SAN JUAN – Joint Meeting: CPH & CSG
Wednesday, March 14, 2018 – 15:15 to 16:45 AST
ICANN61 | San Juan, Puerto Rico

PAUL DIAZ: Is this one being recorded as well?

UNIDENTIFIED MALE: Yes. She checked.

PAUL DIAZ: Okay. Zoe or Sue, thumbs up. Are we recording? This is off.

UNIDENTIFIED MALE: Oh, there is no Adobe Connect.

PAUL DIAZ: Then let's get right into it. All right. Welcome, everyone. I'm Paul Diaz, Chair of the Registry Stakeholder Group. Welcome to this meeting, my meeting of the Contracted Parties House and the Commercial Stakeholder Group. We sort of had an agreement we're alternating who chairs. So, you guys did it in Abu Dhabi, Graeme and I will take the lead today.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

There were two agenda topics as I recall. The first one was a quest from CSG for us to go over how we determine who to put on the board, for us, Board Seat 13, the one Becky currently holds. Kind of chagrin to say that prior to the last round, historically, it was basically done by consensus a number over a handshake.

The agreements that we have is that we would alternate. Bruce served for the maximum nine years. So, when he was term limited, it became registries' turn to identify candidate. And once we did that, we would inform the registrars who would effectively have veto power if it was somebody they really couldn't put their support behind. That's never happened. We all know another, work well together.

But the interesting development for the registries is that we had an abundance of riches. We had a number of folks who said that they wanted to serve and were all well qualified in many different ways. So the registries actually had to have a special election with a run-off to determine the candidate who ultimately was Becky Burr.

And we started, and I have to admit, I don't think we fully codified that process, in particular, what the run-off looked like and the criteria for it. We were making it up as we went and with the view that Becky could serve in the role potentially for as much as nine years. There wasn't a sense of urgency so perhaps before we forget everything that we learned, we should have that written down.

But ultimately, the candidate was identified, was shared with the registrars, certainly supportive of Becky as well and then we just tell the council, "Here's our candidate" and that individual seated. Moving forward, of course, will be the due diligence is done. This is new uniform process that they're working on.

All right. So, that's it in a nutshell. Questions? Steve.

STEVE DELBIANCO: Thank you, Paul. We were referring in the Non-Contract Party House to the annex to the GNSO procedures, that's Annex VI, where it was written down. And so, first thing I heard is that maybe what you did successfully may not be reflected in Annex VI of the GNSO procedures. So if it's possible to reexamine – at some point, you don't have to do it now – if there were anything you would change about it, that would help us because we're basing what we're doing with the rest of NCPH on what's in Annex VI.

And without changing the procedure, if you guys were to share with us any observations and lessons learned that if you were doing it over again, we would have changed this part when there's multiple candidates for instance.

And I'm looking at it now, it's really just a page and a half on page 90 and 91 of Annex VI of GNSO Council Procedures just updated in January. When each of your registry and registrar groups are asked, "Hey do you have a favorite candidate?" that's true out there, you just leave it to the registrars to figure out how they would answer that question and you leave it to Paul as to figure out how he would answer theirs.

So it strikes me that in that process, I don't see that there's any role for the NomCom appointee to the Contract Party House. Do I have that right?

PAUL DIAZ: That was the experience last time around, the last part about NomCom appointee. And as I remember, this particular annex, there was an update but I don't think that was substantively changed from what was there previously. You noted the January date, the rules were there. But there's not an awful lot of guidance, as I remember, when we were going through our process in terms of what was expected of, in our case, the Registry Stakeholder in identifying the candidate. There's a lot of wiggle room in terms of figure out who your candidate is.

STEVE DELBIANCO: And so, the role of the Houses is there and the chair of each of those Registry and Registrar Stakeholder groups are communicating the decision however derived below.

That bypasses the running it through the councilors until you've made a decision and then council ratifies it. So the way that yours is described, and it's one of the reasons we found it so attractive, is that we have the Commercial Stakeholder's Group and Non-Commercial and we would each, in our own way, come up with those decisions and use this back and forth.

But the process you've described doesn't involve your councilors at all. It doesn't involve the Nominating Committee appointee at all. It's done with the two stakeholder groups through the process described. And if that still reflects the experience you just had, we're going to try to head in that direction.

PAUL DIAZ: Yes. I think – and correct me if I'm wrong – anybody, but that does reflect, of course, our councilors in their capacities as representatives of the registry operators participated in the elections and the run-off for the ultimate candidate. But there was not any formal voting by the councilors, that is, and nothing from the NomCom, no.

Okay. I think I got it right. It sounded right from what folks remember?

UNIDENTIFIED MALE: Yes.

PAUL DIAZ: And recognizing again the nature of registries, registrars, a lot of seeing things eye to eye, a very different dynamic. I think you have the commercial versus non-commercial. So, I understand the focus on protocol process. Ours has always been a lot more consensual. Jonathan.

JONATHAN ROBINSON: Paul, I don't disagree with anything you said but you're right, historically, there was just this sort of repeat election of Bruce for many years but I think we were pretty systematic about the way we did it. And although it had to be derived from first principles for that process, it struck me that it was a systematic, thorough process that went through a series of voting rounds. So I think it would do us a disservice if we're represented as being too informal. I mean I think it was quite thorough, quite rigorous, subject to two rounds of voting. We made a cut, we then put two further candidates forward, had them in a run-off against each other, used both Houses. I think we could share with you. I'm pretty sure it was documented at the time. But maybe that's not the –

STEVE DELBIANCO: No, maybe we aren't here for that part of the discussion. It's on page 90. It's Annex VI of the GNSO Operating Procedures for Board Seat 13. We're seeking to emulate that document and we're asking for any clarifications you want to add, so it is a process that's documented in GNSO procedures.

PAUL DIAZ: All right. Tony.

TONY HOLMES: Thank you. Tony Holmes, Vice Chair of the ISPs. And for this meeting, the ISPs are leading the CSG sessions. So just to put it in context, the reason that we're asking this is that we have struggled and certainly we do need to nail this down within the CSG, make sure it's better understood from both parts of our House and we can move forward on that basis.

Now, tomorrow, there's a meeting of the CSG Exec and the Non-Commercial leads for this area where we're trying to hone down some of the outstanding points. So that's the reason we raised it here, was to try and seek some better clarity, and if there's anything particular that works for you to then see if that would work in a better way for us.

So, we'll take it forward. We may need to come back on this with some clarifying questions after. But I think for now, unless anyone has got any particular questions to raise related to this, we could probably move forward and thanks for helping.

PAUL DIAZ: Thank you, Tony. All right. There's nothing else in the big issue, something you guys heard, GDPR and implementation. Understand that the document, Claudia, that you circulated last night, we pushed it out. But it was late in the day, it's been very full days and I understand that you guys have also been working since then. So, I might suggest, for those who have not absorbed it or are not up to date, we spend a few minutes touching on the key points. And please, underline or underscore any changes that you've made so that folks are looking at it while you're speaking or whoever wants to introduce that. I'm just looking at Claudia. Please highlight some evolved thinking wherever you stand. But that way, we're kind of level set so we can continue from there.

STEVE DELBIANCO: I was going to mention that as we walk, and I think, if it's possible to walk through the document in the case people haven't seen it, it isn't very long, it would be a discussion guide from the registries and registrars with the experience you have, the visions you have for RDAP and other implementation concerns.

We would, best of all worlds, we get concrete input about things we've missed, ideas of a much easier, simpler way to do it, considerations for implementation challenges, testing, rollout, linguistic character sets. I mean as much as we can learn working together, at least the Commercial Stakeholders Group, we feel like that would be a very useful way to apply our time together. If at some point, you folks feel that we're too deep in the weeds, it's too technical, take it up a level. But we need to move so quickly that the idea is to get specific information if we can. Thank you.

PAUL DIAZ: Understood. So, Rubens, go ahead.

RUBENS KUHL: One of the things that I noticed was missing in that document was some kind of feedback loop in order to ease people to find abusers because there is one mentioned that, oh, if you are found [abused your] software or something. But there is nothing that would allow people to find the abusers and that would probably go with some sort of logging mechanism like could be a [inaudible] ledger, could be something like you're choosing certificate transparency by the certificate authorities that would allow people to see, oh, that user X have consulted WHOIS data for a million domains. That person should probably doing that and then you can go after the abuse.

So, even having penalties, you need to have something that makes you find those that are committing that abuse. And that's one thing that I found missing.

STEVE DELBIANCO: Rubens, let's get to that when we get to that part of the document as opposed to jumping to that point right away. So, if I could ask staff to load the document, we simply threw it up for purposes of ease. It's a bizconst.org/accreditation. That's bizconst.org/accreditation. I'm not sure who's managing it because we don't have Adobe up. Who is?

UNIDENTIFIED FEMALE: Hold on, Steve, I'll check it out.

STEVE DELBIANCO: Not even in the room, right? For those of you who want to bring it up, it'll be easier for you to bring it up yourselves rather than something else, bizconst.org/accreditation.

And then, with that, I think we have so many people around the table who contributed to the drafting. And I was looking at Fred maybe to start it off on this technical rhetoric free and examination. Please.

FRED FELMAN: So, just to make sure that I understand, you'd like me to review what the content it is as a starting point or would you like me to actually start with this section?

STEVE DELBIANCO: Let's start from the top and try to solicit specific input as we go including Rubens's point when we get there. Thanks, Fred.

FRED FELMAN: Yes, all right. So just sort of thinking about this at the beginning, we started with the eligible entities and eligibility requirements. And this is intended to be just a listing of the non-law enforcement agency list of folks who might access this. And we might actually consider, at some point, adding the law enforcement agencies but I thought that was more the purview of the GAC.

The first group that we considered were cybersecurity and OpSec investigators, and these entities would be the individuals and companies and academic institutions who provide cybersecurity and operational security for themselves for a corporation or provide as a solution or service to other individuals or entities. And with that, we were considering security intelligence in analytics companies, identity access and management companies, application security companies, fraud protection, people who provide or organizations that provide digital forensics and incident response, also e-mail and data security companies and also companies that provide specific protection from spearfishing, malware, botnets, and DDoS attacks.

So, I'll pause for a second to see if there are any questions about the list of folks that we would consider.

[ZOE BONYTHON]: One thing to say, this was pointed out by someone because there are people attending remotely that they're on audio only. So just in consideration of that, could you make sure if you're referencing anything to say, "Page number X", make more clearer references, Paragraph 3, etc., so that it's clear to them, please.

FRED FELMAN: Yes and currently, I'm in Section 1 which is labeled Cybersecurity and OpSec Investigators underneath the header Eligible Entities and Eligibility Requirements.

So, if there's no input on that, let's start to then think about this. By the way, we used, as a starting point, the EWG report to start to think about this.

JONATHAN ROBINSON: Fred, quick question. And maybe this comes later. They might be addressing it later. What is your assumption about what data is being accessed? When we talk about this because you talk about nonpublic WHOIS or WHOIS data but presumably, we're talking about emulating the current public interface to WHOIS.

FRED FELMAN: Yes, that's correct. We're talking about emulating the current interface to WHOIS. And in terms of getting to specific types of data and specific purposes, we have a supplement document that I think was just published a few minutes ago which some folks have been working on that actually looks at each one of the use cases and the eligible entity and goes into great detail in terms of their purpose.

JONATHAN ROBINSON: So, that would be in terms of what fields of those data might be available to them.

FRED FELMAN: In that document, I don't think we go through fields, we just go through specific types of their behavior.

JONATHAN ROBINSON: Okay, but back to my original question, you are not talking about access to some sort of bulk data here. This simply this is a mechanism by which various entities might get access to an interface that looks like the current interface.

FRED FELMAN: Yes, it looks like the current web interface, also it looks like the current Port 43 access mechanism for automated access as opposed to bulk.

STEVE DELBIANCO: Jonathan, it's key to understand that distinction that the word "bulk" only applies in the way registrars and registries deliver data to ICANN and the data escrow providers. There is none of that anticipated. It's a single record, specific query, the full domain name just like Port 43 works today unless you tell us that "don't do it that way, do an RDAP [inaudible] query so that the credential can accompany the request. We'll get to that when Fred walks through that part of it. But if you want to know what data, I would refer to the cookbook where the entire annex describes the data fields.

JONATHAN ROBINSON: I specifically wasn't referring to data fields, more the emulation of current interfaces which is Web in Port 43.

PAUL DIAZ: Okay, I've got a bit of a queue going. James.

JAMES BLADEL: Hi, Thanks. James from GoDaddy, and quick question. That was Section 1, the Cybersecurity Investigators. And then did you say there was a section for law enforcement as well, law enforcement?

FRED FELMAN: Actually, we took out the section for law enforcement and left that to the GAC to consider.

JAMES BLADEL: Okay. Because I'm just curious because I've been having a number of hallway conversations and there's a number of plans and proposals for law enforcement and cybersecurity kind of floating around Puerto Rico. And I'm wondering, was this developed in conjunction with… So you kicked that out over to the GAC or is it in conjunction with like SSAC or some of those folks on Section 1 or is this just coming specifically from IPC, BC, ISPCP?

FRED FELMAN: It came specifically from folks in the IPC and BC but we also consulted some members of SSAC.

JAMES BLADEL: All right. Thanks.

PAUL DIAZ: Thank you. Thomas, I think I had you next. Susan, you want to jump in?

SUSAN KAWAGUCHI: Just a point of clarification, this was not a BC or an IPC approved document. This is members of the IPC and BC and we consulted others.

JAMES BLADEL: Are there more?

SUSAN KAWAGUCHI: So, there's a list of companies that signed on to this.

JAMES BLADEL: Okay. And I'm just trying to get my arms around all the ideas that are floating around because there's some good ones and maybe we can Frankenstein something up here. But are there more coming from the folks maybe who didn't want to sign on to this, maybe working on their own proposals? I don't know.

SUSAN KAWAGUCHI: Stephanie said she had one this morning.

JAMES BLADEL: Okay. Well, we'll watch for that then. Thanks.

PAUL DIAZ: Thomas.

THOMAS RICKERT: Thanks very much, Paul. I think there are a lot of good ideas in this paper and thanks to everyone who's been co-authoring this. I think that's a few [chap]. What I'm missing in this document is still to come up with the two big pillars that you need in order to make processing lawful.

And I think that it was the European Commission even that have pointed this out in their recent letter. They said that you always need a purpose plus a legal ground for processing. And only if those two are present, then you are good to go.

This document says an awful lot about the purposes for which data is used and these purposes can then potentially be legitimate interest of third parties. I think there will not be a legitimate interest of the registries and registrars and that is possible too under 61F GDPR. For those who want to look it up, you can have third party legitimate interest.

I could just take a quick look at the document but I think that more work needs to be spent on how this legitimate third party interest outweighs the rights of the data subjects. Right? And that needs more explanation because the way I read this document – but again I may have gotten this wrong – everyone who is accredited get access to all the information that is not publicized, might be individual queries but still everyone gets access to everything.

And I'm not saying that this is not possible but at least you need to come up with a robust rationale as to why this would be the case. And I think it's quite clever not to touch upon the law enforcements, that side of things because law enforcement access is even more tricky than granting access to private individuals because what law enforcement can do to the individual is more impactful because it's concerning criminal law in most cases than civil law claims that might be pursued.

But all I'm saying is that I think it's a great starting point but we need to document more in terms of what is possible. And I think that we might not end up with being successful to grant every access to everyone but it might be limited and there might be additional safeguards such as volume limitations required in order to ensure that there is no excessive use that where actually we would not successfully be able to do the balancing act because let's be sure, if you do data processing based on 61F that allows for the data subject to object against the data processing. And I think that user groups these days are watching very carefully what's happening. And I think we need to do this job right in order to have the system being less vulnerable against user objections.

And second quick point, just one sentence, if the idea is to have an accreditation system that would work throughout all registries and registrars, I will let the technical folks talk to this but this has been discussed I think at least in the Registrars Stakeholder Group yesterday and I think it's unrealistic for that to happen before May. So I think we should rather be prepared that if there is then accreditation system at all it will only be applied to individual contracted parties.

PAUL DIAZ: Thank you, Thomas. Fred.

FRED FELMAN: So, just in response, we totally agree with you in terms of having a basis or interest specific to each one of these cases. And today, just a few moments ago, we sent a full table of purposes, the objective, the basis and interest, the processing required and the indicated users so that actually it's specified for each use case. And that should be available just after this meeting for people to see. And as soon as I know where it's posted, I'll let you know.

It was just sent to Goran just a few moments ago. We worked on it through the night last night.

PAUL DIAZ: Rough way to spend the night. Volker.

VOLKER ALEXANDER GREIMANN: Yes, that's good to hear. I'm with Thomas that it worries me a bit that once you're accredited, you would have theoretical access to all of the data even if there were subject to a certain volume limitations. I would much rather prefer a system where everyone would theoretically have the access to all data but they would still be required to provide a justification for each and every single request why they are legally entitled to that, to obtain that data, i.e., what is interest in obtaining that data, what is the justification for taking that data, what is the purpose they are following by requesting that data and so forth and so on.

And then that would either be subject to a review mechanism or if we find a better way to validate these requests and that would be okay as well. But I think allowing broad access, I'm not supposed to say bulk but quasi-bulk access where theoretically one would be able to create a mirror database of the WHOIS as certain entities are doing right now, or harvesting WHOIS data for other purposes, how well-intentioned they may be, that would be a problem. So this would have to be justification on a per request basis. And I would also see that certain requesters might be entitled to access certain data in certain circumstances but other data in other circumstances, they would not be entitled to and that those requests should be blocked at that stage. And I see nothing that would prevent unauthorized access in this.

PAUL DIAZ: Okay. Other points? [inaudible], go ahead.

FRED FELMAN: All right. Then continuing in terms of the accredited organizations at the top of the second page, to become accredited, an entity should be able to provide verifiable credentials or a letter of authority or endorsement or/and also be willing to agree to the terms of service to prevent abuse of the data access to be subject to being de-accredited if they are found to abuse the data and also be subject to penalties to be defined.

And also, a subsequent effort going on right now is trying to work with SSAC members and security organizations to establish a list of credentials that would be appropriate for each one of these parties. And that's to be provided in a third document that we're working on now.

So any comments on accreditation and what it requires to be accredited?

MICHELE NEYLON: Thanks. So, well first off, I suppose as others have said it's good to have something to actually look at which it's kind of helpful. The fact that this is still a moving object does make providing any meaningful input a little bit hard. But having said that, few comments, I share Volker's concerns with a lot of this. There's a few things which are missing here that do disturb me. I mean transfers abroad are a major issue. The jurisdictional issues are a major issue.

I can give you specific examples. As a registrar based in Europe, we have clients who are mostly based in Europe. But even within the European Union, we are not going to start giving out information about our clients to third parties who might go after them for a whole range of different things without following proper due process. And yet here, there is no real due process because once you give somebody this credential, they then have access to do whatever the hell they like. And if the actual document goes on about basically giving them the right to recreate the entire database, then that's a huge problem.

So, the other thing, I think, that you've tried to do is try to please everybody, which I think is a problem. You need to be a little bit more narrow in your focus. If you want to look at a narrow focus of say, for example, intellectual property concerns, then that would be treated, I think, in a very different way to some of the other groups that may have interest in data.

Another thing which I think you also need to look at is instead of this mirroring the current WHOIS which seems to be what this is pushing for is more looking at the outcome as opposed to the means to the outcome. There's more one way of recognizing patterns. There's more than one way of mitigating abuse. Assuming that the only way to do so is by getting full access to what is the current WHOIS I think is not exactly accurate. I think there could be more interesting ways of achieving the same goal. So, I think it's an interesting starting point but in its current form, it makes me incredibly uncomfortable.

GRAEME BUNTON: I'm going to jump in. This is Graeme. A piece around credentialing that probably needs to be captured across the board here – and apologies if I've missed it, I also haven't had a ton of time with the document – is that there will need to be a re-credentialing process. Credentials can't be permanent. People need to be de-credentialed when they move. Okay. Great. Sorry. Apologies. Carry on.

STEVE DELBIANCO: Graeme. When Michele asked about there could be better ways and then given the shortness of time, Michele would love to understand how to make this better or surface those better ways as soon as possible.

James Bladel was asking will there be other models. And James, I can say that probably not from the CSG. But if Michele says, "I can think of a better way," or if Stephanie Perrin mentions an ISO process this morning when Goran mentioned something about providing some funding and assistance to get it done, that, undoubtedly, there may be other models that are surfaced.

The purpose of this exercise was to learn ways to improve and refine this so that at least this becomes something viable. So, you're right, there may be other alternatives that can come in over the transom but we're trying to stay focused on this one. So, if you can think of ways to improve this, please put them on the table as soon as you can. Thanks.

FRED FELMAN: I guess I think I should say one other thing. So currently, the WHOIS databases exist as they are and the systems for access exist as they are. There is no relational database that sits behind this that allows you to provide more sophisticated access to this data in a controlled way.

If we were talking about a modern database as prescribed in some of the thinkings with RDS, you'd have that opportunity but we actually have a very short timeframe which is May. And we have a real interest in protecting public safety. So, the idea was, okay, what can we do in May, and then we should continue this process such that when we get to a more modern database that provides more sophisticated access and authentication controls, then we can apply the accreditation and we can also apply more precise controls to it.

But I guess really I do want to hear from you, Michele, because you said if we narrow our focus to IP and so I just wanted to ask you, how do you think that IP owners use the WHOIS database to actually investigate and find and how do you think we should actually change our processes because I'd really like to hear that.

MICHELE NEYLON: I'm not an IP lawyer so I don't know the ins and outs of everything you're doing. The thing is, what I'm asking you to do is to look at it in terms of what is it that you need working on the basis that what you currently have access to is going away. Working on the assumption that you can replicate what you currently have access to, I think, is a false premise. Because if you want this to work globally across multiple jurisdictions and in a clean and predictable fashion, you need to think a little bit more out of the box.

So if I've heard from people – and again I'm not an IP person, okay, so I'm not going to write a solution for you. I can't because I have no idea what it is you actually need. But what I hear is, okay, we have access to this now, that's going to go away.

So I'd counter that by saying, okay, in the ccTLD space, you don't have access to this, how do you handle it? What are you doing there? How are you dealing with that? Because if all things were equal, then it wouldn't actually matter what name space it was, whether it was a [co.uk], a .com, or a .agency. The level of infringement of reported infringement, the level of abuse or reported abuse would, generally speaking, be similar.

Now, that may not be the case but the thing is this is that we have read repeatedly from DPAs that the current WHOIS is illegal under the data protection law. The GDPR is coming. None of you will get fined, we will. And that is the bottom line. So it's very easy for you to say, "Fix my problem" but you are not subject to the fines.

FRED FELMAN: We're not saying fix our problem. And that's the purpose of the purpose is document to specify the specific purposes as opposed to the data itself. We're applying that to the existing WHOIS model and ready to apply that as the technology behind it evolves.

So, no, we're not just demanding that others fix our problems, we're actually tried to specify with some granularity about what our problems are and what we need to actually solve it.

PAUL DIAZ: I'll manage the queue. Sorry. I got distracted. Why don't I let Susan interject, Keith, and then Volker, Margie.

KEITH DRAZEK: Thanks. First, thank you all for bringing this document to us and giving it to us. We haven't had a tremendous amount of time to review it, obviously. I think the additional document where you talk about the uses and the justification will be critical for us to be able to read this, read that and compare the two.

I think it would be helpful for us to go through this document fairly quickly. I think we need to get through it. We can keep some questions and come back at the end and talk about maybe a handful of key points.

So let's get back to the document. Let's go through it. We need to be concise because we're running out of time. And then I think what we need to do is to schedule a follow-up conversation at some point whether it's this week or even the week after we get back from ICANN where we, having the benefit of having read both documents, thought about it a bit, got some additional counsel then we can come back and have a more in-depth conversation. Thanks.

PAUL DIAZ: Thank you, Keith. Susan.

SUSAN KAWAGUCHI: And just really quick. Michele, I can understand your frustration with us not being able to identify things but, as you know, this is all a moving target. And Goran sat there, or JJ sat there this morning and said they will continue to expect everyone to collect all that data. So right now, we may, if all that data is being collected and if there's a legal way to access it, then that's what we're going to request.

MICHELE NEYLON: I understand that. I get that. If I was sitting on your side of the table, I'll be doing the same, don't worry.

SUSAN KAWAGUCHI: But I think that what this model could do is be flexible enough that as the moving target is more defined, then we will, you know, center in on the data that's actually collected and that is accessible.

PAUL DIAZ: Thank you, Susan. All right, I've got a queue. Volker then Margie and then Reg.

VOLKER ALEXANDER GREIMANN: Okay, I'm sitting on Susan's side of the table. You might want to ask your colleague Alex how IP rights holders do it when they find someone infringing on their IP by file sharing. You go to The ISP, you get a court order, the ISP tells you who is behind that IP address. That's a legal process to find out who's behind a certain address.

Now, an IP address and a domain name are not that different so that would be the baseline. I'm sure that that's not something that we desire but if we can find a model that would similarly, in some form or shape, protect those innocent of anything and just allows you still to access the data that you need to find the actual infringers, I think we will be okay with that.

I'm not saying that we should have a system where you should have to obtain a court order for everything especially with some jurisdictions out there where it's not as easy as it is in my jurisdiction to do that. But at least under that system, the personal rights of the individual are protected by a third-party review.

So, what I'm trying to say is if we use that as a baseline and work ourselves up to something that we all want because we don't want to be subjects of court orders and subpoenas all the time as well although that would give us certain legal safety of course. For example, such a system where there would be a certain third-party review of every request even though that would cost money which would probably have to be paid by those requesting and which would also serve to drive down the number of requests on the other end, I think that might be a model that we should consider because it would be protected of [inaudible] data. There would be some third-party review of any requests and make sure that all requests that are made are at least conceivably justified.

PAUL DIAZ: Yes. Okay, Two more and then we'll draw a line under this and go back. So Margie and then Reg.

MARGIE MILAM: Sure. I think part of the problem is that the reason there's an emphasis on having more than one off lookups is because of the volume that's needed to protect major platforms and fight against some of the cybersecurity issues that happen out there. And so that's a real need that is legitimate and needs to be accommodated. The European Commissioners in that letter emphasize that point. And so that's part of what is addressed here.

And so, we just want to have you understand that a one off look up for cybersecurity purposes is simply isn't going to work. And so what we're trying to do here is come up with a mechanism that allows that to happen so that there isn't a proliferation of phishing and fraud.

And then to address the point about the ccTLDs, there is less abuse related to ccTLDs because they typically have more stringent rules on takedowns. They have enhanced verification requirements. And so, you have a lot less fraud because you have to actually verify the registrant in a lot of these ccTLDs. And that's again, an aspect that kind of factors into the levels of abuse that we see.

PAUL DIAZ: Thanks, Margie, Reg.

REG LEVY: Thanks. Instead of starting from the basis of you want access from everything, can you start from the assumption that you have access to nothing and then look at each piece of current WHOIS output and determine whether or not you actually need it?

The WHOIS in the tech field sections, for example, are very often exactly the same as the registrant. So, it is possible that you don't need access to the data. I know that you want it. I know that you think it's easiest if we just give it to you but from the standpoint of data minimization, do you need a fax number? Does anyone in this room have a fax machine? Do you need a fax extension number, Michele? That's a WHOIS field.

MICHELE NEYLON: I do have a lovely fax machine though.

REG LEVY: Everything you have is lovely. I'm sure that, again, that this is something that you want but I feel like it's being looked at backwards. So, start from the baseline of there is nothing, what are the most minimum pieces.

MARGIE MILAM: If I could just respond, this is an accreditation model. Those discussions are the discussions with the ICANN on the actual model itself. So, all we're trying to do with this is hone in on accreditation. And so, I agree those are issues that need to be explored but that's not what the point of this particular document was.

REG LEVY: But what I'm saying is that that's a conversation that I want to have with you instead of ICANN.

PAUL DIAZ: Okay. [Fab], please go ahead.

[FABIEN]: I'll be quick. I'd love to go back to what Keith said about getting through this model. We have a lot of people work really hard on this. And what we're trying to do is work with you so that we don't come to May 25th and have chaos, chaos for both sides.

What this assumes, and maybe we should have, at least when I read this document, I assumed this, is that one the calzone model is going in and Thick WHOIS is being collected. So, it's being collected. Two, that collection sits behind a gate unless you comply with the GDPR. Three, the GDPR applies, ergo, the GDPR Article 61F applies.

And this then addresses how you access the data that's been collected in Thick behind the gate under GDPR compliance. And all we're trying to do here, I assume, by reading this, is go through the possible steps that we envision on accrediting somebody who can comply with GDPR and access the data. I think it would behoove all of us to just work together to go through the document, read it and as Keith said get back to it.

And if Michele, Thomas, anyone has substantive and constructive feedback on this to put it in so that we can work in. And this is why I asked Goran 24 hours ago whether we could all get in a room together and just work something out and hammer it out. Because if we just keep coming up with hypotheticals or what if and what if and what if, the target just keeps moving, the 25th of May keeps coming and then chaos pursues. And I don't think that behooves any of us.

So, I'm asking as a member of the community, if we could all just please work together to come to a resolution and stop playing games with each other. Thank you for that.

PAUL DIAZ: Thanks [Fab]. Okay. Fred, back to you.

FRED FELMAN: Yes. I think for the sake of speed in expedition, I think we should probably go to the page 5 which actually talks about the certification process because between the point that we always specify one more type of usage which is for abuse against and the expiration of abuse for academic organizations and then we also go through some more detail of the different types of cases. But at the top of five, we actually talked about the case and it's listed as certification process at the top of page 5, I think. So it's certification process. If you just do a search for certification process – there you are.

So as a first step, an application would be submitted with contact details and a name, a physical address, an e-mail address, a telephone number. The required documentation for this process for cybersecurity and OpSec investigators, the credentials and letters of authority for intellectual property, evidence of IP ownership or a letter of authorization from the rights holder to act on its behalf. Or if we require more information, I think what we'd want to do is have the Intellectual Property Constituency and the Business Constituency come up with a list of credentials that would be helpful for this certification or accreditation

And then they would undergo a validation by an ICANN-approved agent. And we envisioned an agent, like for example, Deloitte or perhaps a certificate of authority that's in the habit of authenticating credentials and giving credentials to an organization. So a third party, that way ICANN is not responsible for giving these credentials.

Once the entity successfully completes those steps, the agent or the individual would be issued credentials or a certificate and/or the application would be rejected. And in the case that the application was rejected for lack of detail, they could actually resubmit if they paid the fees a second time. And re-accreditation is part of the process. I heard that mentioned, and we'll get to that in a second.

In terms of proposed operating model, we looked at the EWG Final Report. And it looked like that was implying that was the next generation RDS behind it for their recommended model, which isn't the case of how the WHOIS database is architected. So, we took a different approach and we thought about this as a sort of a federated certification model, where a certificate would be generated and given to the entity and they would use that as a credential to access the databases. And there's a diagram at the top of page 6 that talks about how this might work.

So an accredited entity would present its credential to the WHOIS database provider. The credential would go against a centralized access authority and then they would be granted access to the data. And that's how we envisioned it to try and do it in a simple fashion.

In terms of some other elements that were mentioned, if we scroll up a little bit, upon accreditation that the users are given credentials and they're able to access the data, the contracted parties will validate those. In terms of logging, because the databases are again distributed, each one of the WHOIS databases would be able to log the access by the accredited users of the system and they would be able to actually assert who is accessing it. The types of certification would indicate the type of user the purpose, so they'd be able to see why people are actually accessing this database.

In the instance that there is a suspicion of abuse, an audit could be triggered of the usage of the data. And then we looked at sort of the EWG Report and Audit Principles, and we think that the model that modeled the EWG Audit Principles would be one that we should consider.

There are a couple of different ideas we have for a central access authority. And we've reached out to DigiCert and we've reached out to Deloitte to think about operating a centralized access authority and also to run the credentialing system to see if they're able to provide this in time for the May deadline, and hoping that perhaps we might be able to find a practical vendor to provide that.

I'll pause now to see if there are questions about the accreditation and also the operation.

STEVE DELBIANCO: Paul and Graeme will give you a quick heads up. The bizconst.org/accreditation page we referred to. It now has the purpose statement listed there as well. It was the original page we brought up. No need to move – I don't think – to move the screen. We'll say on this document but the document that Fred talked about is now there. Thank you.

PAUL DIAZ: Thanks, Steve. Okay. I have a queue and I'm not sure who I saw first but ladies first. Let Sam [go] then Michele and Rubens.

SAM DEMETRIOU: Thanks, Paul. I wanted to just come back to this audit notion. If I'm understanding correctly, the auditing entity is going to be able to look at the user and what purpose is associated with that user class and the data that they then access. My question is – and this is something that also came up when it came to the terms of use – have you guys thought at all about like how that data gets used beyond what's stated in the purpose? Because I think this is something that's a big open question and the idea of how actually enforce these like codes of conduct or the terms of use that are put in place. I don't really see and enforcement mechanism there. And that's I think a big hole, which is not a criticism. It's just an area to go back and think about.

FRED FELMAN: And what would you envision in terms of an enforcement mechanism? Do you have any thoughts on that?

SAM DEMETRIOU: Not yet.

FRED FELMAN: I guess there are a couple of things that we thought about as we considered this is that, for the case of intellectual property investigators and others. Most of these individuals actually have law credentials and are subject to ethics and other professional responsibilities that actually could result in the removal of their credentials or other legal and other penalties for the misuse of data.

So those folks are actually most often protected by those types of things. So they have a lot at stake actually if they were to steal data and use it to spam people in order to try and solicit their domain name registration. And I think the number of cases that you could find of intellectual property attorneys actually doing that would be relatively low.

With respect to some of the other classes, I'm not sure how we respect those but that's one that we have actually thought about. And that's why we would like for the cybersecurity community to help us assert who and why and under what condition we might actually generate those credentials from the cybersecurity community.

PAUL DIAZ: Thanks, Fred. Michele.

MICHELE NEYLON: Thanks. The separation of the accreditation from the data – there's a bit of problem with that. Because essentially if say, for example, in a wholesale model I have a resellers, now divulging, giving you access, if it's something beyond the gate, if for the example that the reseller name is behind the gate. I'm not saying there is but if it was hypothetically, that's low. That's a low-risk thing. I have no issue doing that in many circumstances. But giving say access to more sensitive information or higher volumes of queries, etc., etc., etc., that's something that obviously would make us more uncomfortable. Because not all data elements are created equal. [inaudible] wants to paraphrase George Orwell. It's just something just to consider in terms of how that would work.

The other thing is well around some of the costings around that. I mean, I think it's good you got some of it covered but expecting the WHOIS operator to cover the cost of the audit if there's a small operator that actually is a bit of a problem. Just bear in mind, if you look across registrars and registries, there are registries who have literally two staff, three maybe. Registrars the same. Some of these are very, very, very small operations. There are others who are obviously significantly bigger. So just looking at it in terms of cost burden and everything else, so that needs to be… In fact, I'm glad you got some stuff in there. I appreciate timing and all that but just something to keep in mind.

FRED FELMAN: That's super helpful. Thank you.

PAUL DIAZ: Okay, Rubens.

RUBENS KUHL: Just concerned on the fee thing. I wonder if you are proposing that not only the audit but the operation of the centralized system, etc. is to be paid by users accessing WHOIS or are you expecting some of the cost to be on contracted parties?

FRED FELMAN: A simple answer, we're not expecting the contracted parties to administrate or to pay for this at all. The central access authority would be funded by the fees and the renewal fees by the users of the system.

MICHELE NEYLON: Day one you have zero users, zero fees collected, so therefore you have zero system.

FRED FELMAN: Yeah.

MICHELE NEYLON: Somebody would have to front the cost of building this. If you're doing it on a cost recovery model, you can't build it until you have money to build it because last time I checked, developers expect to get paid. Now, if you can find a bunch of developers who will work for nothing, could you please share their details with me because I'd love to have them?

But joke aside, if this is going to be built, it has to be funded from somewhere. If it's going to be funded by yourselves or somebody, fine. But if it's being funded via ICANN then ultimately it comes back to the contracted parties, so I'm just trying to understand how you're going to do that.

STEVE DELBIANCO: Let's assume that if we move ahead and got a design, a functional spec that met the legal muster and some degree of acceptance by contracted parties and ICANN, at that point I don't believe there'll be any trouble at all obtaining the funding from those who use it. So please just go on faith that paying for the development of it would be something that would flow from its acceptance and legal muster, and let's not try to cross the bridge right now.

Am I in the queue now? I wanted to address Sam's point on enforcement. Sam, let's make a suggestion maybe that the document while it has audit on the screen in front of you, that audit is well after the fact of when you may suspect that there's some abuse going on. So we would want to add an abuse reporting mechanism so that the clearinghouse – I'm sorry – the accreditation operator could investigate and potentially remove the credentials, put the person on a blacklist so they don't get credentialed again tomorrow. And then, when it comes to enforcement, it's really referring it to a DPA that has relevant jurisdiction because the accreditation agent is not one who can do any law enforcement. So the enforcement I'm thinking of is kick you out, blacklist you and refer to a DPA with all available information. Does that begin to get down the line of the hole you identified for enforcement?

SAM DEMETRIOU: Yes, I think so. I mean, the concern being that the party who ultimately does the disclosing could then have the liability for the misuse of that data, right? So just making sure that that's an area that we cover. So thank you, Steve.

PAUL DIAZ: Okay. That's the queue so back to you, Fred.

FRED FELMAN: That's super good. Thank you. Thank you for that, Steve and Sam. I think maybe we should move to page 8 which is the terms of accreditation and let's talk about what the terms are for usage of the data specifically in the data protection section and then go on to application fees and access.

So first of all, in terms of accreditation, the data has to be used and they have to recognize that this is personal data in their custody and they have a responsibility to protect that data. That they need the gate access to that data while they're using it for analysis, that they have to secure the data at rest through encryption, that they have to secure data in transit through encryption and they have to validate with each login that the users actually have accreditation for use of that data.

The application fees, they'll be a nonrefundable fee and they will be proportional to cost of validating an application and also the operation of the service itself. In terms of data access, the data access is only, as we said, for legitimate use for either single record queries or automated queries for analysis. The accredited access shouldn't be rate limited other than is practical for making sure that the system operates so it shouldn't threaten the database operator with too many queries. The data has to be stored in a safe way by the accredited users.

In terms of the misuse, in the event there's a breach of the terms and condition, the user should immediately lose rights to access the data to retain or use the data is also suspended. And upon the notification of the breach, the user's access privileges should be revoked and that the user is also informed that they must delete any retained data and provide notice to the certifying body that actually the data has been deleted. The data misuse violations could be appealed to the accrediting body in the case that they think that this has been done in error. And those are sort of the main elements of data misuse penalties.

In terms of data misuse itself, they shouldn't be mining the data. They shouldn't be revealing the data accidentally or on purpose as the result of a security breach or some other exfiltration. They shouldn't be selling the data to non-accredited parties for any reason, and the use of data should be appropriate to the accredited user type. And other than that, they should not be using the data. That's more about the terms of service and data protection, application fees, and misuse.

PAUL DIAZ: Volker?

VOLKER GREIMANN: Let me start by something very positive. I actually like a lot of the basic principles, the ideas that went into this paper with regard to who gets certified, how that works, what is required for certification. There's a lot of very good stuff on that that we can build upon. We should divorce the two questions of how the certification works, what the requirements are, what happens in kinds of misuse from the question of what kind of access does certification grant you at this stage. I think we should focus on what does certification mean, who can get certified, what class of certifications we need, what does that entail, what requirements do they have to meet? And once we have that in place and agreed, then we can move on to the second step and say, "Okay, now you're certified, what does that actually get you?"

FRED FELMAN: That's good thinking.

PAUL DIAZ: Other inputs? Thomas?

THOMAS RICKERT: Yes, I have a general question, particularly with respect to the security researchers. And that is has any thought been put into whether they need the real data or whether, for example, pseudonymised data can do the trick for their research purposes? Because that would be less invasive than getting all the real data out there. And just to add to that security dimension, it is perfectly possible for the registries, for example, to hire a security company to analyze their zone, right? That would be covered and perfectly okay under the GDPR. So I think that we need to make a distinction between a registry that claims to have a legitimate interest that claims, that wants to ensure that there are no illegal activities going on in their zone.

And that would need to be treated differently from external parties that want to get access.

FRED FELMAN: So let me make sure that I understand this. So you're suggesting to tokenize the data and anonymize it and actually have relevant fields of similar data tokenized in exactly the same manner? That's worth discussion especially if we could across all registries perhaps with the implementation of RDS to have a standard e-mail address or a standard registrant identifier across all of the registrars and registries. That would be extremely helpful because that's where a lot of the correlation occurs.

I think we've got this sort of baby step model. And I think maybe what we should think about is what can we do in the very short term of getting this done in May and then how can we actually refine this, so that actually we could do the tokenization as you suggest across all of these databases to limit the amount of data that's presented. And then as we go to the RDS, be able to have much more granular control over what fields and what records are available based on purpose. And I think it's an evolving thing and I think that's a super great suggestion, Thomas.

THOMAS RICKERT: Just a quick follow-up. I think the way that I read/research on domain name abuse and stuff like that, there are researchers who look across all TLDs, [other] looking at specific TLDs, and once we are working on the system to be refined, there might be cases where it's good enough to look at an individual TLD and others where you need multiple TLDs. And then certainly the same hash mechanisms or whatever you might use to pseudonymise the data need to be applied to make the research meaningful. But I think that this is exactly what needs to be done in order to reduce the impact of disclosing data.

FRED FELMAN: Okay. That makes a lot of sense. Thank you.

PAUL DIAZ: Yes, Tim?

TIM CHEN: Tim Chen with DomainTools. I think that's a really thoughtful question, Thomas, that you asked. At a high level, based on our experience, what's called attribution, which is really getting to the individual or organization behind a cyberattack or abuse of some kind is definitely in the minority, if you look at all of the security use cases that happened on a daily basis scale that involved this data set. As Fred pointed out, so I won't repeat except to say, the correlation aspect of having a unique identifier is incredibly important. But if you can separate that somehow in the model that happens behind the gate and there are more specific purposes for actually understanding who the individuals are that would fall in the minority. And so I think it's thoughtful to consider that as part of a solution that maybe we can find a balance of the equities here.

PAUL DIAZ: Thanks, Tim. Steve.

STEVE DELBIANCO: Thanks. We have under 20 minutes left, so I think Fred has reached the end of that first document. Right, Fred?

FRED FELMAN: Yes, that's correct.

STEVE DELBIANCO: And I don't really think there's sufficient time to load the second document which again is bizconst.org/accreditation. So I would ask one question of the contract parties. If you were to assume, suspend belief, disbelief for a moment and assume that the functional spec began to meet what Volker talked about, the requirements for the appropriate who and how one gets certified/accredited. And that we – Volker, we came up with a data model mapped to the individual characteristics of those were accredited. Then moving from a functional spec to a technical spec becomes on the critical path but so does helping to figure out the alignment of the appropriate agent contractor and then working through the development and implementation timeline. And it's insanely tight, but all of you are in the middle of insanely tight timelines on implementing your own GDPR solutions with or without ICANN's proposed interim model. So I would benefit greatly from an exercise where the contract parties discuss what you see as suggestions and concerns about the implementation path assuming that we all could come to agreement on a functional spec and a technical spec. Is that possible? Thanks.

PAUL DIAZ: Okay. Well, as we said at the beginning, Steve, I mean the takeaways – and we'll definitely come back to this when we get back to as Keith has suggested – make sure both documents, if you can send them to me because I'm probably going to [inaudible] the address, make sure they get out to the list and give us a little time. But can we kind of straw poll here when do we want to try and get back together? Are we going to do this all over e-mail? You want to try and use… I mean –

STEVE DELBIANCO: We can't use Adobe anymore.

PAUL DIAZ: Yeah. And that's something that – normally I would offer the stakeholder groups' Adobe room for a conference call but maybe it'll be back up. Margie?

MARGIE MILAM: I was just going to say that I'm going to talk to David Olive and the Policy Team to just work on logistics. So the question is would it make sense to have a call next week to follow up on this, give you guys some time to think about it, work with the Policy Team to set up the appropriate time. Is that something you guys think you'd have enough time to be able to start really discussing some of these issues?

GRAEME BUNTON: It's hard, I think. I think it's hard to put a time. The registrars in our Stakeholder Group Day the other day sort of agreed to spend about two weeks working on the interim model and filling in the gaps. And so I think that's our number one priority for the next two weeks. And then after that, I think we can think about it. It's hard to put a pin into that.

STEVE DELBIANCO: Graeme, do you log Port 43 queries today as a general matter?

GRAEME BUNTON: Yes.

STEVE DELBIANCO: I think that's pretty widespread with respect to the contract.

GRAEME BUNTON: I'd be surprised if it weren't.

STEVE BELBIANCO: Okay. So perhaps the logging is there and 43 works but the trick is it doesn't have a credential check at this point. And so what does your mind tell you is the easiest, simplest way to modify your Port 43 response mechanisms so that they only allow a response for some sort of a token or certification key?

GRAEME BUNTON: I don't think… This is not a secret although I don't have anything to share. Tucows is working on its own credentialing model, credentialing program, and it's built on RDAP. And so 43 will exist but it's going to have the minimal data set in it, and anything else is going to be built on different tech.

PAUL DIAZ: All right. So we're back to the limited time constraints. It might be a couple of weeks before we get back to you and that feels like way too long. So I'm not sure what else we can do though. Thoughts?

STEVE DELBIANCO: To try to maintain momentum, we went ahead and displayed this purpose statement, which I haven't read yet. It just came from the companies that are working on it. We'll definitely accommodate sending the link to both of them. And yet, the feedback from today, I think in a constructive spirit – I'm looking at Fred, Margie and others – a constructive spirit was to do a Version 1.2 based on the input that's here today. And where there's comment about which we don't have an answer, we should put in there. As noted on the 14th, Volker was very concerned about X and put it in there. And know that we'll have to get to it later, just to take the functional spec to the next step.

It's way too early to go to a technical spec, but we can take the functional spec to the next step in 36 hours or something. So when you guys have arrived back at your homes, you'll have Version 1.2 plus the purpose statement together. And I think that if you can in 10 days or so try to come back with a further set of questions and suggestions, I think at the same time we'd start to move in parallel on a more technical spec including fleshing out more the data model and how it might map to the access credentials of the individual which was Volker's [inaudible].

PAUL DIAZ: Okay. How do my contracted party colleagues feel? Is that sensible, Volker?

VOLKER GREIMANN: It definitely sounds good although I would see that the technical implementation comes at the end. So when I say the first step would be to develop a credentialing model, the second model would be who gets access to what, and the third would be based on that, what limitations, what we need in the implementation to make sure certified… I wouldn't look at certification alone as the requirement to access certain data but certain other conditions also being met.

For example, I still think that law enforcement should be limited to make requests in their own jurisdiction. That's of course debatable. That's currently my opinion. I'm still prepared to be convinced otherwise. But in that case we go that way, we would have to have certain limitation that would limit the access of a law enforcement agency that has been certified to only gain access to data that they would be allowed access to. And similar rules would of course also apply to other certified bodies, other certified interests.

So starting implementation talks now without having defined first who gets access to what, which would be the second step in my view would be premature because we would be developing something that we haven't still defined yet, which is always unwise. It costs more development resources than it actually should.

PAUL DIAZ: Thank you, Volker. Other thoughts where to go from here?

STEVE DELBIANCO: A follow-up for Graeme, if you don't mind. Graeme, the secret is out, right? I'm just joking, what you said earlier about Tucows looking at an RDAP-based implementation with credentials. Is that something you were thinking we should put on the table to compare and compete with what's here? Is it on a timeframe that is soon enough that an RDAP-based distribution model could be done by May?

GRAEME BUNTON: It's unfortunately not up to me to – you know, I'm not the product guy. I'm not building it, so I don't really have a sense of timeline. Our intent is to get something done by May because we know we need to give access to people and we think that's a responsible thing to do. And we are not confident that something else is going to arrive between now and then.

I'm pushing internally to see if we can get something out that we can share and then we can compare and contrast. My impression is that there is much of this that is aligned but there's going to be some differences for sure. But I don't know when I could really get something out there for people to look at. Now that I've said this publicly, I will up that pressure because I imagine people really want to see that.

STEVE DELBIANCO: I fully appreciate that and understand about the pressures on the backend, too. If you can share anything with respect to your own functional spec without giving away anything that you feel isn't appropriate, I think it would end up being – you'd lay it in parallel to what's here and the differences in accreditation, methodologies, enforcement and so on, we'd be able to meld those pretty quickly because it's almost always going to be the same.

But does the implementation through RDAP instead of 43, does that end up changing how quickly it could be implemented by a broad array of registries and registrars? Will they be able to implement an RDAP-based model by this summer?

MICHELE NEYLON: RDAP is a protocol, WHOIS is a protocol. The WHOIS protocol as it currently exists has a lot of limitations. Some registries have put extra layers on top of it to a degree but I mean it's like trying to drive a Ford Escort at 150 miles an hour. I mean, you might get it to do it but it'll probably explode.

RDAP itself isn't a client. I mean what you would be doing is you'd have RDAP on the backend, you'd have something else on the frontend. So in terms of implementation, apart from anything that Tucows might be working on, I know some of us have been discussing internally with developers and other people different ways of rolling something out. But what exactly that would look like and the timelines around that is something that is very, very hard to speak to with any degree of confidence because we've had this entire – it would be best described as a mess – has been moving so ridiculously fast over the last few weeks.

You've got an interim model out there, which I think that was distributed while most of us would have been traveling here. So you're getting people asking you to make comments about something you barely have a chance to look at. Some of the larger companies might have put some resources into reading it but a lot of us… I mean even the big companies have had difficulty with that.

If you look across the Registrar Stakeholder Group, we have what, about 100 members, Graeme? Something like that. So we've got about 100 members and they range… and some of them are from English-speaking countries. Others are from countries where they speak many languages, English is not one of them. And seeing how they will actually understand and interpret what they're being asked to implement, it's not something that we can just kind of switch on and off quickly.

So I can't give you a… I think as Graeme and others have kind of tried to point to, the interim model is where a lot of us are focused at the moment. This would have to go behind that. I think a lot of us don't have the bandwidth to be looking at both at the same time. That doesn't mean we can't talk to you but it's a bandwidth issue.

STEVE DELBIANCO: Technically specific. I would hope that everyone in this room would agree that it's better for all the registries, registrars and the users of WHOIS to try to have one model than to have a separate one at Tucows, a separate one at Black Night. I see a few heads nodding. But if in fact the contract parties each want to pursue their own paths, then let us know so we'll have to figure out how we're going to have to deal with that. And it's a nightmare from the users of WHOIS side. I got to believe it serves the interest of the thousands of parties involved to try the best we can for a unified solution.

PAUL DIAZ: Thanks, Steve. Alex?

ALEX DEACON: Yes, so I guess I just wanted to agree with a lot of what's been said. I agree with Volker that I think at this point in time that the main focus should be on the accreditation framework. And we are looking for feedback from you guys and we've got a lot today, which we will incorporate. I think the implementation of this is important. I think ultimately we'll end up in an RDAP world. I can't see how you could do any of this on Port 43 easily and it would be throwaway work which is not great.

But I would just caution us not to get too caught up on implementation details at this point. Let's make sure the framework is correct and solid, we have a way to get credentials and to use the credentials at some service. And then we can fold in the details of what data gets returned and the mapping that Steve mentioned earlier based on the discussions that are going to be happening on the interim model. And then once we've put that together, we could start thinking about technical implementations and timing and all of that.

But it sounds to me that we have a path. I mean, the timing is going to be a challenge but I think we're on the right path at least.

PAUL DIAZ: Thanks, Alex. Tim?

TIM CHEN: Thanks, Paul. I apologize that I was late. So if this was discussed then we can ignore my question. But based on just what I've heard while I'm here, if we are going to work… if there's a two-week period where contracted parties need to work on filling in the gaps which I can totally understand, and that's going to focus more on the interim model and then what happens outside the gate. And then we focus on the accreditation process and how that's going to work, which I understand that's a logical thing to say and whatever it is today, May, March 15th – then it seems like this will all take some time. We're going to get past May 25th by the time we actually start giving accredited parties the technical solution to actually get access to some amount of data that a party has decided that they have legitimate access to.

So the question then becomes, if that's the order of events here, on May 25th is there any consensus among the contracted parties as to how you're going to handle all of the data sets that aren't going to exist outside of the gate? Or is it going to be Registrar A is going to just not give any access until we figure out how we're going to do it? Until we do it right we're not going to do it? Or is it still going to remain the way it is today until we implement whatever the future model is? Or has that not been discussed?

PAUL DIAZ: I think it's safe to say, Tim, that it's being discussed but I can't give you an answer yet because nobody's come to those firm conclusions. Volker?

VOLKER GREIMANN: Yes, somebody said this would be a nightmare for many. And I would like to chime in that for most contracted parties, this is a nightmare too in implementation and the chaos that will result because a lot of our processes that are ingrained in our systems will also stop working. For example, we will have issues with transfers and issues with other things that will break. So we are also very cognizant that this is a problem for many parties including ourselves.

And as for the timeline, I expect currently that most registrars are currently in the process of building their own system, which does not necessarily match the template that ICANN is providing simply because of the time constraints of having an implementation that needs to be ready by May 25th. Once that is done, then the resources can be shifted to implementing a common model that would then be closer to the ICANN model. And after that, the implementation timeline would shift to the certification model, implementation of the new WHOIS system. But that all takes time and resources that we will have to devote to this. So there will be a time where you will have to ask every single provider for themselves or use different systems to access that, go to Tucows's individual system, go to Kesis's individual systems because simply there is no more time to finish this in time.

Our implementation schedules are full. There is not much chance of changing anything in the short term. We just have to face the fact that there will be some phase of unpleasantness for all sides – us, you, everyone – will have issues with this. And all we can promise is that we will work diligently with all of you to try to find the common solution down the road. But when that will be implemented, I cannot say at this time. It's just a fact of business realities and timelines that we have to accommodate.

PAUL DIAZ: Okay. It looks like you're going to get the final word, Michele, because we're almost at time.

MICHELE NEYLON: Paul, I love it when you do that to me. Just so that you guys are aware, the Tech Ops Subgroup Committee – whatever it's called – of the Registrars and Registries have written a letter to ICANN to GDD. It's available on the same page as the other documents related to all this privacy discussion essentially looking at how transfers of domain names would work in a post-GDPR space. As you are all probably aware, we currently operationally use certain things. Like we send e-mails for FOAs. There's WHOIS data that gets moved around, that gets copied, etc., etc., etc. So there's a bunch of policies that are currently in place that will no longer really be fit for purpose because the data just won't be available or the access to it will change quite dramatically.

So we're trying to initiate some kind of dialog with GDD because ultimately, from our perspective, the domains still need to be able to move around. I know that some people would love it if they stopped moving around but realistically speaking, that's an important thing that we need to look at. Thanks.

PAUL DIAZ: Okay, thanks, Michele. All right, Keith? One more? Go ahead.

KEITH DRAZEK: Thanks, Paul. I know we're running out of time or are out of time so I'll try to be brief. I think in response to the previous question about what's going to happen on May 25th, or have registries and registrars reached some sort of a consensus about which direction you're going to go and what you're going to do. I think the answer to that is no. I think you heard pretty clearly there's not been an agreed-to position or approach or implementation or this. Everybody is going to probably end up doing their own thing on May 25th or just before because there's no time to implement probably even what ICANN is proposing as the model by that date. So to Volker's point, there is going to be a period of unpleasantness for everybody.

And I think it's important to note that – we heard in the ICANN Board session with the GAC yesterday that essentially – I mean the board, Goran and Cherine were asking the European Union GAC reps to go to their DPAs and seek some either guidance or even some guarantee of forbearance for a period of time. And I think that's again a recognition that time is too short to actually be able to implement anything across the board that will ensure that contracted parties are not exposed to undue liability and risk and uncertainty and that the users, the legitimate users of WHOIS data would continue to be able to have access as they do today. I think there's recognition that that forbearance or something of a period of time would be helpful to all of us. But I don't think there's any guarantee at this point that that's a viable solution or anything that we can bank on.

So I hope that helps just put it in context and provide a little bit of… maybe a higher level view. But I really do think this has been a helpful conversation. We need to keep this conversation going because whether this is what's implemented or something like it on May 25th, maybe its June 25th, maybe it's August 25th, but I think we need to keep this engagement going in this constructive way. Thanks.

PAUL DIAZ: Thank you, Keith. Well said. And to that end, we'll continue to communicate just probably the easiest way, the conduits sharing information. These particular sessions that we've done, we've done them for a while now and personally I find them amongst the more substantive. Good discussion. I appreciate everybody's time today and we will see you around and about.

UNIDENTIFIED MALE: All right. Thanks.

PAUL DIAZ: Thanks all.

[END OF TRANSCRIPTION]