WHOIS Working Group
Teleconference
TRANSCRIPTION
Wednesday 18 July 2007
13:30 UTC

Note: The following is the output of transcribing from an audio recording of the WHOIS Working Group teleconference on July 18, 2007, at 13:30 UTC. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. The audio is also available at:

http://audio.icann.org/gnso/whois-wg-20070718.mp3

http://gnso.icann.org/calendar/#jul

Attendance:

Philip Sheppard - WHOIS wg chair

Jon Bing - Nom Com appointee to Council

Steve Delbianco - CBUC

Avri Doria - Nom Com appointee to Council

David Fares - CBUC

Palmer Hamilton - observer

Genaro Hathaway - observer

Marcus Heyder - observer

Doug Isenberg - IPC

Susan Kawaguchi - CBUC

Tom Keller - Registrar c.

Dan Krimm - NCUC

David Maher - gTLD Registries

Steve Metalitz - IPC

Margie Milam - Registrar/IPC

Jon Nevett - registrar

Richard Padilla - observer

Kristina Rosette - IPC

Fabio Silva - observer
Michael Warnecke - observer

Absent Apologies:
Yaovi Atohoun - observer

ICANN Staff:
Maria Farrell - GNSO Policy Officer
Glen de Saint Géry - GNSO Secretariat

Philip Sheppard: Welcome everybody. We'll make a start now on today's call and maybe some other people are joining us. I ask your patience. They do join us. They join in silence but they'll be recorded on the notes of the call.

Our agenda today is going to start with one of these areas that have some discussion previously on the list that's to do with the Reveal Function or its alternative.

We can then have some brief discussion to do with Section 6.5 and authentication and its practicalities and get an update from Maria on the star support. And if there's any time left we can have a quick review of the edits from last week on the discussions we had then.

I am hoping that if we're successful and in and a bit of clarity today, then we'll probably have another two calls for the next week and the week after at the same time to finish off our work.

And they would be focused really on reviewing the entire report. I am just checking why we needed to change any text or to make any changes to levels of agreement.

So if we can hold your calls on item agenda one which is – you'll find the Section 3.2 of the draft report version 1.4, the Reveal Function.

Now the original thinking behind the Reveal Function was this is revealing the hidden data that would be now to the benefit of natural persons. And there will be circumstances under which reveal might take place.

And this is an activity that the OPOC would do following a certain chain of events we have described previously under the relay function which could mostly be connected with failure of the relay function to give us a satisfactory response to either concern about alleged fraudulent activity or concerns and things like inaccurate to his data.

And there had been some discussion on the list as to whether or not that Reveal Function is necessary. An alternative to it could simply be a direct contact to the registrar by the requester who had some concern in terms of the way that the relay function had operated otherwise it may haven't come back.

And that direct remedies would then be sought by the registrar of the sort can be described in Section 4 under compliance and enforcement.

And so today's discussion really is to see if which of those alternatives is best and to see where there may be circumstances where one of the other is going to be useful in some respect or other.

So I'm very happy to take a list or anybody who wishes to speak on either side of that debate or make some alternative comments?

Fabio Silva: This is Fabio Silva from Burberry. I'd like to be in the queue.

Dan Krimm: And this is Dan. I'd like to be in the cue.

Philip Sheppard: Uh hmm. And there was Fabio and there was Dan Krimm. Anybody else who want to take in the queue?

Steve Del Bianco: Steve Del Bianco.

Philip Sheppard: Steve Del Bianco? Anyone else?

David Maher: David Maher.

Philip Sheppard: David Maher. Anyone else?

That's fine. Let's start off with (unintelligible) Fabio Silva.

Fabio Silva: Yes and first of all I want to apologize that I came into this rather late. This is my second call. So I apologize that there are certain issues that maybe have already been discussed.

And if, you know, at any point fell free to stop me if it means I need to go back and read something here.

Philip Sheppard: Sure. And just to remind us which organization you're with?

Fabio Silva: I am with Burberry Ltd.

Philip Sheppard: Okay, thanks.

(Richard Padela): (Richard Padela) here. Sorry.

Fabio Silva: This is Fabio again. The issue that we have here at Burberry particularly because we're doing a lot of anti-counterfeiting work is that that we need to contact information of individuals that own websites.

And that information is specifically found through WHOIS And the way would - what we have found typically when dealing with for example Proxies which I kind of see is now being the OPOC is that if I contact the Proxy and I provide with them the notice of infringement then I tell them that one of their customers is offering for sell counterfeit merchandise on its website and therefore please disclose to me the contact information of that individual.

Rather than disclosing the contact information of the Proxy forwards my notice of infringement to its customer. And if the customer then goes ahead and takes down the infringing content, the Proxy then comes back to me and says, "We're no longer obligated to give you (unintelligible)."

Now my concern here is, is that we may see a lot of instances as this. And that if I contact an OPOC and I say, "I need this information because this particular website is offering for sale counterfeit Burberry merchandise."

Is there a cure period? In other words, will the OPOC go ahead and relay my message to the registrant? And if the registrant goes ahead and remedies the problem and tells the OPOC, "Tell Burberry that the problem has already been already been taken cared of and therefore do not disclose my information."

Then if that's the case, then Burberry really hasn't gotten anywhere. And of course, I do speak on behalf of Burberry but these are issues that a lot of the brand owners have.

So will there be a fixed obligation for the OPOC to disclose that information even within the next 24 hours the registrant goes ahead and fixes the problem?

Philip Sheppard: Okay. And so for you and this is exactly the debate as to whether or not that Reveal Function would take place. And for you the preference to know who the registrant is as opposed to being able to go directly to the registrant and have the website taken down is what?

Fabio Silva: The preference to know that information is so that way I can get a demand letter sent out to the registrant. And put that registrant on official notice of our demand. And so I can identify them for purposes of possibly a civil suit.

Philip Sheppard: Okay. Pretty clear. Thank you. Dan?

Dan Krimm: Yeah, thank you. The point - the real point I wanted to make here was that we have two duplicated ways of getting to hidden WHOIS data that we're talking about. There is the reveal and there is also the access.

And whether or not a remedy substitutes for reveal is not really the issue here, if you have some sort of, you know, verified access that we were talking about in our subgroup B.

I see no reason for any kind of involvement of the OPOC at all. That would just seem to slow things down. And if we get the access configuration right, then those who need timely access will be able to get it.

They won't have the delay of having to go through a third party OPOC. And they could, you know, they could get it directly from the registrar in cases where it's authenticated.

So I'd still - ever since I first heard of the Reveal Function, I never quite heard an argument that suggested to me why we should have that in addition to access.

And if we do have a Reveal Function, we probably don't need to worry about any other form of access. But at the same time, we still need to worry about authentication of requesters of the information regardless of whether it's reveal or access.

Philip Sheppard: Oki-dok. I mean for me Dan, the only difference I see there is potentially one of who the requester's interlocutor is going to be.

Under the review of proposal, you're still involving one of potentially in tens of thousands or millions of people who may be appointed as the OPOC. And the debate is staying within the realm of the requester and the registrant and the registrant's agent.

In the access discussions, you're immediately going to the registrar for that sort of information. And typically under those circumstances there's always the implication of bad faith I think in some way in our discussions there.

And so, I just think that perhaps the difference is potentially one of scale and scalability.

Dan Krimm: Yeah. But when we're talking about access, we're talking about sort of a pre-authentication before it gets to the registrar and by the time it gets to the registrar it probably will be highly automated along the lines of the port 43 systems.

So, basically we're talking about how do we – how we verify the legal status of this transaction? And I don't know that by going through OPOC, we necessarily clear up the situation in any way.

I think we might as well, you know, we're - if we're - if that is going to go through the OPOC then there is going to be a necessity for some sort of formal legal arrangement with the OPOC.

And, you know, we're going to be dealing with formal legal arrangement that's why we were talking about a law enforcement agents and that sort of thing.

Philip Sheppard: Oki-dok.

Steve Metalitz: Philip, this is Steve. Could I get into the queue at the end, please?

Philip Sheppard: Sure.

David Fares: And could – this is David Fares. I'd like to as well.

Philip Sheppard: Oki-dok. Steve Del Bianco?

Steve Del Bianco: Thanks Philip. I really wanted to respond to Dan's question about justifying why we have reveal responsibility attached to an OPOC. I want to clarify having been the one who pushed for it early.

Is that I took my queue from Proxy today where the Proxy registrant is the place to go to reveal the true registrant. And that's because the registrar doesn't even know who the true registrant is because they put in a proxy's name.

So in the case where the registrar doesn't even have the true registrant's information or it's inaccurate, only the OPOC who is acting as an agent for the true registrant, would have the information of revealing who they are. And Burberry gave an example that for legal processes, the identity of the true registrant is necessary, not just via email.

Dan Krimm: Can I respond to that?

Steve Del Bianco: And I've – well, let met finish really quick there. So I believe that in the cases where the registrar doesn't actually know or it's simply inaccurate, there is a higher probability that the OPOC does know the true identity of the owner of the website.

The second point I want to make is even where the registrar does have correct information of the registrant hiding behind the OPOC, there are

going to be parties who need to contact them, will not be able to qualify I fear for some of the access restrictions that we're placing on access to registrar data.

So for those individuals requesting the OPOC to reveal the registrant becomes an alternative means to getting to the data. And if we knew today what our access rules would be, perhaps that diminishes the need for a reveal responsibility.

So today we are working on parallel tracks and I still stand on this point that you really need to have an ability to get to the OPOC to the registrant in cases where the registrar doesn't even know the true registrant's information.

Dan Krimm: Okay, well the...

Philip Sheppard: Dan, I'll put you back at the end of this if I may. And David Maher is next on the list.

David Maher: Well, actually I'm not really echoing what Dan said. What has Dan all defer to use and he should answer that if you're correct.

Dan Krimm: (Unintelligible).

Philip Sheppard: Okay. The main muscle point to answer that's what I'm concern about then Steve Metalitz is next on the list.

Steve Metalitz: Yeah. I just wanted to point out there is one other difference between the Reveal Function and whatever gets worked out regarding access which were very far from being even having that in focus.

And that is that the Reveal Function is would - if you use that as someone who uses that has to be prepared for the likelihood or perhaps the certainty that the requester's identity or information will be revealed to the - be revealed turn as well.

That might not be the case in the access system. So for example, in situations where there's an ongoing investigation and there's a high value placed on not disclosing to the registrant that the investigation is going on, you probably wouldn't use the Reveal Function, you would probably have to use the access function.

But for the reasons that have already been stated that they are somewhat distinct and I thin k the scalability of this reveal based on three criteria that are listed in the draft report is a very important part of the OPOC function.

Philip Sheppard: Oki-dok to you, thanks. David Fares, you're next.

David Fares: I wanted to just to expound upon the point that Steve Del Bianco made. I also phrased what he said and what's David Metalitz has said. But Dan, you know, you mentioned that there was access provided by working group D.

But if we go back to the working group D's final report there was no agreement among the working group members that private parties would have access to WHOIS data. So we've got that big problem too over and above the point that Steve can – well both, Steve makes.

Philip Sheppard: Oki-dok. And then Dan back again to you.

Dan Krimm: All right. Let me respond to Steve first. He had two points, one about proxies not – or the registrar is not having registrant information when there is a proxy service.

But I don't think that maps cleanly on to the OPOC model at least as we had been chartered to describe that because under that kind of situation, the proxy becomes legally the registered name holder. And it captures all the liabilities of such.

So, you know, that's if we're - I don't think that really fits in well with what we're describing as the OPOC right now because the OPOC is being described in a situation where the registrar does have the registrant's information.

Secondly, if there are issues with, you know, not getting access and therefore wanting to have reveal, well that to me just speaks to the word loophole.

And what we ought to do is get the access' requirements in place so that everyone can agree on them in one place. And if we can't agree on it then and having a loophole to get around our disagreement doesn't seem to be a consensus position.

And speaking to the point about the lack of agreement coming out of the subgroup B, well, we still have some work to do. I think we can find agreement, gets everyone is exploring this idea in good faith within this working group.

But we may not be able to do it with the time frame left to us at this point when you'd have to simply to report it as unfinished business.

Philip Sheppard: Uh-huh. And Dan, what about the point made on the fact that the requester may not want their identity known and that Anonymity could be a point available to them under the access proposal…

Dan Krimm: Well, exactly that would seem to be something in favor of speaking towards going for the access model rather than the reveal model.

Philip Sheppard: Right.

Dan Krimm: Because that would protect certain requesters from having their own information revealed to a bad faith after a registrant. So that seems to point even further towards going to the access model.

Philip Sheppard: Right. So you're speaking in favor of an open access model, right?

Dan Krimm: I'm speaking in favor of an access model that covers all possible access to the hidden data and that is appropriately constructed so that the people who need the access have it on a timely basis. And those who don't or shouldn't have standing to have that hidden data should not get access to it

Philip Sheppard: Oki-dok.

Fabio Silva: This is Fabio Silva from Burberry. I just wanted to say that I totally agree with that.

David Fares: This is David. Can I jump in quickly (unintelligible)?

Philip Sheppard: I am taking new queues. That was Fabio, David Fares.

David Maher: David Maher.

Philip Sheppard: David Maher, any one else?

Jon Nevett: Jon Nevett.

Philip Sheppard: Jon Nevett, anyone else? Okay. Fabio have you finished or more to say?

Fabio Silva: Yeah, well I just wanted to - there was a point that was brought up earlier and I apologize that I didn't catch the name. But it was regarding investigations.

And I'm kicking myself for not having mentioned that earlier because that is extremely important to us. We often go to websites where we see offers for sale of counterfeit merchandise.

And in order to secure additional evidence aside from simply images of sales online, we do on some occasions send investigators in to meet with these individuals under cover.

And attempt to gauge how much of this merchandise these people have in what quantities they're selling it, whether they're actually describing it as Burberry, things like that.

And you really can't do that through a system where the individual who owns the site is basically being told that Burberry is looking for their information.

And tell me there should be some measures to make sure that only people with standing should make such request. And so only, you know, Burberry would be able to identify what on the site is infringing and has led to - has basically led us to request this information and that we feel that there is certainly something illegal going on here.

Thank you.

Philip Sheppard: Okay, David Fares.

David Fares: Just - I support both the reveal and the access function but if we were to consider what Dan is saying, we would need to have at the outset before we could even consider it, we would need to know which private party that seems to be getting access which is something that as I said we did not agree upon in working group B.

And Dan even in his comment said there would be some I think at the end there would be some restrictions on who would be able to do it. So we would really need that clarification from this group to determine whether or not there's consensus that all legitimate parties would be able to get access before we could even consider his proposal to do away with reveal.

Philip Sheppard: I'm doing it. I think for clarity probably it's worth saying that there were certainly discussion and disagreement as to whether or not both law

enforcement agencies and private parties needed to be authenticated in some way.

And there was no practical suggestion to date as to how either parties could be authenticated. And I think that's where we cut the hour on access and authentication.

So David Maher, you're next.

David Maher: Yeah, well, I agree that - I think I agree with Dan that there is no consensus here. And I see no reason for duplicating functions that reveal an access. Clearly, we're not going to have any agreement on that but we should - I think recognize there is no consensus. The need is to develop an access system and move on.

Philip Sheppard: Okay then David and what about the differences other speakers have described in the two functions. The one going by the OPOC, the other going directly to the registrar, one being potentially automatic based on navigations of bad faith, the other being possibly related to some sort of authentication barrier. What's your perspective on those?

David Maher: Well I think, it's again it depends on developing an access system which is what we have yet to do. I think the – an effective access system will resolve most of these concerns.

Philip Sheppard: Okay.

David Maher: But the problem is that I start with the fundamental principle that the personal privacy for individual data has to be respected and we will

develop an access system that starts with that fundamental principle and move from there.

Philip Sheppard: Yes. I think that's right and that is the starting principle. And – But the problem we're trying overcome is that of intentional inaccuracy and bad faith criminal activity.

David Maher: That's right. And that is why it is so difficult to develop the access mechanism where we have to sit down and in a constructive way decide how to do it.

Philip Sheppard: Oki-dok. Jon Nevett, you're next.

Jon Nevett: I'll pass.

Philip Sheppard: Okay. Just to jump for more, I have a question of you as a registrar. One question I'd ask earlier with the group was the differences in terms of scalability of these sort of requests going from a requester to an OPOC as opposed to having none of that for the function it does and everything going to the registrar. Do you see any issues with that?

Jon Nevett: What's that again? Because I didn't understand what you're…?

Philip Sheppard: Okay. The – at the moment we're discussing the possibility of a Reveal Function in terms of the normally restricted data and that entire mechanism will take place as a dialogue between the requester and the OPOC.

The alternative to that is that the OPOC has nothing to do with that at all and the requesters coming directly to the registrar each time they

want that reveal information. And my question is does it raise any issues of cost or time for the registrar?

Jon Nevett: Sure. If the registrar is not the OPOC in other words?

Philip Sheppard: Yes.

Jon Nevett: Yeah. I mean it's a manual process and you're looking at reason of the current version of the 3.2. You're looking at alleged inaccurate WHOIS data as one of the triggering events.

Philip Sheppard: Yes, for instance.

Jon Nevett: Yeah. And I'm - let's focus on the word alleged. So I know I could just allege inaccurate data and then there's a whole ICANN process on how registrars have to deal with alleged inaccurate data.

Dan Krimm: And Philip, this is Dan.

Philip Sheppard: Uh-huh. Okay and how does that process work (unintelligible)? Is it simple and cost effective or is it not?

Jon Nevett: No, it's a manual.

Philip Sheppard: Is it cost and time consuming.

Jon Nevett: It is a manual time consuming process that we don't get paid for.

Philip Sheppard: All right. Okay. I had Dan also wants to speak again. Who else? Hello. Dan you're off you go.

Dan Krimm: What we were talking about for the access function in subgroup B was something where all of the uncertainty in the manual stuff was essentially pre decided before it got to the registrar.

So the point was to remove that cost burden from the registrars and I think it's still possible to create a situation – a system that accomplishes that. So I don't think the cost issue was - should be a major concern here.

Philip Sheppard: Yes I mean what you're describing I think is what we're currently going to report is 6.3 regular access to numerous data records that are on displayed as opposed to 6.2 which was is one time access to a specific full data records that are on display.

Dan Krimm: Well it depends, are there were – various forms of access that would apply to different requesters of different standings but the point is that all that stuff is worked out before it gets to the registrar and becomes essentially an automated process, so registrar's just build a system to deliver it to the right port.

Philip Sheppard: Okay. John, any comment on that? Is that feasible?

Jon Nevett: No comment.

Philip Sheppard: Okay. Anybody else wants to talk on this topic? Still okay?

Steve Metalitz: This is Steve, could I get a new queue.

Philip Sheppard: Yup, absolutely Steve. Any one else? Nope. Steve off you go.

Steve Metalitz: Yeah, just to say that there's seem to be a fair amount of agreement that if the access system were constructed right it would address many though not all of the interested or addressed by the Reveal Function.

But I just think we have to face, you know, kind of take a snapshot of where we are and we don't - we are so far from having an agreement on the access function that I would that there could be some flexibility on the Reveal Function.

Philip Sheppard: Uh-huh.

Dan Krimm: Well, let me just respond to that. On the reveal - the problem with the Reveal Function is that it's also actually not very well specified at this point. And if we go into detail, we're going to end up with precisely the same standing issues that we're dealing with in terms of access.

And if we don't deal with them, then all we've got is pretty much a clear loophole that undermines the whole purpose of having an OPOC in the first place.

So if we're to just have a clear Reveal Function, you know, on demand then why have an OPOC in the first place?

Philip Sheppard: I mean actually that – to me that's also an interesting question because I think if we're saying we're going to did all right direct access to the registrar.

There's going to be no Reveal Function. There's going to be no - not going to be much of a remedy function as currently drafted. It does start to beg the question what on earth is an OPOC all about?

David Maher: Well, I don't know that there wouldn't be a remedy function. I mean the point of the OPOC is as I see it is (unintelligible)…

Philip Sheppard: Well, a remedy function that the - by remedy we mean a function that the OPOC would be the actual form not the registrar.

Dan Krimm: Well, that could be determined for that to be the case in certain circumstances I would think. I mean going to the OPOC to the registrant and I'm not sure where the registrant takes technical responsibility or the OPOC could do that as well depending on the contract.

There are minor remedies that are, you know, available if they choose to act on the information that comes to the OPOC and is relayed. And if somehow that process is breaking down, then there is the demo clean and sort of taking the domain off of the DNS and that is always available.

But, you know, I think this is a more constraint remedies are still made possible by having the OPOC. But if there is a need to actually get access to the hidden data then it should go through the access system such as we constructed.

Philip Sheppard: Okay, thanks Dan. Well, I think in some other thing where we are on this point. I think there is some agreement if the access proposals could be simple cost-effective and rapid.

Then they may fulfill most but not all of the functions we're currently talking about under reveal. And that was perhaps the biggest. There are, however, certain function that has revealed give such as ability to find out who the registrar – or (unintelligible) registrant is. Things like need to serve notice or on those engaged in criminal activity.

And there's also the potential cost issue of a manual process as opposed to an automated one. If this entire issue is – entire burden is shifted to the registrar responsibility as opposed to the responsibility of an agent of the registrant of OPOC.

And I will try to…

Dan Krimm: Just one more comment, Philip. I'm sorry.

Philip Sheppard: …review in the next version. Is that Dan again?

Dan Krimm: Yeah. I don't understand quite why the OPOC is not sufficient for serving notice because if the OPOC has a binding contract with the registrant and there is the ICANN policy can be safe to require that. Then the OPOC could essentially act as a legal representative of the registrant.

Philip Sheppard: Okay, I think there were two conditions in your sentence there, weren't there? You're saying if the OPOC has a binding contract, if ICANN can help to enforce that? And I think neither of those proposals are currently in our report.

Dan Krimm: Okay.

Philip Sheppard: And - so, let's (unintelligible) - then where we are for the moment and for that we say that the topic of authentication. Maria, where are we would start support?

Maria, are you there?

Maria Farrell: Sorry, yes I was coming off my silent mode. Excuse me.

Philip Sheppard: Oki-dok.

Maria Farrell: Okay, so you would ask for an update on the concepting that we have and commission from a US-based consultants with the security on enforcement and background.

It was - basically we engaged to the consultants to – and provide us with information on existing organizations in the US that are potentially capable and interested in providing accreditation or certification services for law enforcement agencies for accessing WHOIS data.

And first of all, we asked you about for an analysis of that on a national basis in the US. We've got – I've got some preliminary – basically a draft that I discussed to – do some light reviewing on to make sure it's formatted correctly.

And - so I just give you a verbal update of what we heard from the consultants. And here few is that – it's not and - I don't know if these to be feasible for – or he has not confident that there is no organization that can properly accredit law enforcement agency in the US alone, let alone internationally.

And he has – what is to me – he's such a – some criteria for actually how accreditation might work at least in a generic sense. And then he did look at the number of law enforcement agencies who are in the US and found it's close to about 20,000 organizations.

That's looking at everything really from, you know, from town-based law enforcement all the way up to state level. He then applied the criteria of how might accreditation work to around if you did our various organizations that are in the field of either recognizing on law enforcement agencies are particularly in sharing information.

So he's basically gone through various of those. And compiled information about them. And the broad filings are that he doesn't – the needs for the accreditation at the moment is going to be certainly very easy to do.

So I guess I can leave it at that, but I think I should have this report out to the group by tomorrow.

Philip Sheppard: Okay, that'll be interesting to see the whole report. So this – to be sure taken – that this is only related to law enforcement and only related to one country, the US.

And that even in a national confines, and even desolate as law enforcement, let alone in the private sector or the countries and it's his problems.

Maria Farrell: Yeah. That's very distinct and analysis. Yeah.

Philip Sheppard: Yup. Okay, interesting. Which is broadly, I think while being the top of the group. And it's currently reflected in a line well enough 476 in Sections 2.5 – I think 0.5 and I could there's needing access for calls indication.

And currently report is saying that there was discussion about boldly to mechanisms I mean, the access either a form of self declaration by the access of - that's the person demanding access.

And that could potentially be backed up by challenge to see divided registrar or the second a means of authentication or the access of by a third party.

I think in previous discussions, it would been agreed that use of Interpol to authenticate earlier is not a starter and use of various ways to authenticate the private sector were also rejected.

And so far, the report is saying there was no practical projection about how authentication may take place in the way that is scaled of a globally and proportionate to cost.

We just heard synopsis of the consultant's report looking at one specific of that which seems to say the same thing. And where we are now is further discussion of the group about authentication would be in the preferred mechanism.

So, I'd be very happy if there's anybody who has some very smart suggestions. I'll take a queue now.

Dan Krimm: This is Dan.

Philip Sheppard: We have Dan. Anyone else? Well, Dan you're on your own.

Dan Krimm: Well, I'm sorry that Pat Cain is not on the call today because he made a very interesting presentation in San Juan. And he suggested that the anti phising working group was actually working on an interesting method of potential authentication that might operate essentially on a private basis but I would assumed with some legal authorities. So…

Philip Sheppard: And that was authentication of alias or private sector or both?

Dan Krimm: I think possibly both.

Philip Sheppard: Okay.

Dan Krimm: He didn't specify in detail at that spectacular presentation. So, I don't have anymore detail than that. But I would be interested to hear from him or the anti phising working group generally after what they're coming up with this along those lines.

Philip Sheppard: Okay. Well, I mean - if there is a specific practical suggestion then I think I would urge you Dan to contact Pat and ask him to write that down in simple words and present to the group because we'd all be very happy to know about the practicality of the system.

And see if how we talked about a theoretical mechanism, we're struggling to look at the practicalities. So, any suggestions in that direction, it would be most welcome.

Dan Krimm: Right. And also I'm interested in hearing well as to report that we were able to weather still like tomorrow because until I understand how this consultant construed the criteria of authentication in the first place. It's hard for me to evaluate that result.

Philip Sheppard: Sure. I think I would encourage you already to make comment on the list about the report once you see it. So we can have that debate over the week and forward.

Anybody else want to say anything on this topic?

Oki-dok. Well, let me just talk briefly and about what work going forward. I think probably we may need another couple of calls at least to finish our work. And what will be useful I think at this stage is to go through the report.

Well, we'll issue a 1.5, following on today's discussions. And then we will then take that in chunks to assess while we have levels of agreement or disagreement.

And see if there is a need to change particular recommendations from saying agreed to support or even to alternative review so that then degrees of presenters on report are clear.

And I'll post an e-mail having spoken with Maria about the practical mechanisms of doing that with a reason we end the report for those numbers and suggestions.

Although I think probably we have been moving slowly to phrasing that is more or less accepted by many people. And we just need to validate to the next couple of weeks.

So that's certainly the idea of (unintelligible) going forward. I'm happy to take any questions on that.

(Unintelligible), well, then in record's time, at first, we bring this (quarter) close which will be a quick, as I believe to many people on this call I think who are aware there are other ICANN-related policy calls happening today and shortly. I give you some time to spend a little longer in our day job.

Thank you very much everybody.

Dan Krimm: Thanks Philip.

Man: And thank you.

Philip Sheppard: (Unintelligible) contacts next week.

((Crosstalk))

END