PANAMA – Cross-Community Session: Accreditation and Access to Non-Public WHOIS Data Post-GDPR
Tuesday, June 26, 2018 – 17:00 to 18:30 EST
ICANN62 | Panama City, Panama

STEVE DelBIANCO: All right. Good evening, all. My name is Steve DelBianco. I'm your moderator for this session from 5:00 to 6:30 on accreditation and access to nonpublic WHOIS data. So the first thing some people are wondering is: Didn't we just hear this? Well, to some extent you did. Any discussion of GDPR, the temp spec, and ICANN's way forward involves how do we handle the current situation as well as how do we fix it going forward. So I get that. So we are going to work hard for some distinctions between the panel that just finished and this one.

The first is that we will use pictures and a lot less slides with words. And the second is I think we are going to try to get extremely specific about the roles that three tracks will play at getting from where we are to where we need to be on accredited access. Those three tracks are represented by the three blue bars on the diagram. One being the community itself, the middle being org, and the bottom being the DPAs. Stephanie, I know that might not just be European; but for the time being, it's European. And across left to right on that slide, we represent with time. ICANN Org is in the middle because they play a vital role right here. I'm going to invite the panelists when they

answer our three structured questions to do our best to explain that accreditation may well happen through legal proceedings, opinions, and guidance by accrediting bodies outside of the community and probably outside of ICANN Org.

But the one part that org and the community can control is once an accredited entity makes a request, it's ICANN's policies and implemented procedures then that fulfill that request, that track how long the data may be kept and what may be done with it. And that is the ability for us to get specific in this panel. Whereas, the previous one was more general.

You'll notice that the time frame on here is one year to do this EPDP. At the same time, we are trying to get some advice and guidance and opinions from European regulators. That's a big lift, but as the CBs' motto is, "The difficult we do right away at ICANN. But the impossible, it takes a bit longer." That may be what it is, impossible.

On the previous session, you heard how it is working so far under the temp spec adopted by ICANN. So look at this picture. As Laureen talked to you about, the temp spec held the registries and registrars must provide this reasonable access for people who have a legitimate interest. And that's in the lower right-hand corner. Any request of a legitimate interest would presumably receive nonpublic registrant data, unless, however,

those interests are overridden by the interests of fundamental rights and freedoms of the registered name holder or data subject. And that's the red text in that block because that determination is extremely complicated. Different parties will apply different standards to figure that out. And it's risky for contract parties to make the decision of that balancing act between legitimate interests and the data subjects' rights and freedoms. It's risky because if they get it wrong, it could get expensive. It's already getting expensive for those who request the data since they have to devote so much more time to work to get it. I'm pretty sure we can do better.

So we have got an expert panel here today. I will do a fast introduction. We'll start down at the far end. We have Goran Marby and John Jeffrey, ICANN CEO and general counsel. They'll wave.

Last week most of you know that ICANN published a framework for unified access model for continued access to full WHOIS. And that's been abbreviated as the UAM, right, the Unified Access Model.

Moving down the line, we have Fabricio Vayra, leader on the drafting team for the IPC BC model for accredited access.

Next to Brian is Alex Deacon. He's with Coal Valley Consulting where he represents some very large brands and content

owners. And Alex represents the business constituency on this panel.

We then have Keith Drazek. He's with VeriSign, and he's councillor for the Registry Stakeholder Group.

We have Cathrin Bauer-Bulst, European Commission and also the GAC's Public Safety Working Group.

Mike Palage, an attorney who has been involved with ICANN since the creation and claims to have helped resolve complex issues that we've all tried to forget.

[Laughter]

Like the UDRP, domain name tasting. Do you remember that one? He's the author of the Philly Special accredited access model. That's one of the reasons that Mike is up here to talk about that.

Then we have Rod Rasmussen who is the anti-phishing working group leader. But he's also chair of SSAC. For those of you who are new to ICANN, SSAC is ICANN's Security and Stability Advisory Committee.

And we also have Stephanie Perrin, Noncommercial Stakeholders Group. I have to remember to add "spending 30

years as a data protection professional with the Canadian government."

Fantastic.

So what we have for this panel are three questions. And across the Board, we will work up and down the line to give two minutes to answer these questions with a level of specificity that will enable us to understand how do we get to where we want to arrive to where we are today.

So the first question -- and I think I will start with you, Stephanie, on this one. We are asking you: What are the most important characteristics we need in an accredited access model as far as you're concerned? Stephanie.

STEPHANIE PERRIN: Thanks, Steve. I think the first thing is clear definitions because as I said in the previous panel, we have some things being conflated here. And forgive me if I didn't say it in the previous panel and said it in the GNSO working group all day. I think there's a parallel universe here in ICANN where we're using words differently. It's like Humpty Dumpty and Alice in Wonderland. This model is disclosure. It replaces the existing instrument of disclosure, which is full access basically. And

there is an attempt to replicate that as quickly as possible. That has been a goal of this exercise.

However, from a data protection perspective, you have to look at it as a disclosure instrument as an implementation mechanism. We haven't determined the policy parameters, and those policy parameters we need to define.

One of them would be as a holder of data, you have the nexus with the individual who has the fundamental right. You have a responsibility to ensure that whoever you disclose the data to, you know who they are. You have reasonable business practices that surround your identification of that individual or entity, that you are -- have reason to believe that they will respect the data protection law and that is not some piece of boilerplate in a contract.

People say that the GDPR is complex. One of the beauties of the GDPR is that we are moving beyond boilerplate. We are now seeing specific requirements under the law to pull out what we expect in expected behaviors. And that means how do you distribute the liability in the case of breach? That has to be spelled out. How do you -- details about retention. If you're not checking that, you're not doing your job.

So when I say we need to start listing things, these are the things we need to list. You can't build a model until you know what you're building.

STEVE DelBIANCO: Stephanie, I think the coffee has kicked in. That was excellent. Two minutes on the nose, and it's definitions and distribution of liability.

Rod.

ROD RASMUSSEN: Thanks, Steve. So I wrote down a few things that we should be looking for. It needs to be consistent across sources, the delivery methods, the formats used, and the rules applied for how access is delivered.

It needs to be clear. The rules for access and usage need to be clearly enumerated and the processes well-defined and available for various users to be able -- to be able to get access to data and to run those data systems.

Usable, scalable. This is an extremely important portion of this. And with proportional encumbrage -- I think I'd coin that one -- for the types of purposes you may be using it for, in other words,

the amount of effort you go to, may be proportionately higher depending upon the bar.

Useful. It needs to be timely. It needs to provide the data needed for the purpose and for -- and just for that purpose. So, in other words, that's a bit proportional as well.

Accountable. All the parties that are involved in the entire process are held to standards, understand those standards, and agree to those standards. And security and privacy by design from the ground up, which is something we all in the software industry tend to miss.

I would just like to quote from SAC3 because we were talking about history a little while ago. SAC3 written in 2002, December 2002, stated that WHOIS must be both accessible and usable. And also stated, WHOIS services must provide mechanisms to protect the privacy of registrants. And that was in 2002. So SSAC has been on this for a little while. Thanks.

STEVE DelBIANCO: Thank you.

Mike Palage.

MICHAEL PALAGE: Thank you, Steve.

I believe there are three characteristics that I would be looking for in any accredited access model. The first is accountability. There needs to be an accountability safeguard to empower data subjects to seek recourse when an authorized user has exceeded their scope of a legal and legitimate scope of authority.

One of the key aspects of the Philly Special is a ADR-like component that is analogous to the URS. All of the other models proposed to date have focused on the denial of future access, without addressing those data subjects that have already been harmed. And I think that's somewhat problematic. And, again, I look back to a historical point with the UDRP that we drafted over 20 years ago where we were trying to balance both the rights of the trademark owner as well as the domain name registrant.

The second point is adaptability. As Stephanie pointed out, there are over 120 national laws. Privacy is a very dynamic area of law internationally. However, not all governments are adopting a unified approach. There are some governments that are actually adopting data localization that adds its own levels of complexities.

So I think what we need to do is to develop -- design and develop a system that maximizes the business certainty for the contracting parties, the registries and registrars that will be

required to deploy these systems, while balancing the fundamental privacy rights of data subjects versus the legitimate interests of users of this data within both the private and public sectors.

The final point which I think is -- should not be overlooked -- and this actually goes to a point that Goran has raised in the previous panel, in Heather's comments about -- I think he said the budget. And this point is economic viability.

I believe that any final model should not place an undue financial burden on any one party. I believe there are lessons to be learned in connection with the deployment of the trademark clearinghouse that can provide guidance to the community as we move forward. Thank you.

STEVE DelBIANCO: Thank you, Michael.

For those who are not familiar with the point acronym Mike used, it was ADR, alternative dispute resolution. One thing I know you are big on.

When I read the Philly Special, a word that really caught me was this notion that we would make data subjects whole. You make them whole. In some sense, that sounded to me like you have a

notion that people will get paid if their data was used in ways that it shouldn't to make them whole.

So when we get to the next round, I would love to have you expand on your notion of making people whole.

Cathrin, your top priorities?

CATHRIN BAUER-BULST: Right, thanks. I want to start with one top priority that was already identified on the earlier panel. We need to cooperate constructively and honestly throughout this process.

So I just need to clarify one aspect up front that the GAC chair has asked me to remedy. There was a misrepresentation about elements of the GAC advice being deferred because they were not compliant with the GDPR. That is not correct. Those elements are compliant with the GDPR. And they were deferred for practical concerns because ICANN Board and Organization did not see themselves in a position to actually implement those at the time.

GORAN MARBY: I have to formally say that's not the case. Thank you very much.

STEVE DelBIANCO: You'll have four minutes between you and John to cover this.

Cathrin, please continue.

CATHRIN BAUER-BULST: I think we're going to take this outside.

[Laughter]

[Applause]

GORAN MARBY: Actually that's something -- we never do conversations like that off line. It's important to put on the record things like this.

CATHRIN BAUER-BULST: Right.

So returning to the key priorities for access and accreditation, we discussed these questions in the GAC this morning. And timely and reliable access, as will not come as a surprise to you, is the key element for the GAC in any future WHOIS policy.

We need a unified, single, and comprehensive framework that provides legal certainty to all the participants.

And there's four levers or -- the four As we can call them that we can use to achieve a balancing between privacy and access interests and those are: Accreditation, authentication, access, and accountability.

So just a few more words on those four. On accreditation, the GAC supports creating different categories. And in particular, it welcomes any recognition that law enforcement falls into a specific category of its own and does not rely on legitimate interests but rather a basis in law.

We also recognize that ICANN cannot serve as an accrediting authority in particular for public authorities.

On authentication, there needs to be a uniform and user-friendly manner according to a common standard for authentication to be provided. And depending on the purpose that is being pursued, the requisite level of access needs to be set, so be that to the complete dataset or to the appropriate data elements.

On access, we need to have technical means of using the authentication to obtain the requested data again in an identified and user-friendly manner. And we need accountability on all sides. So there need to be clear rules about how the access is managed, starting with how to treat lookups, ensuring timely turnaround, but also extending to the rules of misuse of data so holding both sides accountable. Thank you.

STEVE DelBIANCO: Cathrin, you are one of the triumvirate at the bottom of this row. You are with the Commission. The data protection board and governments in Europe, would they share these same four As that you articulated for us today?

CATHRIN BAUER-BULST: I think what's -- we've heard certain mantras already about how this is the law. But I will repeat one of the mantras that we have already had as the European institutions, which is that the GDPR does not prohibit data processing. The GDPR asks us to consider how data is processed and to do so in a responsible manner for legitimate purposes. And that is what we're trying to do through these four elements.

So I believe that depending on the details, the data protection authorities would very much welcome that we use these four aspects to achieve the right balance.

STEVE DelBIANCO: Great. So it's permitted. But for ICANN to mandate it, we need the legal certainty that we're going to need.

Goran, can you -- can you wait or would you desperately want to get in now? Go ahead.

GORAN MARBY: I want to ask a question then because we have not received any information from the European Commission that we should stay with the open WHOIS. Despite that, the European Commission has said that what we have implemented is very good and also sort of recognized by the European DPAs.

So for the record, we have not received that information from the European institution or the European Commission. Thank you.

STEVE DelBIANCO: I bet Cathrin is going to forward an email to you as soon as you get back to your computer.

Keith Drazek, critical factors for an accreditation and access model.

KEITH DRAZEK: Thank you very much, Steve. Keith Drazek.

So I'm detecting some themes here so far, and I expect we'll probably hear some more. The four most important characteristics that I've identified are: Legal, it has to be legal; scalable; predictable; and variable. And I will speak a little more in detail about each.

I mean, any accreditation model, accreditation and access model, clearly needs to be based on sound legal principles and consistent with the law. And that is one of the challenges obviously that GDPR is currently presenting to us and also not exclusive to GDPR. Obviously there are other data protection requirements around the world that we need to be sensitive to.

It needs to be scalable. Particularly for providers, whether that's registries and registrars or the accrediting bodies themselves. It needs to be scalable. It needs to be standards-based implementation.

It needs to be predictable for users, whether it's law enforcement, intellectual property, security researchers or others who have legitimate purpose. They need to have a predictable implementation that they can rely on to make sure it's efficient and effective.

Finally, variable. I think this is a really important point. Whatever model we design as a community, accreditation access, a uniform accreditation model, unified accreditation model, whatever we're going to call it, it has to be variable enough to account for different jurisdictions and different user groups. So if you can imagine a matrix where we will need to be able to turn the dials to accommodate or -- yes, to

accommodate the different interests and the different requirements in various jurisdictions. Thanks.

STEVE DelBIANCO: So, Keith, if someone was authenticated for purposes of certain European jurisdictions, we shouldn't assume they are also authenticated for a data subject's information in Brazil, for instance? There would need to be variability on that arrow that you couldn't assume that all accredited investors in all cases apply to everyone. That's helpful.

We will go to Alex Deacon next.

ALEX DEACON: Thanks, Steve. It's Alex Deacon.

So I think the most important characteristic is that a framework exists as soon as possible. And it needs to be one that mandates a unified global access to public RDS data to those who have been properly accredited and authorized. And that is that it must operate in a predictable and consistent manner globally across all RDAP services, be they registry, registrar, or whoever.

If it only works sometimes and in some places, then I think we've failed at the task. You know, I think we as policymakers, it's important to always keep in mind the ultimate goal here,

which -- and where we need to end up in terms of implementation. And I know there should be and will be a separation of implementation and policy as we move forward here. But given the time frame we have, I think it's important that they inform each other moving forward.

And implementation I think, it's been agreed that it will be RDAP. And I believe it should be secured a technology such as OpenID Connect.

To get there, we need to answer some important questions, right? It's: Who, why, what, where, and when. The "who" defines two things, who gets a credential. That's the accreditation piece and once issued identifies who is asking for RDS data. That's the first part of the access decision.

The why is the second part of that decision. The why conveys the data that is unique per request. things like the purpose; an indication of a legitimate interest of the requestor, for example; and perhaps things like the domain name or set of domain names that's being requested, the data is being requested for.

Once we know and have authenticated the who and the why, then the what follows. The what is what data is returned to the requestor. And finally there's a concept of where and when. And that's important as it represents the logging of all of these requests made in the system. And that data is used to monitor

for abuse, investigate abuse, ensure third-party auditing, and enable a transparent and accountable system. These are very important things. Of course we have to account for law enforcement requirements.

So understanding how the policy will impact implementation and defining the who, why, what, where and when is important.

STEVE DelBIANCO: This is like a competition for the best alliteration in response to a question.

Did you guys get these questions beforehand? Did somebody leak them to you? You guys are too good.

But Alex is trying to make a distinction here that the accreditation, the lower right-hand corner, probably happens outside of ICANN's orbit. Once accredited for the who, presumably for the what they usually do, then it enters the ICANN orbit. As the requests are made, RDAP is used to fulfill the request, to log the request, and then our policies could mandate it. Because you're the first one to use the word "mandatory" in this group.

Thank you.

Fabricio.

FABRICIO VAYRA: Thanks, Steve. So I'm thinking about this as we went down the row. To me the most important characteristics of an accreditation model, accreditation access model, are accreditation and access. And I don't say that to be funny, and clearly it wasn't to any of you.

[Laughter]

I say that because as an organization and as a community, we tend to sometimes overengineer things and miss the point of what it is we're out to do.

So I echo what our colleagues have said down the row about the things we need to have in such a model, but we can't lose sight of what it is we're trying to create. And what we're trying to create is a model that actually affords an accreditation process to allow access. And let's not lose that, because I think we might very well.

The only other two things that I would add are, to Keith's list of themes, I think -- it wasn't on your list -- we need some sort of uniformity. And it's not uniformity of what the model does to accredit but most importantly, how we allow access. We've heard from all day -- I'd say all day long the words of fragmentation, inconsistency, and this model has to go a long

way to resolving that because regardless of whether we have 30 really great accreditation access models and they all allow us to accredit and they all allow us to access, if we have 30, the inconsistency and the fragmentation will do about as much harm as us not having one at all. So uniformity is a big thing.

And then let's not forget that the world did not stop running on May 25th. So the cybersecurity professionals who are out there trying to keep us safe, the calls that I get on a daily basis from consumers where they've been defrauded and they want my help, that didn't stop. And so we need something a little bit more immediate than something that's going to come in 2019.

And those would be my most important things.

STEVE DelBIANCO: Thank you.

Goran.

GORAN MARBY : I think that, for me, the most important thing is that the community actually agreed on a unified access model, which I refuse to do an acronym for a different name for.

The -- I have many suggestions which has been refused.

So as someone have said before in the former panel and so repeated, the more we come together on a unified access model, which then contains different accreditation models, will make a difference there. And the reasoning for that is there could be different laws or different interpretation of the laws that give different user types access to the data. For instance, law enforcement could have a set of laws that makes it possible for them to reach the data. Investigative journalists could have another set. We don't know that. And that's why we make this difference; not to complicate this or something. So that's probably for me. You know, I'm not a member of the community. I don't drive that.

The other thing is of course that it's legal and also protects the rights of the individual which information which is in the -- which is in the system.

But this is not -- it's not a simple thing. First of all, I think most people now agree that it's not, say, the legal basis for having a unified access model is not an easy thing to say. So we need to find together with the European Commission, the European member states and the DPAs the legal basis for doing that.

I would like to also congratulate, EUROPOL is doing work to come up with the reasoning for -- to have a unified access model with the combining accreditation model moving forward. They

do some very important work there. They sort of also realize, they face the same problems that we do in the sense there has to be a legitimate basis for the models themselves.

I also think, what someone said, it also has to protect the individual user, but it also actually have to -- we have to think about this from the contracted parties' house. There is asymmetry in this which is not really foreseen in the law, and that is that the law sort of looks upon that someone collects data and then have the ability to use that data. For instance, for commercial uses. But here the asymmetry is that we -- you have actually decided that the contracted party should collect the data. So there's not a commercial interest to collect the data in the first place.

The next asymmetry, that ICANN Org has very limited use of that data. It's actually other ones outside the whole system who uses that data.

So just to finish off, just to give you some of the -- I mean, it's not even for law enforcement it's (indiscernible). For instance and in context with DPAs that have informed us that, for instance, if a law enforcement agency without the court order requests information from the WHOIS database from a contracted party, it might be so that the contracted party has to notify the investigated party.

So there are many things that we have to deal with, and many of those answers lies within the European Commission, the member states and the DPAs. And we have to work together.

We don't have a proposal for unified access model. What we're trying to do is the simple thing is that we're trying to figure out the legal basis for having ones in the first place by asking many questions going forward so we can provide that information to the community, to take into account the work.

Thank you.

STEVE DelBIANCO: Goran, thanks for that and that first chart recognizes this dialogue that must occur between org and the three legs of the European regulators. But you made a point on the previous panel that you would welcome members of the community, the top row here, to also help you with questions that would be fed in to help determine not legal certainty but to reduce the risk that a mandatory, nonpublic WHOIS access would not run afoul of the GDPR. And I understand we're supposed to work together to work towards getting, in the best case, binding opinions from European regulators but it might only be that we get guidance. And all that will occur over the next several months.

At the same time this EPDP is running to examine how do we implement the temp spec with real policy.

J.J., anything to add from ICANN's perspective?

JOHN JEFFREY: Yes. So I think it's really important for us to frame the GAC advice against what we believe we received from Article 29 and the DPA advice and what's been published in the Berlin group paper.

So if we look at, for example, the top three or four areas where we believe the data protection advice in Europe is different than what we see in the GAC advice, I'll just outline a few of those. And I'd love to be reeducated on this. If somebody has a different view or if they have an indication that this is -- this is -- these are consistent, then this is the kind of thing we want to understand from the community. For example, whether the registration of both legal and natural persons are affected. Whether the registrant email is okay to be published. Whether the queries can be anonymous or whether they need to be logged. Under data retention, the GAC notes that best practices are two to six years minimum depending on the industry, but that's not what we're hearing from data protection authorities.

So those are the kinds of issues that if we've got it wrong, help us understand the different perspective on it. But those are the things that, you know, clarity around this, legal clarity on this is going to help us and it's going to help the contracted parties be able to go and implement this.

So I think it's very critical that we have an understanding, because if we put together a unified access model but the contracted parties' lawyers are all saying to them, "We're hearing something different from the DPAs, we're seeing something different when we're having communications," then they won't implement it because at the end of the day, they are responsible when they're the collectors of that data to, as well as ICANN, to be responsible.

So I think this is a really critical thing. If we're getting elements of this wrong, let us know. If these are right, then help us to bridge this gap.

STEVE DelBIANCO: Yeah, that's helpful. All of you echoed themes of clarity, consistency, uniformity, so that it can be mandatory and applied across all users.

We're going to work now from Fabricio down toward Stephanie on the second question, which is what is your assessment ICANN

Org's proposed unified access model, which all of you've had a full six days to study, and that's more than enough, I'm sure. And I'd like you to assess how could it be improved? And there's an open public comment on that very question, but I'd like to hear your key ways in which it needs to be improved.

Fabricio, you're first.

FABRICIO VAYRA: So first I'd like to comment really quickly on what the model represents, which I applaud, which is ICANN standing up a process. I think, Goran, you and I, John Jeffrey and I had some frequent discussion during ICANN Puerto Rico, ICANN61 about standing up a process, and I'm glad to see three months later that a process is being stood up.

With regard to the model itself, I've reviewed. I've reviewed the charts. And I'd have to say that for it to -- for it to be improved, it needs to be moved beyond what it's self-titled; right? Which it's a framework for discussion. It's not really a model. So it needs to be fleshed out. And in order to do that, you need to go through the machinations that we've now gone through in the past three months in creating a 47-page document on accreditation.

You guys heard me talk about this earlier today, but we're in version 1.6 already of a model that's had plenty of feedback from plenty of people in this room, and I think would be helpful to use that data to then flesh out the conversational piece that Goran and group have put out.

So that's what I think we need to do to move forward, is actually flesh it out. And as brought up early -- in the panel just before this, I think this is one great example of where the community puts together a lot of product, work-product, and we shouldn't just throw it away. We should actually use it to our benefit.

STEVE DelBIANCO: And Elliot Noss and some of the other larger registrars have pledged to share the learnings of the real-life experience. We heard that on the previous panel and I think there's a panel session tomorrow morning on that.

FABRICIO VAYRA: Yeah, and if I could also say, I also heard on that panel that the model I'm speaking of, version 1.6 of the accreditation model, isn't a community model. And I think it's only not a community model if people choose not to make it. The invites were global. ICANN supported. Actually both Goran and J.J. were on the calls. We've asked everybody to input. If you choose to stand

outside the circle, there's nothing we can do about that. But it is something we're asking the whole community to put into. And if we're honest about doing a community effort, then the community needs to talk. We can't just say, well, we don't like that effort so we're going to take our toys and go home. We need to all participate and participate constructively, and that means an exchange, not just a "We'll do what we want," because that's not going to be productive.

STEVE DelBIANCO: And it would be good if the next version that you release is mapped more to the structure of the unified access model proposal, using the same vocabulary, to diminish the distance between the two.

FABRICIO VAYRA: Yeah. And we pledged in the last session, we are going to go through that. So about two weeks out from today you will have a model that follows, Goran, the tracks -- the conversational piece you put out and tries to mirror so it's much more easy to digest and compare and hopefully furthers the conversation.

STEVE DelBIANCO: Alex.

ALEX DEACON: Thanks, Steve. It's Alex Deacon. So I think the model is a great starting point but we need to flesh out the details. There there's more work that needs to be done. I think the fact that the unified access model was created to assess legal certainty and ensure there was a legal basis for access is important, and this work should continue in parallel with the work that's happening in the community.

As Fab said, I agree. I think we need to leverage work that's been done in the community before, whether that's the IPC-BC access to accreditation work that we've been working on, version 1.6. I also think there's a lot of great work and details in the recent SSAC document 101, and so I appreciate that effort, and we should be able to leverage some of what's in there.

And then, again, to echo what Fab said, I think it is important that, moving forward, we see any model that's going to be discussed within the community kind of use the language and the framework of -- of the -- that's outlined in the ICANN unified access model so we're really comparing apples to apples when moving forward.

STEVE DelBIANCO: Appreciate that. But did you really say "legal certainty"? Is that a thing or just an aspiration?

ALEX DEACON: I'm an engineer, so I'd be careful with that.

STEVE DelBIANCO: All right.

Keith.

KEITH DRAZEK: Okay. Thank you very much, Steve. So the question was assessment of the uniform access model that ICANN has put forward and how could it be improved. And first I'd like to acknowledge the work that went into that and acknowledge, I think, the value in trying to seek additional guidance from the DPAs on that document.

So I would like to thank ICANN for the work they did in pulling that together.

I would also like to acknowledge and thank the IPC and the BC for the work they've done on the registration and access model. Michael Palage who is sitting a couple of seats down from me as well as I think the Internet Governance Project. There has been a lot of really good work to try to flesh out some of these tough

questions around access and accreditation. And I think all of those will be very, very valuable inputs into the community policy work that needs to be done around finalizing some of these outstanding questions that Alex referred to either -- earlier, sorry. The who, what, where, how, why, and when.

So I think the right place for that conversation to now take place is within a policy development process, and whether that's a secondary PDP or some work track in the existing PDP, I think the GNSO Council -- I know the GNSO Council is still debating and discussing. But I just want to note that these are all very important inputs into a broader community-based policy discussion that will I think guide where we go over the coming months.

And, Steve, I want to reflect back on a comment that you made, is that some element of the accreditation model will be outside of ICANN's remit. The certification of the accrediting bodies, who determines that I think is definitely an outstanding question that is probably not within ICANN's policy-making remit. But I do think that one of the things in the ICANN UAM model that probably could use a little bit more work was the reliance on the GAC to play a role in that policy-making -- sorry, in the determination of who gets accredited and who doesn't. So probably some more work needs to be done there.

Thank you.

STEVE DelBIANCO: Thank you, Keith.

Cathrin.

CATHRIN BAUER-BULST: Yes, thank you. I'll agree with everything that has been said before about how this is a very good starting point, and we very much welcome this framework for discussion. And I've already outlined the main elements that the GAC particularly cares about, and I think there's hooks in this framework to address all of them, and now we need to urgently work on further developing them.

Now, as I said before, the GAC would like to see rapid progress in particular on the law enforcement issue, but we also need to make progress in guaranteeing access to other users with a legitimate purpose. And in that process we also should ensure that the process to access the data should be as simple and uniform as possible, and that's currently missing in the framework which does not yet provide any detail on this. RDAP was already mentioned as an option.

And just to say Keith already referred to the other models that the community has developed which provide that additional level of detail and which have thought about a number of the aspects that are not yet included in this framework. And that is helpful to us not just from the process perspective here but also if we want to get good guidance from the DPAs.

One thing the Data Protection Authorities have consistently requested is more detail on what we're actually trying to do. Again, the GDPR does not prevent you from doing anything, but you need to explain why you're doing it and justify where it's necessary and proportionate with the view to legitimate purpose. And that's what they need.

So the more detail we can provide to the DPAs using the different models that have been established, the more helpful input they can provide to us on where we need to make adjustments to the model. So we should use the community input here also to flesh out that model to put muscle and flesh on the skeleton that has been helpfully provided by ICANN.

STEVE DelBIANCO: Cathrin, are you sure you wanted to ask the ICANN community to give you more detail? This group can bury anyone with details, and I'm hopeful that that's actually going to help you get to the decisions you need, but you tried to put it on us to suggest

we need to make sure that there's an authentication scheme for other elements in law enforcement.

We still believe that that will be guided by the bottom row of this chart, and once an authentication scheme meets with your legal acceptance, we are happy to accept those tokens and answer those RDAP queries.

So so much of the work is going to happen in that bottom blue bar, but I realize that you do most of your work in response to questions and detail. So we will honor that request.

Mike.

MICHAEL PALAGE: Thank you, Steve.

So the three areas that I would recommend for potential improvements in the ICANN model are as follows. One would be accountability. Again, we talked about the ADR component. One of the points that you had raised is I do propose in my ADR component somewhat of a financial compensation to the data subject. In the -- On the list I proposed anywhere from a couple of hundred dollar. Stephanie has said that is way undervalued. I would submit that this is still in the spaghetti-throwing stages. But the one thing that I think Goran this pointed to earlier is

there were data privacy laws before. Why did everyone care? Fines got everyone's attention.

So I think some type of financial disincentive to bad actors is necessary in that accountability structure.

Two other points. Accessibility. One of the areas where I disagree with some of the models both by the BC, IPC, and by ICANN is having this data available at both the registrar and the registry. I believe that the registrar is best positioned to be the safeguard of this data as the gatekeeper. I believe that this is consistent with the advice that was in the Hamilton memos, talking about privity of contracts. And I believe that registrars are best positioned to protect their customers from future abuse.

Also, when you potentially have data localization laws, registrars are again -- are again best positioned to put enforcement mechanisms to comply with those national laws.

Finally, it is transparency. One of the things that I would like to really complement the IPC BC model is Appendix J. What they did is they gave a very, very clear delineated list of what they thought was legitimate uses. One of the things that I would advocate in any future model is that when an authorized request is made through the RDAP, that that user needs to specify what is the basis of legitimate use. So that if there ever is a challenge

by a data subject at a later data, they can go back and question what that is. So that's my final point. Thank you.

STEVE DelBIANCO: That last one, I think Alex Deacon said that's the "why." After the "who" is the "why."

ALEX DEACON: I think that will be covered technology-wise.

STEVE DelBIANCO: Fantastic. Rod.

ROD RASMUSSEN: Thank you, Steve. So just personal opinion, this is a really good start as other people have already indicated. It needs some fleshing out, but I think a very good place to work from.

Putting on a couple different hats from the SSAC perspective, we came out with SAC101 on Monday, the same day this came out. One of our recommendations was around access models. So thank you for doing that right away. Appreciate moving along that line. Very much falls I think in line in what we were talking about in that. If there is any misconception about that, we will try to clear that up. It seems to be well in line there.

I think there are some issues within talking about improving the model around clarifying and addressing issues around law enforcement and cybersecurity access in investigation-type purposes where the actual act of asking the question in and of itself will -- could tip off a subject of an investigation that's already having a chilling effect. When people ask why aren't we getting requests, talking to cybersecurity professionals and some law enforcement folks, it's because we're not going to talk to a registrar who made them turn around and tell a registrant -- these are things we talked about in EWG and other places. There are ways of taking care of that, but it needs to be addressed. I think that some clarity at this level would be helpful there.

Another particular is around -- I'm going to put on APWG hat for this one because APWG has been contributing around this for well. Just for clarity, I'm not the leader, I'm a leader in the APWG.

We have been working on a code of conduct there. There is a session of this that talks about the organizations that are the -- let me get this correct here. The authenticating body, as it was titled in there, would be responsible for monitoring compliance. I'm not quite sure how that's physically possible. So that needs a lot of -- there's a lot of here-to-there that needs to be addressed there. Those are my two improvement areas specifically. Thanks.

STEVE DelBIANCO: Very helpful.

Stephanie.

STEPHANIE PERRIN: Thanks very much. First point, what exactly do we mean by a "unified access model"? Classic example of a Humpty Dumpty use of word in my opinion.

STEVE DelBIANCO: Registries and registrars would have to operate under it.

STEPHANIE PERRIN: Yeah. But if you mean interoperable, say so. We all agree that an instrument should be interoperable. It is clear that Fab means "uniform," awfully close to "unified."

Privacy is contextual. You are not going to get the same. And we have had 20 years of the data protection authorities telling us that. It is contextual. It will vary by country. It will vary by circumstance. It will vary by purpose. So I don't like the use of the word "unified."

But that brings me to point Number 2, please can we follow due -- the appropriate ICANN processes here? This thing came out

just before the meeting while we were all packing up and dealing with our real lives before we came here.

We have had no input to it as a stakeholder group. We represent civil society and the end user in the noncommercial stakeholder group. We had a look at it. And very quickly on the fly came up with a list of requirements, which as I said earlier, is what we need at this stage. We need a list of requirements that we then build to. That's our view.

Have a look at the Internet Governance Project. It's up there. We will continue in our analysis of this, largely because we have to jump on this train and move with it.

And I'm sorry if I sound critical. I'm trying to liven up an otherwise awfully urbane discussion over something that is extremely controversial.

So we might as well get a peek of about what's going to happen over the next year right now. This is a wrong-headed way to go about this in my view.

We are now going with a model that doesn't have community input and consensus. And we are going to consult DPAs about it? That means I have to pester the poor souls with my analysis of it which will be informed by the way we look at it. I think this is not appropriate. And I have said this before.

Now, you want to cut me off here? Yeah? All right. There's more. Wait for it.

STEVE DelBIANCO: The third question would be a great place to slip that in.

Goran, before I turn to you and J.J., I think it's worth it for you two to recognize seven of eight, including this moderator, thanked Org for taking the initiative to lead from the top with this framework. Stephanie excluded.

We appreciated the gesture and the effort that is brought to it, knowing that taking that first step was going to bring a lot of arrows. But it still gets things moving. And I think you heard some generally supportive comments from everyone else at the table. So take a minute. Glorify in that and tell us what you think of the reactions you've heard.

GORAN MARBY: First of all, I'm actually closer to the last speaker when it comes to that. We haven't present the model. We are not taking -- we are trying to get some legal guidance for the ability for the community to have the discussion. And we are following the principles we did in the Calzone model by actually asking you.

I don't think it came to anyone's surprise because the DPAs has asked us for it. That's right. They also told us that they will -- there's no use for us to do it before August. We -- so the European Commission has asked us to do this as well. And actually -- when we presented the Calzone model, we actually wrote about this as well. So we are building on an assumption. And when it comes to the naming, we can always find a new name.

I will now reveal to you that the proposal we had was salted caramel gelato for the model.

But I want to go back to something that sort of underlies the question, and that's the engagement of this one. If you actually look at the model, you will -- that we have on the table, it's contradiction in it. We have actually purposely put different questions into it, so no one can even -- even if everybody agreed upon it, we can't implement it because there are contradictions in it today. And the reason for that is we want to ask questions to the DPAs.

So the first level is that we would like you, of course, to give us information and we will provide it to the DPAs and other ones the same way we did it before.

We also many times last time -- and I want to emphasize this as well. You also have your own -- your own ways of getting into contact with the DPAs.

For instance, we talk about the European Commission as this big thing that is one thing. And actually Cathrin knows this, the European Commission actually consists of three parts. The part who wrote or responsible for the law, DG JUST, is not here. Cathrin, for instance, represents another interest within the European Commission, which is police forces. And then we have the coordinator which is DG CNECT, who is responsible for the relationship with ICANN.

Then all of those things I think going forward, we also have to be better talking about those things because we want you to engage on the right level. And DG JUST always have an invitation, of course, to come here and talk about it.

And I want to emphasize -- I said this before, to get any guidance, it was actually a big thing that we got the guidance we got from the DPAs. And I'm extremely respectful that we got that. It was the help of DPAs, European Commission, especially DG CNECT was very helpful in that. And it was really good. And it was really multistakeholder model. It would be harder now because now we want to reverse it. Now it was by which we have to put under -- in the Calzone, under the hood. And how do

we now get -- in an asymmetric world, how do we get people to get access to the data and the legal ground we have for that.

And I more or less promised you, which many of you disagreed with, that I will give -- we were able to get some legal guidance from the Article 29 Group and then actually rectified by the Board. It will be harder now. This is harder than we did before. We really need the help of the member states. We really need from the European Commission especially from DG JUST and we really need it from the DPAs to be able to do that.

STEVE DelBIANCO: Thank you. J.J., Goran has left you only one minute to add sprinkles to the top of the salted caramel gelato.

[Laughter]

JOHN JEFFREY: I concur with the last speaker.

STEVE DelBIANCO: Fantastic. Now we are back on schedule for the last and final question, which is we have asked you to talk about your preferred way to implement the model. We're going to start with Stephanie. We're going to mark down the table about how should this be done.

I just threw out three ideas. I suggested that perhaps -- let me go to that slide for you -- that perhaps ICANN Org would do another temp spec. That was discussed at the last panel. Maybe GNSO Council should develop policy via an expedited PDP or two, one of them specifically addressing accreditation and access. And one I have pressed for over the last 24 hours is a notion for org to do interactions and discussions with European regulators at the level of specificity and questions to bring back the kind of advice needed so that GNSO Council and the community can develop an access method that will work once you have worked with the Europeans to figure out what accreditation looks like.

So, Stephanie, we'll start with you about your preferred way to implement a model.

STEPHANIE PERRIN: Stephanie Perrin for the record.

Okay. Firstly, may I just say that I used to be a director of research in policy in the Office of the Privacy commissioner Of Canada. And if I had an organization that decided to get everybody in it, let's say Royal Bank or Bell Canada -- and have them write us after they have been noncompliant with the law for 20 years, I can only -- I can't tell you how annoyed I'd be because this just doesn't make any sense. We should not be pestering the DPAs for this kind of input.

And if you're going to do it, then you have to do it globally because, as I said, there's 126 laws, okay? Let's not pick favorites. Okay.

How to implement this, as you can tell, I think it should -- perhaps I should be explicit. I think it should go to the GNSO. They're responsible for policy. We should do it sequentially. We should do the policy first and then do the implementation. As I said on the earlier panel, there's a price to be paid for being late. You don't get to stack so many things up. If you want to be an accountable multistakeholder organization and expect people to multiply themselves into five pieces and staff all these things, we cannot do that. It is not fair. It is not an equitable use of our process and our time, and we're going to have a stakeholder burnout. Thank you.

STEVE DelBIANCO: Thank you, Stephanie.

[Applause]

When you said "imagine how annoyed," I think we didn't have to imagine. We got a pretty good look at that right now.

Rod.

ROD RASMUSSEN: So the implementation -- the implementation side of this is really, you know -- there's -- I don't have a strong opinion around how we get the sausage made, we just need to make the sausage.

In your questions that you have thrown to us, you asked should we do a temp spec, a separate spec, another PDP? Should we get somehow org and everybody to work together? I think that last part is really the goal here, is getting people to work together. I think there were some frustration in the way that we got up to GDPR as in knowing what everybody was trying to do, especially when we -- vis-a-vis interactions with European data protection authorities. And while ICANN was very good about getting feedback to us about what was said, it's kind of wanting to know can we get together on the strategy of how to approach them, especially as we're being asked to go to various contacts we have to work through some of these issues.

I will put my APWG hat on. We have been working with European authorities right quite awhile on how to share cybersecurity data because we have some of the same issues. So we're trying to work through that. But it would be really good for organizations like us to be able to be on the same page as we're going through this process to help bolster the shared goals that we all have and getting the system set up. So better

coordination and shared goals that we can agree on to take as part of the process in working this whole thing through. Thanks.

STEVE DelBIANCO: Rod, that's helpful. You are the chair of SSAC. The other advisory committee we have been talked about a lot this week is the Government Advisory Committee. Both advise the Board but are being invited to please participate at every stage of this policy. Instead of surprising the Board with advice at the end, feed into it early. And I know that the GAC is committed to do that, and I'm glad that you are as well.

ROD RASMUSSEN: Just to -- I mentioned this yesterday in the open meeting. But SSAC did send a letter to the GNSO today with -- just to highlight the recommendations we put in. We have been part -- we have members participating in the GNSO process prior, and we continue to do that. And any clarifications wanted on that advice, we're here to help walk through that. And as things come up, we will, of course -- as they relate to SSR issues, we will comment on them.

STEVE DelBIANCO: Thank you, Rod.

Mike, what's your thoughts about the path?

MICHAEL PALAGE: So in order to look forward, I actually want to look back in history. And, unfortunately there's kind of been an inverse relationship between the maturity of the ICANN community and the ability of that community to act in a timely manner.

I would encourage everyone to go to the GNSO website. They actually have a chart there that lists the PDPs that have been undertaken with a start date and an end date. And when I was looking at it, I believe that it's been over a decade since a PDP has been able to be completed in one year. So that would give me a little pause before engaging in a second expedited policy development process.

From the history lesson, I noted in the Philly Special, the work that was done back in 2008 with the add grace period. And I think that is a relevant data point to look at because what happened there was while that PDP was going on, there were actually multiple registry service requests put in by registry operators seeking to solve the problem.

So I'm encouraged by what Tucows has done, and I would encourage other contracting parties to come forward with pilots. I think it's time that we think outside the box.

And I'll just end it on this: Failure to achieve our objective as a community in connection with the current EPDP basically gives rise to a systemic risk to the very bottom-up consensus-driven process that some of the people in this room have been working for, for 20 years. So I will end on, We got to get 'er done because failure is not an option.

STEVE DelBIANCO: I often hear that from my wife and kids, that my greater maturity reduces my efficiency. I think that's really what you have said.

Cathrin.

CATHRIN BAUER-BULST: Right. I just want to clarify the role of the European Commission. So if they so choose, it's for the data protection authorities and ultimately the courts to provide guidance, not for the Commission.

Just for the record, my life would be much easier if the European Commission only had three parts. I'm very sorry I apparently come from the wrong part. But I don't sit here representing my department. I sit here representing the European Commission.

We have really provided as much expertise and guidance as we legally can, in writing, in meetings, in phone calls, trying to

facilitate the interaction with the Article 29 and now the EDPD. And I can just re-iterate that we are committed to doing whatever we can.

Now turning to the preferred way to implement temp specs, EPDP, whatever, Laureen has already mentioned that access is already part of the temp specs. So we could consider elaborating on those temp specs at the end of one of the 90-day periods or adopting a separate temp spec. Whatever it takes.

The GAC, in any case, is of the opinion that we cannot wait for the end of this year, until next May, to see progress. And in any case, it should be part of the overall WHOIS policy which needs to take a comprehensive approach, as the EU data protection authorities, in fact, have pointed out. They have specifically called for ICANN to provide this model, as Goran has already said, because data processing governed by the GDPR does not stop at the redaction point. It also covers the processing of the nonpublic data that takes place after that.

So registrants and users need to have certainty about the entire process, including the conditions under which the nonpublic data is disclosed.

STEVE DelBIANCO: Cathrin, if in fact you and the EC could provide an example of an accreditation body that would be suitable for, say, law enforcement, and ask us to design systems that would accept that authenticated token and provide the responses, you would jump start, kick start the entire process, and it would be done within the entire remit of the Commission to do so. And I would invite you to consider that.

CATHRIN BAUER-BULST: And I can say we're already considering that and working on it with the member states.

STEVE DelBIANCO: Standing.

Keith.

KEITH DRAZEK: Thank you, Steve. Keith Drazek.

So the question was the preferred way to implement the access model. And I think unquestionably in my mind, this needs to be a community process run through the GNSO, and obviously with the participation and input of other parts of the community. And just to remind everything, if we expect contracted parties and the gTLD space to take on new responsibilities, be

compelled to implement a new accreditation and access model, and to have an enforcement capability from ICANN, that has to be the result of a consensus policy. And the only way to achieve a consensus policy is to run a GNSO PDP.

So I think it's incredibly important for everybody to understand that the GNSO is the home for this type of work, but I also recognize that the GNSO Council this week is considering the best path forward to tackle this challenge. And so the question of whether that's an EPDP, a PDP, somehow incorporate it into the currently conceived temp spec PDP, these are all questions that are being discussed actively by the GNSO Council.

I need to say, however, though I think the idea of requiring another temp spec to trigger this is unwise and, from a contracted party perspective, could be outside the eligibility of a temp spec. I think to carry on there, it is actually unnecessary to have a temp spec to be able to achieve an EPDP focused on an access model.

The GNSO Council has within its power today to trigger an EPDP without the triggering event of a temporary specification.

So just to note that this is something that the Council is actively working on, and I expect there is a recognition across the Council that this is a very, very important component of the work ahead.

So I also want to note that, as I said, this is a GNSO process but this is really going to be a community effort conducted through a GNSO PDP of some sort. And ICANN Org has skin in this game. So I would expect that ICANN Org would be an active participant in that process, probably needing the legal advice and legal guidance particularly around coordination with DPAs to make sure that the community effort is very closely coordinated with and informed by the conversations that are going on between ICANN Org and the DPAs as it relates to GDPR.

And again to note, at the end of the day, this is not only about GDPR. When we're talking about an access model or a unified or uniform access model, interoperable, whatever the word is that we're going to choose, this needs to be flexible enough to handle the variations in jurisdiction and user cases that I mentioned earlier.

Thank you.

STEVE DelBIANCO: Thank you, Keith.

And I would note that those I've heard mention a second temp spec were not doing so in order to trigger a Council process. Instead, it was to trigger immediate mandatory compliance with accredited access; immediately, as opposed to waiting a year;

right? And I heard Elliot say on the last panel bring it on because he'd rather disobey that than risk the fine.

Keith.

KEITH DRAZEK: Thanks, Steve. And just to follow that up, the current temporary specification requires registries and registrars to do certain things, and one of those is to provide access for legitimate purposes and legitimate use. We're not you know balanced by the legitimate interest of the data subject.

So we have today a requirement for registries and registrars to collect the data, to transfer the data in the cases where there's a thick registry, to escrow the data, and to make it available for legitimate purpose and legitimate user cases. That is all in the temp spec. And ICANN has made very clear that they will enforce, you know, for compliance around all of those issues.

STEVE DelBIANCO: Got it. But what's not in the temp spec is the lower right-hand corner of the diagram which would be that if one group of accredited requestors, such as law enforcement, provided authentication tokens, there's no mandate that all of you honor that. That is what a temp spec potentially could do. So making a distinction between the action of having it work and the

triggering of policy development at GNSO. Because we control that entirely within the GNSO.

Okay. Alex.

ALEX DEACON: Thanks, Steve. It's Alex Deacon for the record.

I don't have a strong opinion about what vehicle we use to do this work as long as it starts soon. Now would be cool.

I think that my gut -- my gut feeling is that the existing temp spec and the process that the GNSO is working on is the way to go as long as accreditation and access is, in fact, in scope of the EPDP. If it's not included, then, you know, I think it's incomplete in its effort to bring the WHOIS system into GDPR compliance.

So I'll leave it at that.

STEVE DelBIANCO: But, Alex, you and I were talking earlier. More than likely, the PDP won't actually do any accreditation. That's going to happen by accrediting bodies that are respected by the European regulators. So it's the access piece, not the accreditation piece, that's within the hands of Council.

ALEX DEACON: That's right. So there's work to be done on accreditation. I see what you're saying. Yeah, I agree.

STEVE DelBIANCO: But not so much by Council. Council is going to assume that accreditation provides a token. Council doesn't itself design accreditation systems, would be my contention.

Fab.

FABRICIO VAYRA: So if you don't mind, before I jump into answering this question I did want to address Stephanie's point.

So, Stephanie, I was purposeful in using the word uniform, not unified, and I didn't mean uniform to mean unified. I meant uniform when it comes to uniform application of like-situated parties. Because I think you're right, GDPR has different standards for different things. And what we're seeing and what we've heard about all day today with the data we've seen is like situated people today are submitting the exact same request and not getting uniform application of the law. And that's why I used the word uniform and I did not mean unified.

And we'll carry on this debate, I'm sure, later.

To answer the question here, Stephanie, I agree with you hundred percent that the DPAs shouldn't be bothered by this because being in a firm that represents at least the top 50 global companies in the world, they didn't go run to DPAs to ask them how to apply the GDPR. They sought legal counsel and then they applied it. They did the thing that mature businesses do.

I agree with Palage that we have to get this done because, as we've heard all day and what I just referenced earlier, we can't continue to have organizations, companies, law enforcement beat their head against the wall and get un-uniform response to the exact same legal process. And I'd agree with Cathrin that as far as implementing, we do have one of two choices. We can either elaborate on what's there today, which actually has a whole placeholder for access, or we need to come up with a new temp spec. But sitting around and pretending it's not there or not addressing it or saying we don't have the time to address it is unacceptable.

And the reason it's unacceptable is because the Article 29 in writing us, and ICANN, Goran, some of the advice you requested, praised a lot of what you had in your model but actually said that they praised you for having access in the model. And the one thing that they asked you to do was to flesh out the access model. And they actually said, "We wait for you to put that out there in a fleshed out format and in a mandatory and

enforceable manner for contracted parties and enforceable by ICANN."

I don't have the letter with me but I remember reading it to both of you and the Board a couple months ago.

So lastly, I would say I agree with -- with Alex, which is that it would be really cool if we could get this conversation started and everyone stopped positioning themselves so that we can avoid the moniker of community consensus and get to actually working together. Because I keep hearing a lot earlier about how much we all agree about accreditation, how much we all agree about access and how much we agree that this is important. And if we truly mean what we are saying then we need to actually start working together and stop sitting on four corners of the room saying, "But that's not my model."

We need a model. Let's talk about it, let's fight it out, and let's get this done.

STEVE DelBIANCO: Thank you, Fab.

Goran and J.J. will wrap up this round, and then we will move to audience and remote questions after that. So get your questions ready. If you raise your hands, one of our attendants

will bring a number and a mic over to you, but hold on because we're going to hear from Goran and J.J.

GORAN MARBY : I'm going to change the pace a little bit, because I want to -- yes, because I would like to recognize the relationship improvement we've done with the Article 29 group and the fellow DPAs. Yes, we received a lot of letters from them for many years, but yes, the relationship has improved.

And just to quote a letter from them where they start a letter to us which is published on our web page, "Working Party 29 recognizes the important functions fulfilled by the WHOIS service." That's an important statement. We asked them for a moratorium, which they didn't provide us, but they also said, "The Data Protection Authorities may, however, take into consideration the measures which have already been taken or which are underway when determining the appropriate regulatory response upon receiving such complaints."

Actually, they are complimenting us for the work we have done to put in the temp spec. And that's an important basis for this.

But I'm going to change completely just to say that this -- we are not the only ones with this. I am just receiving from a good friend, won't mention her name, that right now, North American,

UK, Asian, and regulatory press, the EU data and privacy exemptions, financial watchdogs from North America, Britain and Asia are urgently seeking a form exemption from the European Union's tough new data privacy law to avoid hampering cross-border investigations, regulatory officials told Reuters.

So it's another example where we as ICANN are in a situation where we're trying to deal with very complex issues. And here are an example with other governments, apparently, if I read this correctly, are reaching out to the European Commission and the DPAs to get an extension because they think it's too early. There is lack of guidance how to implement this.

So it makes me comfort to say that other organizations who represents many has the same problems we have.

And because what the problem is, most of the of the 2500 contracted parties are not big companies and if all of them were asking questions to the DPAs, that would actually be 2500 questions instead of one.

Thank you.

STEVE DelBIANCO: Thank you, Goran.

J.J. We'll go to audience questions now.

Number 3. Mic number 3 is first, please. Wait for the mic to be active.

Go ahead.

HADIA EL MINIAWI: Hadia El Miniawi for the record.

So Keith mentioned at the beginning of this session that the model needs to be legal, scalable, but he also mentioned that it needs to be variable. And in my opinion, the model that we issued, being variable should not be an aim in itself.

So having a model that actually provides the same level of protection to users' interests and rights across the globe should be the aim.

So I think that putting it this way, having a variable model in my opinion is not correct. If we end up in the end with variable models, that's fine, but we should keep in mind from the very beginning that what we're aiming for is a model that actually provides the same level of protection to the users' rights and interests.

Thank you.

STEVE DelBIANCO: Keith, any response to that?

KEITH DRAZEK: Sure, Steve. Thanks.

Thank you for the comment. I think -- I think there's no question that our goal is to provide protection for individuals and their rights, but we have to also do it consistent with local laws and jurisdictional requirements. So it is a balance that needs to be struck. But I completely take your point and agree that, going in, we need to recollection that that is a key concern and a key consideration.

Thank you.

STEVE DelBIANCO: Hadia, note that when Keith said "variable," variable to be more protective than Europe is with respect to an individual. Variable might be the example I gave. If Brazil's regime was more protective than the European regime, then an authenticated European law enforcement request would be turned way.

So variable could be both more and less protective.

We'll go to microphone number 2 in the middle of the room.

VOLKER GREIMANN: Thank you. Volker Greimann speaking, Key-Systems.

I've heard a lot of things about what the model is supposed to be, but one thing I didn't hear, that the model must be proportionate, as in not overdesigned for the purpose that it's actually supposed to achieve. By that I mean would you not agree that any model that we propose should not be designed in a way that it would have to be implemented at great cost and effort for a party that might only get 12 requests per month but could very well be handled by the regular abuse team in a manual fashion, and having to implement any automated systems would be disproportionate to the amount of requests that they actually receive.

STEVE DelBIANCO: We'll invite replies from all panelists on that.

Goran, would you like to start?

GORAN MARBY : Sorry, I -- my brain just melted.

STEVE DelBIANCO: Would cost be a consideration in demanding contract parties to provide mechanisms to respond to queries? Would cost and

quantity be a consideration so that proportionality could be maintained? If I got that right, Volker.

GORAN MARBY : One of the things that we are trying to figure out is the actual cost for doing this. And someone said before that no one should pay for it. There is a cost attached to it. For instance, to build something, an accreditation vehicle would cost money. Three, five, four -- five, six million dollars or something, and there would be cost to maintaining it.

But the intention is not try to build a cheap system. The intention, if we can come up with the legal guidance and the community, then, of course, will come up with the model, is that that's what that's going to reflect.

So we are more from the other end, is that we will see what is the cost and then we have to do it, but we don't put budget restrictions into what they actually can do. The legal implementation and the policy set by the community is the important one. But of course money is important because I have to take them from somewhere.

STEVE DelBIANCO: I have responses from Rod, from Alex, and then from Mike.

ROD RASMUSSEN: Thanks. One word that I've thought of after answering that first question was practical. And I think that's part what have you're getting at there, Volker. Whatever we implement, needs to be practical. And I think that -- and I tried -- I thought I had proportional in what I said earlier. I think I -- I think I got it in, but if not, I apologize.

But, yeah, any solution, you can't have a massively overwielding technical solution if you have a hundred domains in your registration. You know, it just doesn't make sense. And I think that that, too, gets towards good design. And anything -- any advice you get otherwise is not -- is probably not very good advice.

STEVE DelBIANCO: Yeah, a variable fee per query would be useless if small volume was not enough to offset big fixed costs.

So we have Alex and then Mike.

ALEX DEACON: Volker, I appreciate the question. It's a good one. If I could talk again about implementation in a policy forum, if you allow me. I think, you know, the technology available to implement this is

open. It is available in open source form. I believe there's history at ICANN where RDAP code has been written. I'm sure it's pretty dusty.

I would like to see us explore a set of libraries, a set of code that could be leveraged by the whole community that will ensure that we have this kind of uniform, global ability to respond to these -- to these requests. And, you know, hopefully the fact that the costs will be shared to develop this or somehow funded would lower the cost of implementation. It won't go to zero but it will be lowered.

STEVE DelBIANCO: Mike Palage and then Fab.

MICHAEL PALAGE: So, Volker, I agree. I acknowledge that cost should be a consideration. It in and of itself should not be dispositive.

One thing that I would ask ICANN to look at as they move forward with any model -- and this is a shout-out to Jonathan Zuck -- is let's look at metrics. They should be hard coded at the very beginning to track use, abuse and financial viability. Because as Keith said, this is going to be a dynamic system. So as it evolves, we need data points. And that I think is really critical to put in any implementation model.

STEVE DelBIANCO: Thanks, Mike.

Fab.

FABRICIO VAYRA: So, Volker, I couldn't agree with you more. And I think this is a great opportunity about that community discussion that we keep so talking about.

The model that I keep harping about in version 1.6 actually offers up a couple of things that I think Alex alluded to. One of those is a draft RDAP OpenID content profile authored by Keith Sperrione (phonetic), Scott Hollenbeck and that's been out there for sometime. So a great place to maybe start our community discussion would be if you could take a look at that and give us comment on whether that is an actual free, open source, available, implementable technology that would actually be lightweight, practical, scalable, and proportionate.

STEVE DelBIANCO: Rod had a tiny follow-up.

ROD RASMUSSEN: Quick follow-up. Fab, you got one part. Second part it needs to be practical for people making requests just as much for people providing the data.

STEVE DelBIANCO: Fair point. Microphones in order. We are going to go to microphone 1, 3 and then 2. And I believe that will be all we will have time for. 1, 3, then 2. 1, your mic is on.

MILTON MUELLER: This is Milton Mueller, again, Georgia Tech.

I want to challenge kind of an unstated assumption that the panel seems to have shared, which is that this is an extremely urgent matter and that we have to get something into place immediately, even if it means we don't think things through, even if it means we don't follow our process.

I think Keith Drazek was pointing out that it's already in the temp spec that you have to provide access. That's correct. And according to the Federal Trade Commission person from the GAC in the previous panel, it's actually already legally required to provide access.

So I think Elliot Noss was right to emphasize the need in the interim for basically market-driven mechanisms of registrars to

develop access mechanisms in the interim while we are developing a policy and then developing an implementation.

There is no way -- people, get used to this. There is no way you're going to have a unified, implemented -- you're going to have a unified policy and an implemented system in anything less than a year. Get used to that idea. If you try to do that in four months, you're going to break something. You're going to get litigation. It's not going to work. So just get used to the idea that we're talking about something that's going to happen 12 to 18 months from now, if it ever happens at all. Thank you.

STEVE DelBIANCO: Milton, the urgency was not for the access provided today under the discretion and patchwork of systems. The urgency was for uniform, reliable, mandatory access.

And I will leave the panelists to reply on the notion of urgency. I see Goran.

GORAN MARBY: I think actually Milton is making a point about the timing, honestly.

The asymmetry means that the contracted parties as it looks today has a legal responsibility for the data which are contained

in their databases. I think everybody now agrees on that. But it's a fundamental thing in that.

So what we are actually talking about is building a framework that is acceptable for the DPAs that we can have a unified access model.

And I have said this several times over the last couple of days. And I will probably say it a couple times more, is that I think we have a harder challenge to get that guidance going forward. And that will have an impact on time.

So I've -- a quick fix, I think that will be very hard to do. Regardless of the ambitions, I think that -- in the previous panel, one thing that was said which I appreciated a lot was the -- that Tucows said that there are things that we can fix on the individual access to make it easier. That is something that can be done easier. We have to work very hard together to get as much legal guidance as we can.

And there are three alternatives really which have an effect. One of them is that we get good legal guidance, and then we can jump off and do what we want to do with that.

The second is that we don't -- we have a "no." You will not -- you are not allowed to do unified access model. It's not within the law.

And the third alternative is that we don't hear anything.

And I think that during this period now, we have to figure out a way how to work together on those assumptions instead of saying that -- because how do we test that legally if we don't get -- if we don't get legal guidance going forward? I think we have to build -- the mind map of the strategies we have to build together are almost endless at this point.

So don't expect this to happen fast.

STEVE DelBIANCO: Goran, the arrow right there says legal guidance. I know you will do your best and so will the GAC and Cathrin to move that arrow way to the left so that it comes in sooner rather than later even if only guidance about a test case on law enforcement authentication, as we discussed earlier.

I have Stephanie and then J.J.

STEPHANIE PERRIN: Thanks. I just wanted to point out something that hasn't been mentioned in the discussion so far this week, and that is that the GDPR sits on a basis of a human right in the fundamental rights, the Charter of European Fundamental Rights.

Other data protection laws that I keep harping about also have a link and a nexus with their constitutional and charter rights within those states. When these cases go to court, a court is going to look at those charter rights.

So I think it's really important to think about that as we move forward with the policy development and the instrument. Note the order.

And I think that we need to consider doing a human rights impact assessment or at least a privacy impact assessment as specified in the GDPR so that we've evaluated these things. And so far we haven't done that.

And that is something we need to put on the table as part of our process. When I whine about process, that's some of the things we are leaving behind. Thank you.

STEVE DelBIANCO: Great. J.J.

JOHN JEFFREY: I just wanted to add before we go to the last question, I want to remind everyone that you should submit your comments and questions -- again, there's a lot of good content here. And we

will try to capture it and include it in our discussions of the model.

But also if you send something to gdpr@icann.org it becomes part of what we can consider and how we can include that in any formal communications that we have going forward with the DPAs, the data protection board or any of the parties involved in the discussion.

It isn't that your only access is to put a hundred comments into the DPAs. We also are trying to consolidate that and make that part of our -- of the impact of what we're saying.

STEVE DelBIANCO: Thank you.

We'll now go to microphone Number 3. There are only three minutes left.

So James Bladel.

JAMES BLADEL: I will try to be quick. James Bladel from registrar stakeholder group. Just a couple points listening to the exchange. I think Goran made an important point about challenging assumptions. A lot of comments I've heard in the last couple of hours seem to be presuming there's a bridge back to May 24th and we just

need to find it and formalize it. But that may not be the case. We may have to invent something new to meet these needs. We may have to step back to requirements capture to do that.

I think previously -- and I didn't mean to do this when I got up here, but I find myself sort of agreeing with Milton in this regard, which is that my concern is I heard of a number of comments proposing that another temporary spec might be useful in terms of expedited access. I would -- and I think Keith very rightly raised his -- you know, raised the concern.

Another temporary spec is an acknowledgment that this community has failed and this model is incapable are ill-equipped to address this problem. And I note that temporary specs are very narrowly called out for. There are other mechanisms in our contract for direct negotiation.

If we wanted it done really quickly, we could just take registries, registrars, and ICANN in a room and lock the door and we could probably knock this thing out. Nobody else would be invited unfortunately, so I don't think that's a popular option but it is an option.

And then, you know, I just finally want to say we need it quickly. There is an urgency. Let's not break the model to get there fast. Thanks.

STEVE DelBIANCO: Thank you, James.

And, Kavouss, you have the last word, provided it's brief.

KAVOUSS ARASTEH: Yeah, thank you very much. It's not last word but just giving my comments.

Yes, I think the most important issue is respecting the local law and national law of the country. We are not going to subordinate that to the law and views of a specific limited group of the countries. We have 204, 205 countries and territories. We now base ourself on something based on the European Commission and something also based on the ICANN input.

These are not representatives at all. We need, in fact, input from community. That is lacking at the time being. It's very, very important. I think we are too ambitious to do the things in four months. Impossible unless would be the same example I meant three times, vite fait, mal fait, quickly done and badly done. So if you are looking for something that you mentioned that's uniform, reliable, mandatory access, we need to carefully study the matters and have input from the entire community of the ICANN but not from a specific group of countries. They are very lucky that they have the uniform information among

themselves. But look at Asia-Pacific. 75, 80 countries, impossible to have that one. Thank you.

STEVE DelBIANCO: Understood. Remember, that everything that ICANN has put out in the framework is subject to local law when it comes to revealing a request. Keith Drazek talked about making it variable. That was his whole point, is that any registry or registrar answering an RDAP query from an authenticated source is going to have to answer subject to local law.

Let me first thank our panelists for today's session. I think you have done an outstanding job. Thank staff for the work they did. And since we don't want to stand any longer between you and cocktails and the foyer, let's have a hand for the panel.

[Applause]

[END OF TRANSCRIPTION]