the question itself, but we do have the EPDP. A question from Fabricio.

Based on these conversations, it seems irresponsible to develop WHOIS policy that will likely conflict with approaching law. Do the speakers think ICANN should pause EPDP work to accommodate governmental developments we've discussed here?

Philippe, I see you are typing. If you would like to answer that question live, that would be wonderful.

PHILIPPE FOUQUART: Thank you, Joanna.

This is Philippe here.

And thanks, Fabricio, for the question.

The question was put in a radical way. I'm sure people will understand I cannot answer in the same way.

I mean, pausing, suspending everything we do doesn't seem to be on the table. Appreciate the argument that it's a moving target, should we wait that the target has settled down for us to sort out the solution.

What I can say on this is that also mindful of the resources, limited resources, as a waste within the community to actually do the work, we need to focus. And I think that's implicit in the question.

Yes, we do need to focus. We do need to complete the things that we've achieved already, implementing moving forward with the SSAD, for instance; completing Phase 2(a) as far as the GNSO is concerned.

As to pausing, suspending defining triggers, et cetera, as I said, the jury is still out. It's very much to the community and not to myself to decide.

But the point is really to sort of identify our interest or main points in the evolution.

As I said, those are -- for most of them, they're not quite new. They're not quite new. In terms of topics, we pretty know what's coming at us.

So there is, indeed, things that we can move forward with. But, again, I would stress that the -- our resources are scarce. So we do need, even at council as far as the GNSO is concerned, think about what we can achieve in that respect. Thank you.

OLIVIER BRINGER: Joanna, may I also jump in?

JOANNA KULESZA: Yes, please do.

Go ahead, Olivier.

OLIVIER BRINGER: So I would not agree we would need to pause the process in ICANN, as Philippe was mentioning. We have been working and the Commission as part of the GAC has been working also hard in the different ICANN processes.

And, again, our idea with the NIS2 proposal is to have a legal framework in place when it becomes applicable. It could point to policies and guidelines developed in the ICANN process. So by that time, which sometimes take a bit of time in the European Union, we would really expect to have the policies, in particular the policy on ICANN, finalized and implemented. That would be really our preference.

JOANNA KULESZA: Thank you very much, Olivier.

Since you are taking the floor, I'm curious if you would like to pick up the question from Mark Svancarek we are seeing in the chat. I will read it out for those of you who are only on audio participation.

It is welcome that both NIS2 and second additional protocol to the Budapest Convention define legal bases for the disclosure of WHOIS data. However, neither seem to clarify the impact of GDPR

Article 22 on WHOIS processing. Until it has been confirmed whether or not Article 22 applies to WHOIS disclosure, we should expect that manual inspection of disclosure requests will continue, meaning that many high-impact cybersecurity use cases will remain unavailable.

What is the position of the European Commission on GDPR Article 22? If the position is that Article 22 does not apply, how is the European Commission planning to ensure that this position is represented in a member state's law when the directive is transposed?

Mark, thank you for the question. I leave it to Olivier to respond.

Let me just note, this session in itself is not focused on GDPR. It seems to be a very lively theme. I'm noting this also in the chat. I leave it Olivier's discretion to decide how specific you would like to be in that answer.

But there is a dedicated GDPR session tomorrow, as Matthias already noted. This does seem to be a very lively theme within the community.

Olivier, if you wish to take that question, do feel free to do so. But I just wanted to note that there are other venues where GDPR and the application thereof is being thoroughly discussed within ICANN.

Olivier, go right ahead.

OLIVIER BRINGER: Thanks, Joanna. I would prefer maybe to take this question bilaterally because I must say I don't know GDPR by heart. And I would be -- it would be difficult for me to reply precisely to the question.

But as I mentioned, the NIS2 activities is about increasing the level of cybersecurity in the E.U. It is not about implementing GDPR. It is in conformity with GDPR, but it is not about implementing. So you cannot expect to have interpretation of one or the other article in an instrument like NIS2.

But this is a precise question, and I would be happy to take it bilaterally with Mark.

JOANNA KULESZA: Thank you very much, Olivier.

And now I would like to combine questions from Mokabberi and Sharon that both deal, to my understanding, what we call DNS abuse and what the outside world often refers to as cybercrime.

Mokabberi asks: As you know, pornography contents and services are considered illegal in some countries' laws based on their social and cultural values and respecting family values, especially child pornography. How ICANN could help in this regard to fight against illegal activity and establishment of domain name management mechanisms, for example, domain name system for adult XXX content, according to the national laws at DNS level?

That's a very interesting question.

And the question from Sharon: Does the Budapest protocol discussed apply only to requesting authorities with a legal mandate under criminal law, or are there other types of national authorities also captured under the protocol? E.g. authorities in signatory countries with compliance and enforcement mandates under civil law.

Alexander, this looks like a question for you especially when we talk about child pornography and pornography and child abuse.

I'm curious if you would like to pick it up. And I'm also going to check with our panelists if there are any answers to these two which I think have a shared theme of DNS abuse.

Alexander.

ALEXANDER SEGER: Thank you. I believe when it comes to child abuse, I don't know of a country that specifically permits child abuse, sexual abuse of children. I mean, there's different positions it comes to adult pornography and that sort of things.

So I don't see any particular reason for not cooperating on child abuse, child sexual abuse online, in particular because the Budapest Convention itself already contains Article 9 on so-called child pornography. So I don't see an issue there.

When it comes to areas where some countries have, let's say, criminalized adult pornography, others not, then, of course, sort of dual criminality considerations come in. Only those countries that have the same type of criminalization would be able to cooperate with each other but not everyone. I think that's the situation.

And now, the question from Sharon. Okay, once -- so next year hopefully in spring, the protocol will be open for signatures. And parties will implement it. And then we have parties to the protocol. So the protocol only applies to those that have ratified it, that have undertaken the commitments, the obligation, but also the rights under the protocol.

So I'm not sure I understand the link to the civil law here.

Actually, sorry. It's a criminal law to the Budapest Convention and also this protocol is a criminal regulatory. It applies to specific criminal investigations and proceedings. And it applies to competent authorities in this case requesting or ordering the direct to be produced. That's criminal justice authorities.

There's a specific definition in Article 3 of this protocol defining what competent authorities are. So, sorry, would not apply to civil law and issues, I'm afraid, no.

And just on maybe if I can add to one of the previous questions. I couldn't find the raise-the-hands button here anywhere.

And just on -- if maybe I could answer to one of the previous questions, I couldn't find the Reyes raise the hand button here anywhere, maybe also wondering when this protocol was negotiated, should we wait for ICANN having come up with this expedited policy development process, having come with a conclusion, and we should wait, then, before designing Article 6. And we said no, we cannot wait for that because we have a time limit also for this protocol. But, therefore, also, because we have such an interest, we decided in such a flexible, pragmatic way that it should work with any solution that comes out from the -- in the ICANN process. So I have little doubt there.

However, this question of GDPR, it's not for me to interpret Article XXII of the GDPR. It's, of course, important when it comes to practicality of whether you can have automated processing or not. But a priori, the legal effect comes in in particular when then there is an investigation later on, and not when the data is transferred at that point yet. So when it comes, then, to the legal consequences -- namely, there's an actual investigation taking place, prosecution, criminal proceedings -- that's where the legal effect comes in. But again, it's not for us to interpret Article XXII. That's for Olivier and other people in the European Commission or even the court in Luxembourg.

Thank you.

JOANNA KULESZA: Thank you very much, Alexander. This is really, really an exciting discussion, and thank you to our panelists for agreeing to take all of these questions.

My job as a moderator is primarily to stay focused on the time. Now, I am being helped here by our wonderful staff, but I have been informed we just have three minutes left. So I'm curious if any famous last words from our speakers, our panelists should be shared within the two minutes remaining, and then I would like to try, which is going to be challenging, and summarize this discussion and invite everyone to join us for further sessions this week where specific issues, like the advancement of the multistakeholder policy development model and GDPR and DNS abuse and reputation blocklists will be discussed.
If our panelists have anything they wish to share they haven't had an opportunity to do so yet please feel free to raise your hand.

Thank you very much, panelists. That is a very disciplined group. Thank you very much for making my job easier.

With that, please let me summarize.

Thank you again for giving us examples of European legislative processes that welcome the multistakeholder input and thank you for taking on all of these specific questions and concerns as they came through the Q&A pod. And I observed the very lively discussion in the chat itself.

Clearly the purpose of this session was not to give specific solutions to a very complex landscape that national regulation and ICANN processes form. Rather, it was to raise awareness about how challenging these processes are, and to try to put our heads together on how best to anticipate further legislative progress and make sure that it reflects the multistakeholder nature of DNS management.

I hope that this session has added to the awareness of the community how our internal discussions on EPDP, on DNS abuse feed into different regulatory initiatives in Europe and beyond.

As noted previously, the purpose here is for us to stay aware of what legislative processes are in development. Please let me note we have tried to invite more examples, and it has proven tremendously challenging.

I want to take this opportunity to thank everyone who helped develop this session. I've already thanked at least twice our panelists, but again, thank you very much for taking the time.

Special thanks to the GAC and Nigel Hickson who was wonderful in setting up the agenda and inviting our speakers. Thank you to the GAC participants who took part in the organizing sessions.

This collaboration with the Governmental Advisory Committee and, as our panelists noted, with respective communities working in their local -- local environments is essential to make sure that we learn from past lessons. And I'm not going to use any acronyms to describe these past lessons.

We are exactly at the top of the hour. Thank you very much to everyone who participated. I understand it's not a finished discussion, but I hope that it was a useful introduction to one.

Thank you, everyone.

This session is adjourned.

[END OF TRANSCRIPTS]