MARRAKECH – GNSO - IPC Open Session
Wednesday, June 26, 2019 – 15:15 to 16:15 WET
ICANN65 | Marrakech, Morocco

UNIDENTIFIED MALE: It is Wednesday, June 26th, 2019, at ICANN65 in Marrakech. This is the GNSO IPC open session, at 15:15 in Tichka.

BRIAN WINTERFELDT: We're going to get started in about two minutes, so let folks get to their seats and get ready, and we will get started. Ria, do you want to go ahead and start the recording, please?

Great, welcome, everyone, to the IPC open meeting at ICANN65. I'm Brian Winterfeldt, president of the Intellectual Property Constituency. I hope everyone has had productive meetings so far, here in Marrakech. Similar to our closed session earlier this week, we've scheduled two subject matter experts to brief us on hot topics, focusing first on a potential unified access model as it relates to third-party access to registration data.

And second, an update by another expert on evolving multi-stakeholder process. Looking over to Heather Forrest for that update, our expert in residence.

I want to thank Mike Palage and Heather Forrest in advance for their willingness to engage with the IPC. I want to make sure that

the audience and IPC members have a chance for Q&A. We're hoping their sessions, like the ones earlier that we had in our closed session are interactive. So, with that, I'd like to introduce our first speaker, Mike Palage. Is he here?

UNIDENTIFIED FEMALE: Yeah, he's here. He's right there.

BRIAN WINTERFELDT: There he is. And he's joined by Brian Beckham from WIPO as well.

MICHAEL PALAGE: And Frank Cona.

BRIAN WINTERFELDT: And Frank Cona as well.

MICHAEL PALAGE: Hello, everyone. Being open and transparent, those of you who may have ... We've used one deck the entire week. No deck for different people. So, some of you may have seen this deck already, and if that's the case, we apologize. But I think it's important to go through the whole evolution of how we came to

this particular moment, and what we've been doing over the last six-eight months. So, with that, I'll turn it over to Brian.

BRIAN BECKHAM: Thank you, Michael. Could we have the next slide, please? I think it's fair to say that with this audience, as Mike mentioned, we have actually provided this presentation to the EPDP team and to the GAC earlier this week, and we gave a little bit more background about WIPO, and that was, I think, useful for those audiences. I think I can assume there's a little bit more familiarity here with the IPC, so I don't want to belabor this and really want to just tee it up for Mike.

Really, the message I want to convey is, as you know we've produced the report that led to the UDRP. We need registration information for due process for cases. We've been getting that through the temp spec. We obviously have an interest in how those policy conversations play out as a UDRP provider. Besides the UDRP, which a lot of you know and love, or maybe don't love, we provide other services. One of which is the Madrid system for registering trademarks.

And so, we've been approached since prior to the GDPR coming into force to see if there's maybe a narrow role that WIPO could play in these policy discussions around the unified access model.

And mainly what we think that could look like is some sort of a validation of an IP right, which would then lead to the issuance of some sort of a unique token to the IP rights holder, or their agent, which would then be turned over to a contracted party as part of the process towards the unified access model.

So, with that, I think we can actually skip the next three slides. One more. And with that, I will turn it over to Mike and Frank. Thank you.

MICHAEL PALAGE: Thank you, Brian. So, what we're going to try to do here is, unfortunately, we've not had the chance to really demo the software, so I will try to get through this presentation, and then we could take questions, or answer your questions by actually showing how the software works from an operational standpoint. To begin, this is not something ... The genesis actually has to do with the work that I've been doing with the Universal Postal Union and dot-post over the last ten years. Dot-post is a registrant verified TLD. So, the software actually started off as a basis for validating the credentials of registrants within the .post TLD.

It's important as the UPU ... One of the things that is very key in the design of this system is that it needs to be open, transparent, and be respectful of different technology frameworks. As a UN

treaty-based organization with 192 members, it is important that they are technology agnostic.

So, that is part of the key DNA of how we have built out this system. The reason why the postal operators have, I think, provide an interesting reference point for some of the work that we're doing, and some of the work that ICANN is doing right now is that they have been very active in the identity space. They have actually adopted the S68 standard on postal identity management trust.

There are right now currently several national postal operators that are actively engaged in a number of digital identity initiatives. One of the more interesting ones is one involving Correos Post, which is the Spanish national postal operator. They have actually been participating in a three-year program, a three-year pilot that has been sponsored by the European Union that looks at using the domain name system as a trust anchor for identity.

And I think that that's kind of important here. Having been involved in ICANN for 20 years, I've been through a number of rounds of new gTLDs, and I don't think that any of those rounds have necessarily lived up to the hype or expectation. So, I think it's important that we begin to look at how we can use the existing DNS for some other innovative uses. As I said, right now with the

software we actually have integrated with a number of registries at an EPP level. And those that have, or are currently operating, public RDAP servers, we've actually been pulling the data from those servers. So, with that, to the next slide.

So, one of the things that was important, an again, when first sitting down and talking with Brian and the rest of his WIPO colleagues, it became very clear early on that WIPO was interested in serving a very unique role, or a very unique and small role in this overall holistic approach.

One of the things that they identified early on was the identity of the individual. Some of the other solutions that have been proposed and had been discussed this week talk about a centralized approach, where there is a single party that is verifying the credentials. We, however, have taken a more federated approach, and we actually want to use existing private and public digital identity trust frameworks, those that will either meet the eiDAS, the European standards, or potentially the NIS standards, regarding digital identity.

So, this is something that we think is important. Another aspect that has been driving this is, while most of the discussion with ICANN over the last two years has been primarily focused on the GDPR, we have in fact looked at potential data localization as a growing potential privacy construct, and how that would scale or

implement with the work we're doing, and the potential work that ICANN is doing.

Another important thing that we've done is in actually talking with some of the members of the community, and this became clear after some of our discussions with people in Kobe, is that there are clear, distinct uses on how people access the traditional Whois or registrant data set. In connection, obviously, with the IP community, you want to find out who is behind a particular domain name, to bring a particular legal action, UDRP, whatever that may be.

And that tends to be a one-off or a small group. In talking with law enforcement, cybersecurity researchers and some of the national CERT teams, they actually need access to a larger subset of data. Not necessarily the underlying PII, but they need that larger data set.

So, one of the things that we envision, or what we propose as a structure, is to potentially synonymize registrants' identifiers, if you will. Kind of going back to the old concept of a NIC handle. But we want to use that synonymization to allow that particular element of the community to do their work without necessarily giving rise to data privacy laws, whether they be GDPR or data localization.

Another key aspect, and this is something that was obviously important for us in doing what we're doing for the UPU, as well as working with WIPO, or any UN agency, is we're looking to basically build on open standards, and proven technologies. Some of the original work, and for those of you that may remember the Philly Special, which I had authored last year and presented in Panama, there were specific references to blockchain.

Some of our discussions with people said that based upon the nascent nature of that particular technology, they didn't feel comfortable. So, that's one of the reasons we went to more proven, established technologies. Also, some of the other guiding points that we were looking at is we wanted to minimize the overall risk for the entire ecosystem. I know there's talk about how do the registrars, or registries, or contracting parties, how do they minimize their risk? What is ICANN doing? We think our approach here actually minimizes the risk for the entire ecosystem.

Two final points before moving to the next slide is that we intended this to be, if you will, economically self-sufficient. And what that means is basically user-fee generated. Now, with that statement goes to the next one about competition, innovation, and new opportunities. We believe that with this approach of

potentially synonymizing the data and making it available, there are other potential value-added services that can be recognized not only by the contracting parties in providing identity services but potentially other value-added services.

And for those, and since I have Susan sitting to my right here, one of the things that I think is interesting as far as value-added services is DENIC right now has been a big supporter of the ID4me initiative. And this has been an initiative that has been driven largely by DENIC. And what they look to do is they look to have DENIC, the registry, serve as that DNS trust anchor that I was referring to earlier, and potentially using registrars as identity service providers.

So, these are some of the innovative ideas that I think we're trying to educate the community to think outside of their traditional narrow boxes. Stop thinking defensively, do not look at this as a zero-sum game, that there are other opportunities. So, again, the two things that I would look at, and I would encourage everyone in this room to look at, regarding the use of DNS as a trust-anchor, is lightest.eu, that was the European Union pilot that I mentioned earlier, and ID4me. Next slide.

So, I'll go through this rather quickly. As part of the ... If you will, some of the requirements for success. Obviously, the verification of requestors is critical. I think all of the proposals that have been

discussed requires a code of conduct. The one thing that we have discussed here is an ex-post dispute resolution process. And I touched upon this during last year, in the Philly Special. There has been some evolution, and still some unanswered questions.

The one thing that remains is, we believe that an ADR component is, we believe, an important safeguard for data subjects that we think the EU and the European Data Protection Board would look upon favorably. What we have done is, we've tried to do some further investigation and analysis into the privacy shield. Under US law with the privacy shield, if you qualify you are required to designate basically an ADR provider to handle complaints from data subjects. Under the privacy shield, there is no monetary component, so that was one of the things that is perhaps different from what was originally cited in the Philly Special.

We're still doing research right now on how we would potentially modify the privacy shield to comply with this. We're working with some specialists in that area right now. And unfortunately, we did not meet the deadline of having a draft of those rules and policies available by Marrakech. One of the other things that is important is, for those of you that have been following the EPDP, Steve Crocker recently presented to his group what he calls ... I think his group is Barbecue or BBQ, and they have come up with a matrix.

We have a similar approach. Our approach is a due process rules engine. And this engine is designed to be configurable. Specifically, at the top of the stack would be those rules that are defined through the EPDP consensus policy. So, they would exist at the top of the stack. However, below that, there would then be able to be customization by the individual contacting party to comply with local or national laws. Under the proposed federated approach that we have, those engines would actually exist at each contracting party.

However, as the final point here notes, any activity within the entire ecosystem will not only be logged locally, but it will also be logged centrally. And we believe that that centralization logging function is important to allow ICANN to identify any actors that are not necessarily complying with the letter or the spirit of the new consensus policies as well as the representations to local and national laws.

A couple of other things that we've looked at here. Again, if there is an abuse, there will be the potential to revoke one's credentials. We're looking to actually build that into the ADR, to basically have the ADR be a process to handle multiple violations of this proposed framework. There's also ...

We believe that not all requesters are created equal. We believe there are some requesters whose volume of use will be of such a

quantum of, perhaps, the individual attorney, or even firm, that may be doing UDRPs. We're talking about maybe a couple hundred per month, versus hundreds of thousands, or millions. We believe in those higher volume users should be required to have some type of bonding requirement or financial instrument in place, and I think that's important.

One final additional component that we have been looking at is we have actually found a US-based insurance agent who is willing to undertake engagement with multiple insurance underwriters in perhaps providing an insurance policy to provide coverage for the contracting parties if in fact there was a breach. I know a lot of the people in this room have heard about contacting parties saying what are you going to do? Is ICANN going to indemnify me? We figured the best thing to look at was is there a mechanism in the private sector, in the insurance community, to provide this? If we could go to the next slide.

So, I'm going to try to go through this real quick, to let Frank actually start demoing the software. Or we could answer questions first, we're flexible either way. As I've noted before, there are going to be requestors' logs. We're going to be using federated credentials that can be used at any contracting party's UDAM gateway. One of the points of confusion that we have heard from some of our presentations earlier this week that we would

like to correct is, this is not sitting there and saying that an IP owner that may have 50 domain names will potentially have to go to 50 separate registrars. You can have a common public gateway submission, but that will then be forwarded to the respective party. That is part of how the RDAP protocol is designed to work.

So, I just wanted to point that out that that is one misconception, either on our part for not making clear enough, or just an overall misunderstanding of what we're proposing. We have the ability to submit multiple domain names. Each of the requests, as Frank will show you in the demo, will involve a digital identity with an underlying PKI element. And one of the things that we're looking here is, part of our analysis was to look at different e-contracting and digital signature laws, and we believe that that PKI element is a necessary requirement from an attestation, to make sure that the framework that we're proposing here is enforceable.

If I could go to the next slide here. Thanks. So, this is one of the examples that Frank will be showing you. And what we've done here is, this is a request that has been provided by a contracting party in connection with a credentialled cybersecurity researcher. Because this is a cybersecurity researcher, you will see that most of the data has been redacted. The key here is what they do have access to is the synonymous identifier.

So, this again is one area where we want to potentially allow the national certs, the cyber security law enforcement, to do their larger meta-data analysis, without necessarily disclosing the underlying PII. Next slide. This is an example of a credentialled individual as an IP owner. Is this bonded or unbonded?

FRANK CONA: Bonded in this example.

MICHAEL PALAGE: Okay, so in this example, this would be a bonded attorney who has submitted a request in connection with the domain illegalcontent.com. And again, for those of you that want to further explore, it's surprisingly amazing. There are a lot of domain names that we were able to register. Illegalcontent.com, .biz, .info. So, there you go. So, this is some of the Whois that would be available through the proposed system.

Next slide, please. Again, one of the things that I think is very important here is every request that is going to be submitted through this eco-system will be logged locally and centrally. That request by default, the requester is synonymously identified. We did that as a default, recognizing that there would be some instances where law enforcement may not want to be identified at all, so we have that potential. If in fact there is a data subject

that feels that their rights have been compromised, we do provide an unmasking, by which the ADR procedure would be able to be exercised by that data subject.

Next slide. So, I kind of want to loop back to this, and while this may not be of particular interest to the IP community, again, since we're using one slide deck of everybody, we really do want to hit home on why we think this approach is, if you will, fundamentally different than a lot of others. It's using the DNS, again, as a trust anchor for digital identity. I recently wrote an article that was published by CENTR in February that talked about the growing use of digital identities by ccTLD operators. Estonia, DK, NO.

Again, this is a growing trend. You look again at some of the stuff that I was talking about with ID4me. While that does not require verification of identity credentials, they are still moving in this general framework. And I am hopeful that this discussion will spur some of my colleagues in the contracting party house to open up their eyes to view this not as a threat, but as a new business opportunity.

One of the other things that I think is interesting as well is, I talk about here the potential use of a chain of title. When you begin to sit there and use these synonymous identifiers, in association with each registrant of a domain name, there now is the potential

to store this information. Under the GDPR, you're required to potentially purge this. One of the problems I've experienced over a number of years is, how do you go back and reconstruct who owned a domain name? This is a potential ... Using this to create new opportunities, new service offerings that have never existed before. If in fact the service offerings drive revenue, this actually reduces the overall cost of the system.

The final point I will make here is, what we have done here, as far as ... Again, which originally started out for a registrants-verified TLD, but which we've kind of morphed or ported over to the proposed pilot, the UDAM pilot here, is this can be used to actually solve the privacy proxy implementation conundrum.

You'll notice most of my references in today's presentation refer to contracting parties. I didn't specifically say registries and registrars. In the privacy proxy framework, there is a recognition that those providers will need to be contracted. We think the ability for them to perhaps serve a role as an identity service provider will fit in well. It would be really problematic if this group was to go through a lot of work in implementation, only to find out that once you've gone through the automated request, you get a response back saying, oh, this is registered to a privacy proxy service provider. That would be incredibly frustrating.

This is one of the reasons why we have tried to be forward-thinking in our approach. And instead of putting on a band-aid to metastasize cancer that has plagued the industry for the last 20 years, let's do what the GDPR says. Privacy by design, let's take a fundamental look at how we could get it right. Next slide?

BRIAN WINTERFELDT: Couple questions, quickly, if that's okay?

MICHAEL PALAGE: Yes, we're done.

BRIAN WINTERFELDT: Oh, alright. Do you want to wrap up and then start questions, or?

MICHAEL PALAGE: So, we could do one of ... What do we have, time-wise, left?

BRIAN WINTERFELDT: We have a few minutes left, about 15 minutes I believe.

MICHAEL PALAGE: Okay. So, I guess we won't get to the demo. If anybody wants to see the demo, we really have some cool QR codes and YubiKeys,

and we can actually show the multi-factor authentication. Okay. We'll do the demo.

BRIAN WINTERFELDT: Well, could we ask the couple questions quickly, and then use the remaining time for the demo?

MICHAEL PALAGE: Yes.

BRIAN WINTERFELDT: First question. I'm wondering what the pros and cons are. I'm sure you guys have thought very much about this, about having the decentralized rules engine as part of the model. The concern, obviously, from the IPC perspective, would be contracted parties picking and choosing, or interpreting the local rules in a way that might not be favorable for us, and I'm just wondering ... I'm sure you guys have thought a lot about that.

MICHAEL PALAGE: Yes. So, what happens is, in trying to come up with a solution that works, we figured that we were going to upset some people. And in talking with the registrars, one of the things that they talked about was reserving their ability to potentially do a manual

review. So, one of the things that is key to this system is we were originally designing it to be fully automated. After talking to registrars and actually hearing some of the potential horror stories of a fully automated system, we decided to build in the functionality to have a manual review.

Now, while pushing this out, and implementing those rules engines locally, I fully understand the people in this room's concerns about potential gaming. I share that. That is one of the reasons why the logging is done centrally. So, right now, if you have ICANN Compliance being able to look at the entire ecosystem, not only of when requests are submitted, but when in fact the request has been honored. So, it's not just going to sit there and say, oh, the request was submitted on this date, that's it. The log file will say it was submitted to the registrar on date X, and it was completed on day Y.

So, there will be the ability to have analytical tools to identify potential bad actors. We thought that this was a risk, and if you look at some of the problems with DAAR, that's been a concern within the contracting parties. Here, we're actually going to have ... The registrars will have a log of what's coming into their system.

So, they will be able to know, hey, I'm probably potentially a little deficient. And we think that after some time, our belief if that

once registrars see that if this framework is approved by the European Data Protection Board, or individual DPAs, something we are looking at doing right now, there is that potential to allow some registrars to switch on the fully automated mode, because they're probably going to get tired of going through and doing that. So, that is the balance we tried to strike.

BRIAN WINTERFELDT: Okay, thank you. I guess one thing, kind of thinking about it, is it sounds like there is a lot of manual review involved, potentially, in that process. No?

MICHAEL PALAGE: Not by ... So, the manual review would rest solely with the contracting parties, the registrar, the registry. And in talking with them ... And this is something that I've done, and I'm trying to come out ... What is the number? And talking to what I would say, some of the more responsible registrars, they have generally said they're looking at a 24-72-hour turnaround.

One of the things that Frank could point to is, in the way we have designed the system is we have an end-point to end-point transfer of the data. So, when in fact a registrar or registry would complete the request, once it's been requested it would automatically appear. So, you wouldn't have to go back and

check. You would just log into your gateway during that period of time and look at it. One of the things that ...

FRANK CONA: I was going to say, I can actually explain some of that in the demo, so it might be easier to show it?

MICHAEL PALAGE: Okay.

FRANK CONA: Okay.

BRIAN WINTERFELDT: And one other quick question ... Or were you not finished? Okay. Alex had a question, and then Paul.

ALEX DEACON: Hi Michael. Earlier on, or maybe midway through your presentation, you mentioned you thought there would be a need for a PKI to be used in order to meet ... I forget exactly how you worded it. Was that for the identity of the individual, or for something else?

FRANK CONA: Yes, so Mike's reference to PKI was that we could incorporate the ability to digitally sign, whether it's an attestation or some document that needs to be uploaded.

ALEX DEACON: Okay.

FRANK CONA: All different technologies can be incorporated, and that's obviously one of them.

ALEX DEACON: So, you aren't saying that you think some type of PKI credential would be required to access or submit requests into the system? I think that would be a bad idea, by the way.

FRANK CONA: No, no. And to that point, I think one of the things to emphasize, and I think Mike touched on this, is the way we built this platform intentionally is highly adaptable. There are a lot of policy decisions that still need to be made, and that's obviously ... The access requirements is one of them, and a big part of our philosophy is number one, that this is actually bigger than one organization, one group, etc.

Two, that it's highly dependent on a lot of decisions that still need to be made. But we felt it was important to actually develop a platform where we can actually test some of this stuff, see how it plays out, gather data through an operational system, and also that it's highly adaptable. So, if there's a decision not to require actual signed attestations, that's fine. And on the concept of manual versus automated processing, there's a big spectrum there.

And there may be a set of fairly common situations where there may be automated processing, yet a larger set for manual review, [or I should've said an] edge-set for manual review, and where that falls. The approach here, which isn't dependent on any particular technology, is highly adaptable so that it can accommodate both.

Even where the processing takes place. Obviously, we've talked about decentralizing. That's more from a role standpoint, but the actual processing from a rule standpoint could be centralized, could be decentralized, could be both. You can actually, in theory, have one of these access gateways at any contracted party, or at a central location. And the requests actually get routed, but the data does get sent back directly, so you're not circulating data, obviously, around. So, if I can share my screen.

BRIAN WINTERFELDT: Great. Next, in the queue, we have Paul.

PAUL MCGRADY: Thanks. Two questions. One, is this system agnostic to whether or not we end up with a distributed system, or whether or not all this, ultimately ICANN, is deemed the controller, and it's centralized? In other words, does Strawberry matter in relationship to this? And secondly, in terms of the process for accreditation of attorneys, are you guys anticipating any audit or other requirements?

Because we of course have confidentiality obligations that ... We're not like other businesses, we just can't open our books to everybody. Is that something that you guys are baking in now for people who are already essentially certified to be doing what they're doing by the states or nations in which they reside? Thank you.

FRANK CONA: Let me take the second one, you can take the first one. As far as what are the qualifications for an IP attorney ... Okay.

PAUL MCGRADY: To be more specific, what would be the audit requirements for an IP attorney? So, this is some sort of quasi-contracted party status,

right? And right now, contracted parties have audits, and they have to open up their books to ICANN. That's not something that attorneys in most jurisdictions can do.

FRANK CONA: So, as we mentioned, all queries are synonymized by default. So, those are synonymized and would only be unmasked if there was a particular need. Now, I guess the question I would ask is, is the law firm ... This would be a law firm as a requester seeking access to data, as opposed to a law firm that's acting as a registrar. I just want to be clear.

PAUL MCGRADY: Correct. Just with the legal hat on and say that there's a run that week and there needs to be 100 queries instead of the average 19, and somebody gets unhappy about that, and wants to have ICANN look into whether or not those particular credentials are being abused, or whatever. There's only a limited amount ... We can't say, oh no, we needed all 120, here are the 120 things we're working on, right?

And so, it's different than if I were a regular business who had some reason to be asking these questions. And I think the same question holds for law enforcement, too. They also can't undress

and tell you everything they're working on just because the query number spikes, or something like that.

FRANK CONA: So, back to your question about law enforcement. Obviously, in some cases, they are legally required by law. For some contracting parties around the table, you cannot disclose that. So, that, again, is built in. From an audit standpoint in using this system, I don't think a couple of hundred queries is probably going to trigger an audit, I think you're probably going to ...

PAUL MCGRADY: Yes, I maybe be ... By trying to give you an example, I think I've done the ICANN blunder of giving you an example so that the example can be addressed instead of the concern, so I apologize for that. My question has to do with what kind of audit or investigation powers will result from a law firm signing up to participate in this? Thank you.

FRANK CONA: Yes, and I want to address your original question too about agnostic. And the short answer to that [is] it is agnostic. As I tried to convey earlier, the basis of the architecture here, and the platform is, one, it's open technology, it's not specific, I think I

touched on that. But in terms of the policy requirements, like the auditing and stuff, like you mentioned. Those are policy decisions that are yet to be finalized.

We certainly have proposals and, like Mike mentioned, a code of conduct, obviously, rules of use and other things that we would put forward. But those are ultimately policy decisions. And so, what the requirements are for the accreditation process for the submission of request is going to be a policy decision that has to get decided. Our approach allows for any adaptation that comes out of that.

PAUL MCGRADY: Thank you, so I guess just to highlight to whoever else is listening in the room that may be involved in these policy decisions, this system could be of great help and assistance to protecting consumers from confusion and/or abuse, but if the audit and other restrictions are too heavy for lawyers to participate in, all this work could result in zero effectiveness for that. Thanks.

FRANK CONA: Sure. And that's exactly what the policy decisions need to balance. And that was one of the things we wanted to key on when we outlined the approach, that it wasn't just about privacy and GDPR specifically, it's actually about accommodating a

whole series of legitimate interests, right? That's everything from IP and investigations of illegal illicit activity to cybersecurity research, to everything else. And I think, to your point, the policies that get put into place need to balance that. That was I think that Mike touched on this, too.

We anticipate, and we can adapt to a light-touch consensus policy that may focus on certain types of activity but allow for a certain level of adaptation for things that are outside of that. For example, there was a lot of discussion I'd heard this morning around legal and natural person, as well as sensitive persons, which could be either natural or legal. And of course, legal persons ... And that data being outside of GDPR, as an example, altogether.

And so, part of our holistic approach is also moving toward verification of registrants, or at least data from registrants so that that distinction can be made. So, there could be a whole set of processing, that, for example, could be automated, because it falls outside of GDPR. And so, a lot of policy decisions that have to get made ... The reason why we built the system and we built it to be adaptable is we can start testing that stuff now to get data to help inform those decisions.

PAUL MCGRADY: And I apologize. The other thing to think about is for situations where it's not abuse. So, for example, if we have a client that's buying something, and we need to do due diligence on the domain name portfolio, how do we deal with those consent issues? And you guys may have already addressed that, so, thank you.

MICHAEL PALAGE: We actually have a ... Can we do the special use?

FRANK CONA: If you want, I can submit the special use [show].

BRIAN WINTERFELDT: You guys, actually we're over time. We only have 15 minutes left for Heather's portion of the presentation today. It seems like we have sufficient interest, though. There's more questions and more people in the queue, and we haven't gotten to the demo. I would propose that we could set up a separate call after the meeting to do the demo and have a further Q&A. Does that sound like a good way to move forward for everyone?

So, we still have time to hear from Heather?

UNIDENTIFIED MALE: [Sure. Thank you.]

BRIAN WINTERFELDT: So we can see this is the beginning of the conversation. Thank you so much for your time today, we really appreciate it and look forward to having a more in-depth discussion after the meeting here. Thank you. Great, so I would love to turn the microphone over to Heather Forrest, who has graciously agreed to talk to us about the evolving multi-stakeholder model today.

HEATHER FORREST: Thanks, Brian, very much. And hi to everyone. So, I'm not convinced, I've just said to the guys sitting here with me, I'm not convinced maybe that this is the most important thing, but I do think it's a great idea that we follow up with these guys separately and spend lots of time with them. So, on balance, you get 15 minutes with me, and much more time with them, which I think works out brilliantly for everyone.

So, I've asked Jen and Brian to simply run with our comment on the evolving multi-stakeholder model, so that's why we're looking at this, as opposed to a set of canned slides. The thing that I would like to direct our attention to today, with the time that we have, is not so much to rehash the comments.

Brian's very kind in saying I'm an expert here, and I'm not. What I am is the champion of this business of the need for reform in the GNSO. And in the broader organization as well. I'm delighted to see that we're taking this on at a more macro level. Of course, I did sacrifice myself on the altar of PDP 3.0, kicked that project off. I know Jeff Neuman despises the fact that it's called PDP 3.0, and I disagree, which is rare.

I think this is an opportunity not just to tinker around the edges, but to do some real change. And I would really hate to see ... It's the only frustration that I have. I think the council's going brilliantly, and everything's carried on very well. But I would hate to see that this one just dies as an initiative that got off to great fanfare, and then nothing happened to it. This is an opportunity to do some pretty significant stuff, and what I would like to encourage the IPC to do is not let this die in a ditch.

I was interested in the, to some degree, fruitlessness, of the session yesterday afternoon with Brian Cute. I noted with interest that I walked out the door with a few former board members who said that that session was evidence of the dysfunctional way in which we go about doing things. And I said you'll know how far up the ICANN food chain you are if you get to cast yourself in ICANN, The Movie.

So, look. What you see in front of you is the IPC comment on evolving the multi-stakeholder model. You may remember that this is a process that was kicked off, very wisely, in my view, by Cherine Chalaby, the ICANN Board Chair, at ICANN63 in Barcelona. He took the mic on Monday morning, and said mea culpa, mea culpa, mea maxima culpa, and said it on behalf of all of us. We all need to change. The first step in any program is to admit that we have a problem. Cherine did that collectively for us, and I think he did so quite eloquently.

That has started a broader period of reflection in the organization, which coincided with PDP 3.0 and the GNSO, which was awesome, in terms of timing. We were then asked, as a follow-up to Cherine's opening remarks in Barcelona, to reflect on the list of challenges or problems that had been noted by the community. And I believe there were 18 or 19. It was a fairly high number.

But we were not given free rein in our comment, we were asked to identify particular evidence of these problems in our orbit. And so, Brian Scarpelli came to me, asked me if I would help with a first draft of his comment. I relied fairly heavily on the IPC comments to PDP 3.0, so you'll see there's a great consistency here with the comments in front of you, and those previous

comments, which you'll find on the page that Jen brought this one up from.

And what I thought we could usefully do here ... Let's just have a very quick look at this document. If we scroll down, we'll just highlight the three. And of course, this document's public, we're not airing any family laundry here. Just to highlight the three examples that we focused on. First obvious one, phase one of the EPDP. And you'll see here some of the very many issues in that list in relation to the EPDP. We raised issues of timing, culture, representativeness, consensus.

We can scroll down to the next page. Thank you. And volunteer burnout. Issue number two is the RPM PDP. I think the comments that were made by Paul in the council meeting in this room, immediately prior to this meeting, were super sensible around timing.

So, you'll see that's issue number one. And of course, I'm slipping in timeline, and so on. Culture, we're all very familiar with challenges there. We can scroll to the next page. Recruitment representativeness, again, and inclusiveness. And I think we have one ... Yes, a few more. Good. Consensus precision in scoping the work, and I'd like to come back to that precision in scoping the work, but we'll carry on for now. Accountability, transparency,

costs and volunteer burnout. And I believe that get us to the end of our comment ...

Oh, no, that's true, we have one more. IGO-INGO curative rights PDP, and I was asked to come into discussions this week with the GAC to try and resolve how we move forward on this. Again, repetitiveness, but each of these, of course, a very good example of these problems. Culture, representativeness, inclusivity, precision in scoping, trust and volunteer burnout.

For those who attended the session yesterday, the focus was on prioritization and on scoping. And I thought this would be an interesting question for the IPC. I know it's an open meeting, but it's good for the community to hear. What are our priorities for the year ahead? It's great that Org says, you know, "Over to you, community. We'll be led by you, what are your priorities?" But my thinking here is, what are our priorities?

And I can give you, just by way of context, the way that we kicked this off in PDP 3.0 in the GNSO was to start 2018 by listing everything that was on our agenda and then saying which was the most important. And let's devote our time, energy, and resources to those things. What do we want done? We want an IGO-INGO curative rights done. We wanted Red Cross done. We wanted SubPro to be at a particular phase in its work. We wanted the RPM

PDP to be at a particular phase in its work, and we pushed hard on the Chairs of those respective efforts to try and get that done.

We had a few implementation teams that were in play and tried to do that. So, I would encourage the IPC ... This is just kicking off the discussion now, but I'd like to turn it over to leadership, really. What are our priorities in the years ahead? So, Brian, I'm happy for you to facilitate that conversation if you want. I'm happy to, but if anyone has any thoughts, that's great?

BRIAN WINTERFELDT: Anyone like to reply to Heather's request for our priorities? Lori?

LORI SCHULMAN: Hi, Heather. Thank you so much for your work in this area. You and I had many discussions about this, and in full candor, I had very mixed feelings about yesterday's session. I mean, on one hand, I understand that priority-setting and very short-term thinking is super important to the over-work issue. So that, I thought, was super helpful. To have that conversation about, we have a limited bandwidth, and we've met or exceeded it at this point. And I think most people agree to that point.

What I found sort of disheartening, particularly after the conversation we had in Kobe, is there's fundamental structural

problems that create this problem. It's not simply a question of priority setting, it goes much deeper. And I think as the community evolves and develops, we're seeing now ... And I am going to speak from an IP perspective here, that we're finding many of our members wear different hats in different parts of the association.

And I think part of the gridlock issue, and the slowness, the inefficiencies, come from this continuing need for silos, which I would argue we don't need anymore. Brands have become registries or registrars. We know inside the IPC itself, we have so many members who may not vote in other constituencies, where they have interests in other constituencies.

I think part of the issues with EPDP, it forced this ... Continuing the two houses and the constituency model has a tendency, I think, to force people into particular positions, which, I'm sorry, like, I'll just, yes ... [inaudible] I feel like it's forcing people into corners, rather than bringing people into the middle. I think that's a fundamental issue, and I was disappointed that it was not addressed, particularly after Kobe.

HEATHER FORREST: So, Lori, this is Heather. What I interpret from that is maybe structural reform should be our priority. I'm thinking much bigger

here, right? I think the problem with some of the criticisms of PDP 3.0 is folks aren't tapping into the bigger mission behind that, right? And likewise, my question about priorities, let's think big here.

LORI SCHULMAN: Heather, this is Lori, responding to this point. I apologize if I'm out of the queue, but I do want to continue the dialogue if you don't mind. Exactly. I think the IPC, given the strength that we have, and the influence that we have in the global economy, versus the voting structure, is completely out of balance.

BRIAN WINTERFELDT: Thank you, Lori, for your input. Anyone else have feedback to share with Heather? Anne?

ANNE AIKMAN-SCALESE: Hi, it relates to Lori's comment in this discussion. Yesterday in the session, I sort of felt that we're looking at it only from how the model works right now. I felt that most of the issues that were raised by commenters, a lot of good comments, went back to what's called issue number 11. It says roles and responsibilities.

And to me, unless the community addresses that first, as a priority issue, they won't be able to resolve the other ones, because

they're all interrelated, and they all come back to roles and responsibilities, and that would also be a matter of structure, and whether you need to change your structure, because that's what roles and responsibilities are.

The second comment regarding that session is, the other assumption underlying it was if everybody's responsible for it, then nobody's responsible for it. And I don't think I actually agree with that principle in the ICANN model, in the sense that we have …

I'll draw an analogy to corporate situations. You have people in charge of daily activities, you have people in charge of departments, you have people in charge of several divisions, and then you have an exec, and a board of directors. They all have responsibilities, and in the ICANN community, we all have responsibilities. Even in the PDP manual, which I think is fairly sound, even individual members have responsibilities. So, I think there are a couple of the underlying assumptions that aren't truly applicable.

BRIAN WINTERFELDT: Great, thank you, Anne. Fab?

FABRICIO VAYRA: Thanks. I just want to make sure ... Heather, the question was about the IPC's priorities, right? Not the community's parties? So, I would proffer that, as the IPC, the Intellectual Property Constituency, we focus in the short term on what we can about, which is intellectual property protection. And I think it's very obvious, it should be, at least, to everyone in this room, that the number one thing afflicting us from our ability to protect IP and the DNS is our inability to get access to Whois.

So, I would say that what we, as the IPC, should be focusing on is solving access to Whois. We were supposed to get a demo, but we got a description, we've got something else floating around. Let's focus on those models, and let's make sure that people like the GAC are talking about the existence of code, and models that actually exist. Because the community is actually telling us that can't happen, right? We're being told we're decades out. We're watching people tell us it's weeks or months out.

So, we should be pushing that sort of thing, and showing that access to Whois is actually here, we can do it. Because otherwise ... We can talk about intellectual property, but within the DNS, we can't enforce our rights, our clients' rights, or anybody else's rights, if we don't know who we're enforcing against. So that's, I think, the number one thing we should all be focusing on. And to get at that, we need to make sure we push on these models that

the community is telling us aren't available and can't actually happen.

BRIAN WINTERFELDT: Thank you, Fab. Excellent contribution. Susan? And then we're going to have to close out the queue because we're out of time.

SUSAN PAYNE: Yes, I think that's a really good point from you, Fab, and it is really important for us to remember what we're actually all here for. But in the context of this evolving the model thing, one of the things that strikes me when you're talking about that is the consensus, what is consensus, how we get to it, seems to me to be pretty crucial in trying to achieve that aim. Both in the EPDP, and we'll face it in the RPMs Working Group as well. So, fixing some of the underlying ills, I think have an … Or the lack of a fix on the underlying ills has an impact on whether we can deliver any of those objectives.

BRIAN WINTERFELDT: Thank you, Susan. Unfortunately, we are out of time for today's closed meeting. But that was a great discussion. I want to think Heather, again, for leading that for us. And I do think that this should be another topic that we continue to talk about. I think it's

very important. And I think especially as we think about setting our priorities and thinking about how the IPC is going to feed into the work and thinking about how to evolve the multi-stakeholder model.

I want to thank everyone for participating in the session today. A quick reminder to please join us Thursday afternoon for the hot topic session, titled Impacts of EPDP Phase 1 Recommendations on other ICANN Policies and Procedures. This will be a good opportunity for the IPC to raise concerns regarding the issues related to the identified 14 unique policies that will be impacted by GDPR. In addition, this should be an appropriate time for us, once again, to raise questions that came out of the CSG meeting this morning, as they relate to the privacy and proxy implementation, as well as the Strawberry team objectives and timeline.

So, hope to see all of you there. Please feel free to let me know if there are any topics or things that we didn't get to today. We can be sure to include them in our next IPC meeting, which will be coming up in July in a few weeks. And if there's anything that needs to be addressed before then, let us know.

We'll be sure to reach out to our first speakers today to set up a follow-up, so we can actually get the demo and continue the Q&A that was very robust already, and that will continue. I know a lot

of people had questions that we didn't even get to today. Again, thank you, everyone, for your time, and look forward to seeing you in the rest of the Marrakech meeting. Thank you.

[END OF TRANSCRIPTION]