Registration Abuse Policies Working Group
TRANSCRIPTION
Monday 31 August at 14:00 UTC

Note: The following is the output of transcribing from an audio recording of the Registration Abuse Policies Working Group meeting on Monday 31 August 2009, at 14:00 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/gnso-rap-20090831.mp3
On page:
http://gnso.icann.org/calendar/#august

All recordings and transcriptions are posted on the GNSO calendar page:
http://gnso.icann.org/calendar/#august

Present for the teleconference:
Greg Aaron - Registry C. - Working Group Chair
James Bladel - Godaddy Registrar C.
George Kirikos - CBUC
Mike O'Connor - CBUC
Berry Cobb - CBUC
Faisal Shah - IPC
Rod Rasmussen – individual
Jeff Neuman - Registry constituency
Philip Corwin – CBUC
Richard Tindal - Registrar
Robert Hutchinson

ICANN Staff
Margie Milam
Marika Konings
Glen de Saint Géry - GNSO Secretariat
Gisella Gruber-White

Coordinator: Thank you for holding. I would like to inform all parties that the call is being recorded. Any objections to disconnect, thank you, you may begin.

Greg Aaron: Okay, wonderful. Let's begin with roll call please.

Gisella Gruber-White: Yes, good morning good afternoon to everyone on today's call we have Greg Aaron, Mikey O'Connor, Berry Cobb, George Kirikos, James Bladel, Jeff Neuman, Richard Tindal, Faisal Shah, Rod Rasmussen, and we have a Robert, apologies I didn't get the surname.

Robert? I'll get on, with staff we have Marika Konings, Margie Milam, Glen DeSaintgery and myself Gisella Gruber-White and as I said there's a Robert who's joined the call but I don't have his surname.

Robert Hutchinson: Hutchinson.

Gisella Gruber-White: Hutchinson, thank you.

Greg Aaron: Bob Hutchinson. Okay. All right, and a few of you are on the phone but not on meeting view, if you can log into meeting view from your location that would be great but it's not required.

As always want the transcripts to accurately reflect who's been speaking so if you're not recognized by name please identify yourself when you begin speaking.

So thanks for joining us here at the end of the summer. What we're going to do today is a brief run down of the work that our subgroups are doing and then we're going to launch into new topics, specifically spam and phishing and malware.

Let me ask just briefly if there's any other business? Hearing none let's go ahead and with our cyber squatting group, their action item was to be working on the Wiki and tell us about the DPA.

Has there been any progress in that group over the last two weeks?

James Bladel: This is James, I'm trying to think if there's anyone else from that group on the call.

Greg Aaron: I don't believe so.

James Bladel: Okay, I end up being the de facto spokesperson regardless, but yes, it seems like we have had some exchanges on the list.

I'm not sure if Mr. Rodenbaugh has submitted that to the Wiki yet but I think we have arrived at a definition of cyber squatting that is mostly comprised of the definition that is contained within the UDRP.

There are a couple of other elements that were borrowed from the ATPA that are fairly non-contentious elements in that they are already either considered as part of UDRP proceedings or like one, having intentionally fraudulent or incomplete WHOIS information is grounds for suspension.

I think that's fairly universally understood. So I will try to get that posted to the Wiki if it has not already been done by Mike.

Mike O'Connor: James I'm - this is Mikey, I'm looking at the Wiki and there is quite a bit of stuff out there, maybe it made it.

James Bladel: Okay, and was it recent as of let's say last Wednesday and Thursday?

George Kirikos: Posted it August 17, George speaking.

James Bladel: Thanks George, yes I can't tell.

George Kirikos: You click on revision, compare revisions.

Marika Konings: Yes, because this is Marika, I checked today and I didn't see anything change from the previous version we looked at. I can pull it up if people want to use Adobe Connect.

James Bladel: I tell you what, I will reach out to Mr. Rodenbaugh here today and we will get this added to the Wiki as quickly as possible.

George Kirikos: This is George, I have to raise the same objections as last time that unless it's changed dramatically from what's on the Wiki right now, you know broad end of the definition cyber squatting, way too much. You know several here would be considered cyber squatters under that definition.

Which isn't the definition of law.

James Bladel: Yes, and I have them both in front of me George, this is James again, sorry. Not having both in front of me I can't really tell the difference. I had a lot of those concerns going into this subject George.

But from what I can tell we have essentially taken the UDRP definition as it currently reads and added a section to maintaining accurate and complete WHOIS.

George Kirikos: Okay, I'd have to see it to be able to comment.

James Bladel: Yes, so I don't want to speak out of school here because I don't have those in front of me, but when we post it if you could please just take a look and then if you still have those concerns or if there are still gaps in the definition, if you could raise that on the list it would be great.

Because I think you and I spoke and I have a lot of the same concerns.

George Kirikos: Okay.

Greg Aaron: Okay, so it sounds like we need to review what's on that Wiki and make sure we understand what the latest is and then we can have some further discussion about whether that needs modification.

James Bladel: Yes, and Greg, this is James again I just want to extend to the group my apologies, I wasn't aware that I was going to be the only member of that group on this call.

I certainly played a peripheral role in developing the definition so I apologize that I'm not prepared to speak to it.

Greg Aaron: Well okay, appreciate it but hardly any apologies necessary.

James Bladel: I didn't want there to be silence, so.

Greg Aaron: Okay, well anything else on cyber squatting then? Sounds like we have some action items to work.

George Kirikos: George here, just a boarder question. Are the people listed on the Wiki still all members of the working group? Because I noticed a lot of people haven't shown up for several meetings in a row.

Are they still engaged?

Greg Aaron: They - well let's see, sporadically. I mean there are - the GNSO has no requirements for membership, put it that way. No one has indicated they have dropped out amongst that list of folks.

Okay, next on the list then is uniformity and contracts. And Berry is helping lead that process, so I'd like to turn the floor over to him.

Berry Cobb: Hi, good morning this is Berry. My apologies, I'm driving right now so hopefully this will still come in clear, but I'll be pretty brief.

We met again last week. We completed our second run of our research trying to build the picture of dispersion across contracts. We reviewed through the data, basically what we're going to say is the picture is starting to emerge.

Certainly not formal yet and for the most part there are a couple more questions and several decisions that need to be made about what to do with the data, how to clean it up a little bit more.

And certainly what our actions are going to be after we've made some of those initial decisions about the research. So the team is - we're still moving forward with our work.

I think it's still a good effort overall across the teams and we're going to meet again next week at the regularly scheduled time. I'll be sending out a doodle to get a schedule set up.

And that's really about the only update we have and James and Mikey you're welcome to add to that as well. Thank you.

James Bladel: This is James, I think that's a very concise and comprehensive synopsis.

Mike O'Connor: Yes, Mikey here, same. We are very engaged but we need to polish off some things before we come back to the group with our results so same here, Berry did a great job summarizing and he's also doing a great job being our leader.

Greg Aaron: Okay, excellent. This is Greg, so as our next conference call, do you think your group will be ready to present you know a significant overview of what you propose and the questions that you've come up with and so forth?

It's - we're probably coming up on the time when we need to tell the group in more depth exactly what's going on and allow them to understand the shape of your project.

Berry Cobb: This is Berry, I would like to say yes, but I think there's some pretty hard core decisions that we need to make as a group first before I commit to anything.

There - that's about all I can say. I would like to say yes, but I can't guarantee that we'll be able to share information by the next meeting or not.

Certainly between now and our next sub team meeting we will be trying to get together offline to wrestle some of the bigger decisions.

But I believe it's going to require us another group to call to actually iron out some of these decisions before we can move forward.

Greg Aaron: At this point what are some of those decisions that you're wrestling with?

Berry Cobb: The data itself, it touches on you know comparisons across the industry so we need to make decisions about how that data should be shared, should we slow it down to an anonymous form?

There's data that's collected that is beyond the scope of the registration abuse - or sorry the uniform media contracts sub team and the registration abuse teams for that matter as well.

So probably need to trend some of that out there as well but it was necessary in terms of kind of creating an inventory so to speak. So those are the main decisions that need to be made before we can share the information.

I guess somewhat of a small preview about the picture that is emerging from - about dispersion is that at least I think that it's kind of coming in line with what I anticipated.

At the top tier we see a lot more uniformity, in the middle and lower tiers the dispersion seems to increase.

But that's my interpretation of the data, that's not a collective group's - I'm at a loss for words. We as a team haven't collectively come up with what that - what the actual results would be yet.

So it's still up for interpretation.

Greg Aaron: Okay. All right, go ahead Mikey.

Mike O'Connor: Just to elaborate a little bit, we are actually engaged in a very tasty conversation about a number of facets of this. And the reason we're dancing around it is because we had a really productive call last time and at the end of the call we all sort of came away saying wow, we've got some pretty substantive issues that we need to think about.

And the reason we're dancing a bit is because the way the data looks right now it's probably not prudent to release it in the wild for several reasons.

We need to sort of digest all that one more time, so Berry is correct in being very cautious about whether we're going to be ready for the public unveiling at the next full working group call.

I would second that, we may be ready but I wouldn't want to take us into the agenda with a hard commit right now because it's - we've just got a lot of stuff to work through yet.

Greg Aaron: Okay. When I guess - this is Greg, I guess my suggestion is once you guys have kind of talked about it internally and come up with a recommendation, then when you're ready to present this to the larger group we'll need kind of a summary of the big issues that you guys wrestled with.

Berry Cobb: This is Berry, absolutely.

Greg Aaron: Why you're recommending - I'm sorry, and why you're recommending what you're recommending. So we all understand kind of the major issues and potential pitfalls, etcetera.

Berry Cobb: Yes, this is Berry, we'll absolutely be - you know one of the deliverables about it is to create a summary presentation and talk about the findings. And I just want to make it clear that we haven't even started down the road of developing any recommendations or thoughts about what actions should we take relative to the topic of uniformity.

We are strictly still at the data level and the research mode. I don't think we've even remotely talked - the only question that's come up so far relative to any kind of recommendation is that is it important for us to be uniform or not?

Or should a minimum baseline be set? And outside of that we hadn't even started going down the road of details about formulating any recommendations or anything like that.

Greg Aaron: Oh Berry, that was my impression as well. When I was talking about recommendations, I wasn't talking so much about policy recommendations or anything like that.

I was talking more about your recommendations for how the research should be conducted (unintelligible). Okay, no problem. Okay, any other thoughts on that work under the way?

Don't see any hands, so it sounds like you know you guys are making some good progress. Thanks again for your diligence on this and the meetings that you've been having, much appreciated.

Good to see work progressing so nicely on this. Okay, nothing else on that topic we move on to malware and dot net control that's Rod and myself.

I've been working a little bit on the Wiki on and off. We're not at a point where we have any recommendations like that either. Rod, do you have anything to add right now?

Rod Rasmussen: Yes, I put in a little time on that too and just tried to work on some definitional stuff to differentiate between the time control rendezvous things and the top - the next area of topics which are more of you know large ones I think, at least large scale registrations of domain names in order to support malware drops and things like that.

So, kind of tried to separate the issues --that's about it. It's been updated on the Wiki as well.

Greg Aaron: Okay, so some progress there. Any questions on this topic from anybody? Okay. Not seeing any hands next is front running. And George is point on this topic, so George over to you.

George Kirikos: George here, well we had a good discussion last time, we have some people here today that weren't here last time so maybe they have a chance to discuss basically since last call we've had the question answered by the - Ben Edelman with response to some of the topics that were raised on the mailing list.

And some additional questions were asked but we haven't received responses from those at least yet.

I did update the Wiki to reflect the conversation during the last conference call and our discussion up until last night, so I guess I'll look to the group to see where we want to go from here.

Greg Aaron: I see Marika's hand.

Marika Konings: Yes, I just wanted you to know that the follow up questions that were sent in following the feedback received from Ben Edelman were forwarded to him and I hope to get some further feedback from him again shortly.

And as soon as I do I'll of course post that to the main menu.

Greg Aaron: Thank you. Okay, so George anything else you'd like to report so far?

George Kirikos: I did add a section on - let me send a link to the page to the chat room. I did add a section about who is harmed by Front Running, that's a topic that Greg raised during the last call.

And I did add a section about the card hold that James Bladel had raised last time. And other thank that do folks prefer that people start going over the you know issue of background recommendations level consensus now or do we wait till we make our first pass through all the topics?

And then make like a second pass later? Or I'm not sure on the process what should be done on the Wiki as opposed to waiting for further discussion amongst the group.

Greg Aaron: Okay, James has raised his hand.

James Bladel: Yes, this is James and question for George, Greg and the rest of the group. I mean based on all the information that we have collected, and in light of you know some of the quantified reports, I mean do we still believe that this is an actual documentable abuse?

What I mean by that is that you know this is - I kind of - I was joking a little bit with George that this is kind of like the Loch Ness monster of abuse types, as everyone is convinced that it's happening but yet no one can really demonstrate that it is.

And then as a registrar I mean it's one of those things that we're convinced that all the other registrars are doing it but we know that we're not.

And I think that if you ask all the other registrars they'll answer similarly. So I guess I am still skeptical that this is happening.

On a wide scale basis. I understand we've got some isolated cases with malware, we had some different service attempts that kind of went off the rails and treaded into this.

But in conjunction with the modified policy relative to the ADP, it's just - I'm still not convinced that this exists. And if I'm premature in saying that Greg I apologize.

Greg Aaron: I raised my own hand, this is Greg. I guess factually it would be safe to say that front running has happened in the past because it was documented with the network solutions thing.

The new add grace period limits policy has certainly changed the landscape of what's happened.

And it would make probably certain kinds of front running no longer palatable or profitable perhaps. It's unclear at this point whether it's actually happening or not.

I mean I - and I say that because I haven't seen any documentation that would demonstrate real front running. I think the Edelman report, I think there's some questions that I have about methodology used there.

So we're waiting for some replies. I guess maybe one question is, is it - despite whether we've seen any attempts recently or not is it still an abuse that we should be concerned about?

So James you raised your hand.

James Bladel: Well I think that's exactly right. I mean if it is a theoretical abuse or a vulnerability let's say that has not been exploited successfully since you know we can point to a few isolated incidents.

And I think that if we had representatives from those folks here they would say that they were using a technique to combat tasting that looked like abuse, right?

So I think there's more complexity even to the example that we pointed to as you know instances that this does exist.

I just want to make sure that we're not spending a whole lot of time and resources on you know something that isn't quantified as something that is definitely occurring, something that is definitely causing harm.

Again I think it's something that is plausible, but I just - you know I think that you know the Hippocratic oath of policy development is make sure that you're first not hurting something.

And if this is a wild goose chase I just want to make sure that we're focusing our time and efforts on the things that are definitely occurring and causing harm today.

Greg Aaron: Okay. Oh by the way, this is Greg, I think we had an interruption in the Adobe Connect, at least I did so I can't manipulate it right now, is anybody else having any trouble?

George Kirikos: Looks fine here, George here.

Mike O'Connor: Yes, Mikey here it's okay for me.

Greg Aaron: Okay, maybe it's just my connection. Okay, so I saw James's hand and then Mikey had raised his hand. Want to go ahead Mikey?

Mike O'Connor: Yes, I want to lobby for the sort of a middle position. I'm not quite ready to give this one up yet, partly because of the methods and that's why I stuck my hand up and then took it down.

Sort of to amplify your point Greg that there are concerns at least in my mind about the methodology in the Edelman report.

I'd like to see more of how that was done and I'm not sure that - you know we're sort of in a prove the negative problem.

But I think that the other way to run at this is to acknowledge that it is indeed a vulnerability.

There's certainly lots of anecdotal evidence floating around out on the net, folks who have run into this.

And so you know I'm not adamant, but I do think that this is worthy of more work before we let it go.

Greg Aaron: Okay. I see Jeff Neuman's hand.

Jeff Neuman: Hello, this is Jeff. Just a question, so the way the definition is in the chart is a lot more narrow than the way it is reflected in the conversations that we've had. And I think George accurately reflected the transcripts of what we've been talking about.

And I apologize for missing the last call but so the question I have is are we talking specifically about front running by registrar when a registrant checks the availability of a name?

Or when you guys are talking about is there really an issue, all the other things that are brought up in this document, things about use of traffic data and others and traffic data would refer to an unregistered name.

I'm just - I mean George has documented everything, I just want to make sure we are clear on what specifically we are talking about.

Because I see there are, you know, three or four or even more issues in the transcripts.

Greg Aaron: Okay, George?

George Kirikos: George here. Looking at the document it seems to be the same as the original definitions back when this document was first produced, March or June or whatever.

So it doesn't reflect the latest definitions which was basically taken from the SSAC report.

So I'm not sure whether we should be limiting it to just that or whether it's to be limited to the broader issues that were raised in this working group and also in the past research.

Jeff Neuman: Right, so this is Jeff again. So then we need to make decisions on - and I'm not saying one way or the other at this point, well you know my view on using traffic data for unregistered names. I don't think that that's an issue we should focus on.

But I mean I do think as a group we need to decide what we are and what we're not focusing and what we are and are not calling front running.

George Kirikos: George here, I agree and just to back to the past discussion by James and Mikey Greg, I think empirically and statistically we don't have a large amount of front running taking place right now despite the research and anecdotes.

I think the scale has fallen due to the AGP limit rule. But I don't know whether we want to consider that independently or not because those AGP limits ever changed then you suddenly bring up the topic of front running again in the future.

I don't know whether people want to be preemptive about discussing the theoretical attacks that are possible.

Because right now I don't consider the theoretical attacks to be mostly by the registrars any more, it's probably at the registry level. And if it's for registrars it's probably for sunrise periods and land rushes, not for like mature TLDs like dot com.

And so if the policies are to be preemptive they should you know take into account some of the possible recommendations that I made which are things like a better education and disclosures and you know providing - having the registries produce lists of all registered domains which allows more you know paranoid local domain checking instead of querying the registry.

So that you know at least allows people to thwart the possible use of data by the registry since they won't have it to begin with.

And the last part I guess about traffic data is something that obviously the registry constituency might have problems with.

Greg Aaron: Well who's - George, this is Greg, who is harmed by front running?

George Kirikos: Well I added that fact in, it would be a guess. Lower cost registrars because if higher cost registrars are doing things like card holds then that allows the - that prevents comparison shopping.

So it means that my name is stuck at for example Network Solutions at $35 a year instead of GoDaddy at $7 a year if the card hold is put on by a higher cost registrar.

Also there are registrants that are harmed if a name is held back from the pool of available names for some temporary period.

And I guess more generally it’s people that create new ideas for a domain name and have their name supposedly taken by somebody else.

The question is whether that - they had a real right to that domain name in the first place. So to the extent that that domain name was novel they might consider that you know they had a presumptive right to it for a few seconds.

Greg Aaron: My recollection of the SSAC report was that they focused on front running by registrars because there was basically an expectation of trust between the two parties.

You were basically trusting the registrar not to take the domain that you were inquiring about or interested in basically or have somebody else take it based upon your interaction with the registrar.

So it’s that one way of focusing on the issue?

George Kirikos: It’s not necessarily just the registrars because the act of checking leads information to multiple third parties, either the registry, also the - you know all the name spinning tools and analytics checking like Google Analytics, you know Omniture, all the other potential areas that the name could be exposed to if registrars aren't designing front end properly to minimize that information leakage.

So the registrars are typically the front end to it but other people do have access to the data including the registries and I guess I think when we regulate the registrars and registries there's only two targets of any policy.

Jeff Neuman: Right, but that's where the problem lies right, because - sorry this is Jeff, the problem is that registries have even less data then ISPs have on unregistered names.

And if you're only going to regulate the registries and registrars simply because that's who we have contacts with then that kind of makes you know you're basically unfairly targeting one sort of group just because you can.

And really most of the problem with unregistered names, I won't even say it's a problem, but most of the monitoring of unregistered names actually happens at an ISP level.

George Kirikos: George here, well you're taking one view of what that insider information is, that the information is the DNS check, the you know traffic hitting the zone file or hitting the TLDs root operators or the - not the root operators, but the TLD operator's name servers or the ISP name servers.

But there could be other data. Like for example if I did a registration of example.bus and you (star) figure that's a great name, and the (all star) or the manager for dot shop, they might register example dot shop preemptively.

That could be like a form of you know correlated front running but you know 30% of people might you know also want the dot shop so they'll grab it instantaneously or you know they might raise the price of that domain name.

Noticing the increased demand for that string, so that's a kind of thing that they're probably not doing, not investigative enough to be doing it.

But we have to just decide as a group whether we want to have a policy to preemptively prevent that.

Mike O'Connor: This is Mikey. It just seems to me that we're not quite ready to drop this one yet. I think at a minimum what we would want to do is have this conversation documented in our final report a little bit more than it is right now.

And I guess that's where I'm at is I'm just not quite ready to let this one go.

Greg Aaron: I see James' hand.

James Bladel: Mikey, understand that position but I would also say that prior to sending this as a part of that documentation of this conversation I just want to make sure that when we send this on to potential future work at policy development, I mean in order to correct this issue or to offer remedies, we need to really understand where it's happening, how it's happening and the mechanics of you know front running.

And I think that in the absence of that we're probably doing a lot more harm than good.

Mike O'Connor: This is Mikey again, I agree with that wholeheartedly. I am very uncomfortable with the data that we're working on right now.

It seems thin to me.

Greg Aaron: Okay. This is Greg, well - I'm sorry, Jeff do you want to go ahead?

Jeff Neuman: Yes, and I just again I just - if this issue does make its way into our report, I still don't like the issue of traffic to be grouped in with front running.

Because I don't see it fitting into the definition. If you want to call it out as something separate we can discuss that, but I just don't like calling that front running, I don't think it meets the definition that the SSAC actually set forth.

And I think it's a negative - it's an automatic negative connotation on that activity.

Greg Aaron: Okay. One of the places that the work can take place on is the Wiki. George has filled in the template with some material and summaries of previous conversations.

My question to the group is does somebody want to also start adding or editing the Wiki as a way of moving the work forward?

If the Wiki - because then anybody can work on it. So if you want to have a view point crystallized I think that's one of the places we can do it, but then it's in writing, people can absorb it.

And we have material for the report. So I'm just going to throw this out there, if you feel strongly one way or the other or think that there's something that needs to be reflected in the report, then that's a place to put it. George?

George Kirikos: George here, or people can send this to the mailing list because I've been collating all the views so those aren't just my own views on the mailing list, I link to the original mailing list discussions or link to the transcripts where possible.

So if people just you know - people have raised it on this call for example I would reflect it in the next version of the Wiki.

Mike O'Connor: This is Mikey, part of the problem that I'm facing is just the end data, and I really don't know how to solve that problem.

George Kirikos: George here, I agree that empirically it's more of a theoretical attack so in terms of prioritizing the work, it might be you know giving it you know more than a proportionate amount of time given the current level of abuse.

But I thought I'd say that you know it wouldn't be higher in the future, so based as a group people need to decide whether they want to make it a priority or not.

Greg Aaron: Okay. All right, any other thoughts on this topic? And I'm wondering if we can take it - take some work to the Wiki and move on to new topics today.

Jeff Neuman: So Greg, this is Jeff, sorry. How do we update the Wiki then so my comment saying that we should take the whole subject of traffic out of the concept of front running, how do I reflect that in - other than making the comment in the document, how do you actually end up doing something like that?

Because that's...

Greg Aaron: Okay, what George has done on this Wiki is he's got different subject headers which kind of summarize points that have been discussed. I suppose once - if there's not a subject header that addresses your issue I suppose one thing to do would be to create one.

George Kirikos: George here, I think go into...

Greg Aaron: I'm sorry, or provide a proposed alternate scope or definition in the - near the top in the references section. Go ahead George.

George Kirikos: I was going to say that we're going to add more points under the definition section.

Like right now I have three points under definitions of front running, if one wants to you know refine what the definition of that insider information is, that's a possible route. I was going to add it anyway based on the transcript of this call, so (unintelligible) directly. He just needs to log into the Wiki, I think anybody that's logged in can edit.

Jeff Neuman: Yes, and this is Jeff, I mean I think about doing that. Again this is all under the topic of domain front running, so I mean I guess I'm just thinking logistically here, I don't have a problem with the definition that's in the chart.

Maybe it is the definition of insider information, but I mean it would be its own - it would be a topic unto itself, use of traffic data.

Mike O'Connor: This is Mikey. One approach to this might be to start a section on the Wiki that just talks about definition and scope or scope of the definition, something like that.

And lay in the universe of possible things to be included in the definition and then group them as to ones that we're going to consider and ones that we're not or something like that.

George Kirikos: George here, actually if you people scroll down on that page on the front running in the Wiki, it actually has a section already, is traffic data for unregistered names in scope?

No, and then has a section from Jeff Neuman, Yes, and then it has a section from Roland Perry. I think we have covered it in the actual Wiki, not the...

Mike O'Connor: This is Mikey, that goes on the never mind.

George Kirikos: So there it is.

Mike O'Connor: Sorry.

Greg Aaron: Okay. So everybody good on working on the Wiki?

Richard Tindal: Yes, this is Richard, I just wanted to make a quick comment.

Greg Aaron: Please.

Richard Tindal: Yes, I've got to agree with Jeff. I think that just sort of in a blanket way suggesting that registries or registrars collecting information about their customers is inherently a bad thing.

I don't endorse that viewpoint. I think that if they're collecting information and using it in inappropriate or harmful ways then I think maybe that finds it's way into our scope.

But just a general approach that anyone collecting any sort of data about their customers is bad, I don't support that viewpoint.

Greg Aaron: Okay. Anyone else? Last call for last comments on this topic and then we're going to move on to new business. I'm not seeing anyone's hand raised.

Action items is for folks to work on this front running Wiki and it will come up for discussion in future meetings of course.

Okay, I see Richard's hand then George's hand.

Richard Tindal: That was from before for me.

George Kirikos: This is George, I just wanted to say that if people are adding to the Wiki please be careful about deleting existing text. It's good to just add paragraphs but not to delete any of the existing material.

That makes it easier to track changes.

Greg Aaron: Yes, okay good. Okay. All right, so if we're good there, we should move on to our next topics and open up the issues of basically spam, phishing and malware.

I saw a note from Gisella about a meeting for that group which was tentatively schedule for Wednesday, is that correct?

Gisella Gruber-White: That's correct.

Greg Aaron: The - I was on vacation so not checking my email very much last week. I'm a subject expert in these areas so I'd like to be involved. The only problem is I have a management retreat on Wednesday, I wouldn't be able to join the meeting.

Mike O'Connor: This is Mikey. I have a newly refurbished boat and that particular day would be perfect for testing it so I would lobby for rescheduling that meeting.

Richard Tindal: I would like to go on that boat.

Mike O'Connor: Anybody is welcome.

Marika Konings: We can set up a new doodle to find a time maybe later this week or beginning of next week?

Greg Aaron: Yes, I don't want to inconvenience anyone but it's a topic I do a lot of work on professionally.

Marika Konings: But I think James were you on that group as well? Do we need to check who signed up so to make sure to inform people and we'll send out a new doodle then to find a time for that group.

James Bladel: Yes, I don't think I was on that one. Certainly possible that I'm misremembering it.

Greg Aaron: Okay. Gisella would you be able to put on a new doodle on that one? And - well and one of the - we haven't gotten any...

Gisella Gruber-White: Sorry about that, I've just come on the call, I was on mute.

Greg Aaron: Yes, one of the questions is whether we - can you go ahead and do a doodle to reschedule that meeting? I guess actually we have not really approached these topics formally yet.

So we're all I assume pretty familiar with spam and phishing and malware, but just to run over the definitions very briefly, spam is traditionally defined as bulk unsolicited email...

Gisella Gruber-White: (Speaking in a foreign language).

Greg Aaron: Phishing is something I hope everyone's familiar with, but it's an attempt to collect a person's personal information, especially credit card or bank information by putting up a website which purports to be something other than what it is.

Usually those sites mimic banks, loaning websites or financial services. Malware is pretty big topic but basically it's distributing harmful code without the recipient being aware of it and that code can do many, many different kinds of things.

It can rope people's computers into a bot net, it can steal personal information. It can take control of (unintelligible) and have them execute actions without the user's knowledge and many other things.

So the very first question is are the - what are the scope issues associated with these topics? I'll throw one out which is these are activities that malicious parties do after they've registered a domain name.

So one question I have is are they in scope for policy making at all? I'll throw that out there. I see James and Mikey, so James you want to go first?

James Bladel: Actually the order is reversed, Mikey was in the queue.

Greg Aaron: Oh sorry, go ahead Mikey.

Mike O'Connor: This is Mikey. I share that scope concern. I think that to the extent that domain names is - you know once we're out of the registration of a domain name period I think the activity falls out of scope.

And so much like the bot net discussion maybe if there are activities that happen during the registration cycle, I think those are in scope.

But the activities themselves mostly happen independently of registration and I would report the view that they're outside the scope of this group.

Greg Aaron: Oops, okay, thank you. I guess James was next.

James Bladel: Yes, I wanted to echo a lot of what Mikey said and even to take us back to our workshop in Sydney where we discussed some of the aspects of intent.

And I think that what we would need to do, we need to bear in mind what while no one is certainly taking the position that we should do nothing, to address these issues, they are problems, they are harming folks.

But anything that would be right for ICANN policy development would have to be able to discern at time of registration which domains were registered for the purposes of spam, phishing and bot nets and malware and which ones were not.

And I think I have yet to be convinced that that is even possible. So I think that once we get into use, you know as Mikey said we certainly can have some different collaborative approaches.

There are a lot of cross - I want to say cross stakeholder efforts underway right now that include registries, registrars, security groups, IP concerns.

And all these folks are working very, very hard on these issues. But I think that trying to address them or come up with remedies within the context of policy making requires us to be able to tell in advance what the domain will be used for.

So I just wanted to get that out on the record and echo a lot of what Mikey said.

Greg Aaron: Okay. I think next was George?

George Kirikos: Yes, I just wanted to agree with the former speaker that I don't think it's in scope. I'll be brief that way.

Greg Aaron: Okay. Anyone else like to chime in?

Rod Rasmussen: This is Rod, I'm not on Adobe Connect at the moment. If any of you have a Mac and are updating the snow leopard, it has a lot of surprises at the end if you've got a lot of mail in your mailbox, so just a word to the wise.

The - have to disagree a bit with some of my colleagues there. I can tell when some of these - some domains are going to be used for phishing, malware, etcetera before they actually get used and then during the registration process based on who's registering them and how they are registering them and name servers they're using, things like that.

So it's certainly possible to know that yes, these are being registered by criminals. They're usually doing a large swaths, they usually do them - or they can do them either one of two ways, with cooperation or semi-cooperation of a registrar agent, typically a reseller.

Or using stolen credentials, so that is a registration process abuse I would say if you're using - at least you're using stolen credentials is abusing registration process.

So I think parts of this are definitely in scope, at least for discussion purposes.

Greg Aaron: Okay, thank you. I see George's hand raised.

George Kirikos: I think the topic of minority report and pre-crime was brought up on past calls. In fact this is an example if you can read the minds of people and know what they're going to do with a domain name before they register it, that's pretty amazing.

Well statistically you can do it but I think you can't do it with 100% error free operation, so that's something I just wanted to toss out there.

Greg Aaron: And I suggest that 99.99999% is pretty close.

Mike O'Connor: Yes, this is Mikey, I'd like to chime in supporting Rod on this one. I want to make the distinction between kinds of behavior that Rod's describing and the broader what I think is out of scope.

And George I think you're hitting on it too, we can figure out a reliable way, 99 point - and some sort of mechanism remedies mistakes. I think that that is important.

Greg Aaron: Okay. I still see George's and James hands raised, are those new or old?

James Bladel: This is new and just wanted to say that Rod I think that we can come up with a very good indication of how a domain will be used but we can never know specifically because that implies future intent.

And I think that you know this goes to drawing a line between policy development and work in terms of security practices, security efforts, monitoring and suspension and take down and all those other activities that we all know that we work very hard on.

But to address those things, when we actually get into trying to predict and intercept those registrations ahead of time. I think that becomes a little bit more of a challenge.

Greg Aaron: Okay. I see George's hand raised.

George Kirikos: Yes, what I see is it's really an attempt to mix together ex ante and ex post. Personally I'm not against any policy that strengthens registration, you know forcing people to better prove their credentials, etcetera because I think ex ante that reduces the amount of abuse.

But I don't like to see rules in place that people could point to ex post saying you know this was a registration abuse when it wasn't because they'll be able to look at you know future behavior.

And then at a future date say oh ex ante, we knew that that was an abuse and so you know you're an abuser, blah, blah, blah. You know you copied the policy.

Whereas it really should be directed to the law enforcement or other mechanisms, you know civil law suits etcetera instead of being done at the registry level.

Because people could say for example you know I knew you were going to use that domain example.com to infringe upon you know the trademark of example.

That doesn't go into bot net but you know this ex ante versus ex post, you can't just you know mix them up and you know wave your hand magically to call something an abuse.

I think that will tend to be abused by the people. And actually if people are going to be 99.9% accurate there should be severe penalties when they're wrong and if people actually are as accurate as they claim to be, you know they would be able to have insurance policies which are very, very expensive.

But I think in reality there are insurance policies that could be really high because of the rate of false positives would be higher than they say they are.

Greg Aaron: Okay. Mike O'Connor?

Mike O'Connor: Yes, this is Mikey. I actually think this is a very full discussion and I agree with all of it. Ron I think that to the extent that there are mechanisms that can come up with 59 reliability in predicting abuse, those would be (unintelligible).

But I also agree with George and James on (unintelligible). So I'm thinking that this is a useful conversation that needs to be continued, not simply parked as out of scope.

The piece that's in scope (unintelligible).

Greg Aaron: This is Greg, so which part might be in scope?

Mike O'Connor: This is Mikey again, the part that covered by an extremely accurate prediction of intent. So you know the issue that James and Richard raised that possible, I think that if the answer is yes it is, high accuracy and reliability, that those are in scope.

That is (unintelligible) rather than domain name broader category.

Greg Aaron: Mikey, you're fading in and out a little bit.

Mike O'Connor: Man, all the good stuff fades out, let me try that again.

Greg Aaron: I lost the last sentence there.

Mike O'Connor: So the broader - I think that the sort of Damocles on this for me is, is it abuse at registration time or is it abuse later, i.e. domain name abuse?

I think domain name abuse is outside our scope. But if there's an ability to accurately predict or accurately assess that the registration process is where the abuse is occurring, that that is in scope for us.

And you know I guess the hard part is this accurate prediction, because I agree with George that you know if we have a lot of false positives then that's not helpful at all for the community.

Greg Aaron: Okay.

Rod Rasmussen: This is Rod, I'd like to point out that registries and registrars are already doing this and it's just not on any kind of formal and controlled basis I would say.

I know for a fact that many registries and registrars delete massive numbers of domain registrations that have never been used for phishing, malware etcetera when they discover that the person or organization or what have you that has registered them is actually using at least in part some of their domains for those purposes.

So it's already being done. I guess one of the things we need to consider is whether or not we want to codify how that gets done across the entire spectrum of you know ICANN regulated registrars, or ICANN involved registrars, I guess ICANN isn't a regulator.

But you know it is being done already as a matter of business practice.

Greg Aaron: This is Greg, and although Rod, is that being done because those registrants have already broken terms of service by using their domain names?

Rod Rasmussen: Most likely.

Greg Aaron: In other words have these registrars and registries sometimes identify bad actors.

Rod Rasmussen: Yes. And then as new registrations come in from those registrants, whether it's the registrant or the configuration of how they're setting up their domain registrations at the time they're trying to register them, they are immediately suspended or deleted or blocked.

Greg Aaron: Okay. I see James' hand raised.

James Bladel: Yes, and I think you're absolutely right Rod and you know I'll say for the record we are very aggressive at rooting out this type of abuse. But I think that it is important that we recognize that ICANN Policy will inject uniformity into an area where I think flexibility is often required.

It will tie - possibly tie the hands of registries and registrars and reduce or limit their options as far as how they can or cannot act in those situations.

And it will impede a different data collection efforts that will help us uncover new types of abuses before they can be fully understood and how it would be developed against those.

So I really feel that it's important that we keep some degree of latitude in the registry and registrar's ability to monitor, track and interdict these types of abuses that is not necessarily the most - or more appropriately done ICANN policy.

Greg Aaron: I certainly agree with that, I think that that is part of what the discussion should involve is that you're probably going into an area where you'd want to recommend best practices rather than policy.

But I still think this discussion should happen so we can help quantify the issues. And hopefully get some of the people who aren't doing these things to be able to participate.

Mike O'Connor: This is Mikey, I think that we may be right at the nub of discussion for the working group. I agree that again with both points of view.

I think it's important to leave the registries and registrars the flexibility to innovate, but at the same time introduce some either minimum standards or best practices or something to broaden the base of behavior.

Because you know what we're starting to see as a pattern is that the very engaged registries and registrars in ICANN are the best practices practitioners. And what we need to do is figure out a mechanism to broaden those practices outward.

Greg Aaron: Okay. I see George's hand raised.

George Kirikos: Yes, I just wanted to talk a little bit about the notion of bad actors and how you know they shouldn't be allowed to register names any more. That's really going into a dangerous area.

Let me give a counter example. In the UK there's lobbying right now that if people violate copyright you know for downloading of music, etcetera, downloading copyrighted material that you know they be unable to access the internet entirely.

And countries are obviously able to make their own laws, but for ICANN to be doing it and allowing registry and the registrars to be interpreting that I think that's a dangerous area.

Like I think we can do things accurate WHOIS policy and then if on a civil basis or a criminal basis it's some court determines that you know Acme Inc. is no longer - you know determined, sorry, defined as a bad actor and can no longer register domain names for a period of five years.

Let's say that they're bound by some criminal decision or some court decision, then you know after that point you could say oh we've seen them you know two years later register domain name, they're guilty of violating you know the court sanctions.

You know delete the domain name, but to preemptively you know have an ICANN policy that goes into these areas I think is really you know fully out of scope.

Greg Aaron: Okay, and I think - and this is Greg, I think what Rod touched on was you know some registrant goes to a registrar and you know you get some domain names and starts using them to you know post malware and such.

And what happens at that point is the registrar says I don't want this person as a customer any more.

And may close their account and refuse to deal with them any more, which I think is a very reasonable thing to do. There's no requirement that a registrar be required to take on any given registrant.

I think that's a business decision.

George Kirikos: Right, but that's supposedly tapping into the registry level, George here, at registry level to one doesn't want to have for example VeriSign deciding who they want as a client.

Because you know obviously they would delete my 500 domain names first. There needs to be you know clear rules on what they can and can't do. I can see you know them you know suggesting oh, you know we don't want you as a client, but you know to do that we're going to make sure that you have accurate WHOIS.

And because you've been proven to be operating a bot net you know we're going to send the police to your door. That would be the proper you know due process because even criminals are entitled to that due process.

And indeed that should be the right way to get rid of them rather than just having the registry you know in a high handed manner.

You know you're an abuser so we're going to delete all your domain names. You could see you know where that road could lead to.

Greg Aaron: I'm not actually aware that any ICANN registry has ever done such a thing.

George Kirikos: Oh right, because they're not authorized or they would face major law suits if they did.

Greg Aaron: Yes, I don't know if that's an activity or - that actually has ever taken place. I mean every day mitigation takes place every day in registrars. You know somebody says you know this registrant's doing something bad and the registrar looks into it then makes a determination based upon their terms of service.

And then they may decide to do something, suspend a domain name or something like that. That's the kind of activity that takes place every day and has been for many, many years.

And that's based upon the contracts that the registrar has with the registrant. Okay, comments from anyone else?

I'll add something, this is Greg. I'm actually still wrestling myself with this issue of intent because I don't know if that's the proper measure even.

Intent is how you're going to use the domain name, what you're going to do with it. I think one scope issue is that again the - in the issues report we saw the ICANN council say that use issues are outside ICANN scope.

So I don't know if we could - if you said well you've got a repeat offender who's using the domain for bad things, even then I still don't know if ICANN could reasonably within scope say something must be done about that.

But I think that's an issue that needs to be wrestled with. I don't know if intent is the right measure to wrap a policy discussion around. So where does this leave us?

We're trying to feel out the bounds of the policy and scope. Mikey?

Mike O'Connor: This is Mikey, one approach may be to delineate some of the current best practices. This is kind of throwing the ball back to those of you who are real smart about this stuff.

And once we understand the current best practices, take a look at those as the basis for some sort of a minimum standard.

You know this might be sort of like pornography, this maybe I'll know it when I see it kind of stuff rather than intent.

I think intent is very tricky but maybe there are best practices that are out there now that we can agree are at least to be recommended and perhaps even going so far as to drive them into policy.

Greg Aaron: James?

James Bladel: Yes, I just wanted to point out that one of the other pitfalls of this approach is that a lot of these abuses are conducted through the hijacking or compromising of legitimate domains.

And so we should recognize for example that that sort of throws the intent issue out the window in that any domain registration could be compromised for these purposes.

And if that were the case then the legitimate registrants under some hypothetical policy is the legitimate registrant blocked from future registration?

So I see a lot of trouble when we start to put any type of prescreening or pre-authorization onto the registration process.

And therefore I think that this is something we should tread very carefully and in fact I would advocate avoid altogether.

Going to an earlier point that was made about best practices, the concern would be that registrars that have very effective best practices or internal business processes in place would abandon those and simply stick by the minimum that is required by the policy, any ICANN policy that would come out of this.

And then you could even see bad actors hiding behind the policy or at least their interpretation of it. So I just - I feel that taking what is something - I just feel that making this the realm of ICANN policy will only worsen this particular issue.

Greg Aaron: Thank you. This is Greg, I - James brings up an important operational or functional point which is about compromised domains.

With malware most of the domains that have malware on them actually are infected or compromised and that means the registration isn't aware of it and not responsible for it.

The phishing 80% of phishing domains are compromised or hacked, again the registrant is not aware of it.

And with spam, the - you know a lot of spam is sent out of bot nets so the nodes and computers that that mail is sent from, they're infected, the registrants probably aren't aware.

And then sometimes email headers are faked and people don't know actually which domain the mail is actually sent from, you have to be able to open up a mail header and actually understand what's going on.

That's an issue. So I think that's an important issue to wrestle with. I also have a question after Mikey. Mikey, you said on one hand best practices are something we should look at because we want to get the entire community engaged in dealing with spam and phishing and malware.

I encourage that, I want more registrars to think about their procedures and those kinds of things. But you also said then some best practices could be adopted as policy.

And I don't - I'd like you to tell us more about that idea because dealing with issues might be out of ICANN scope. So if there was a best practice that a registrar had for dealing with spam, for example what's in or out of scope and come back to the same problem again don't we.

Mike O'Connor: This is Mikey, yes, I think that's right. I think where I was headed with this is you know there's kind of a sliding scale. There's kind of the current situation which is where the best practitioners are innovating and working hard and acting aggressively and doing a bunch of stuff.

But there's not much cross pollination, there's not much advice about that. It happens informally. Then there's sort of a middle zone that says ICANN as the convener of a community encourages the dissemination of those best practices more broadly.

But doesn't enforce them on anybody. And then there's sort of the highest level which is that maybe some of those pass the litmus test of being in ICANN scope, being appropriate, etcetera and perhaps graduate to become policy.

My thought is that to the extent that ICANN can improve the community in its convening role, that's a good thing. That you know I'm certainly not dismissing the points that others are raising about you know like James' point that says if we impose a minimum and that drops the level of activity, I certainly wouldn't want to see that.

But at the same time, I'm - I would like to have more than silence I guess on this because I think it's important and I think that ICANN is really the only community where this conversation can take place.

So that's a long winded answer to saying no, I don't really want to see a lot of things in policy necessarily. But I also don't want to see silence.

And I also wanted to run back to your point, or the point that was made earlier about compromised domains and agree with everybody that the abuse of compromised domains I think is out of scope of this working group.

I would fully support that. I'll just tag that on the end.

Greg Aaron: Thank you Mike, sorry I was on hold. I see several folks' hands raised, I see Margie's hand.

Margie Milam: Yes, hi, I wanted to clarify, we seem to be taking a very narrow view of scope. I mean I just wanted to remind the group that we've had several presentations on scope.

And when you're talking about what's within ICANN scope, are you talking about whether you can you know adopt an enforceable consensus policy? Because that's one issue.

But you know in terms of what's within GNSO scope, you know the GNSO scope as described in the bylaws is fairly broad, you know dealing with you know does it apply to you know generic top level domains as an example.

So I think you know we don't need to be so restrictive. It may ultimately impact what the end result is if we're attempting to adopt policy that's binding on you know on a contracted party for example.

You'd have to look at the contract, but if you're talking about best practices and you know the topic relates to you know gTLDs, there may be more room for things like best practices or other types of policy work.

Greg Aaron: Okay, thank you. Let's see, I see - I'm just going to take these in order. I see George, Mikey and James, so George, you want to go first?

George Kirikos: Yes, the discussion about spam kind of caused me to think a little bit more about best practices and how you kind of differentiate intent at the beginning.

If we look at for example versus the spam, one of the big sources of spam is you know Gmail and Yahoo and Hotmail themselves.

And if you took a look at how they actually allow people to register accounts that might be educational to this work group.

Their best practice appears to be anybody who can pass a Captcha, you know a computer automated task basically to test that you're a human.

If you can pass that then you can register an account, irregardless of whether you've committed abuse in the past or regardless of your IP address for the most part.

If you can pass that Captcha you can register an account. And then any deletion or abuse that takes place afterwards is dealt with.

And so you know these are huge domains with hundreds of millions of users and the amount of abuse that comes out of them is substantial relative to their size is not substantial.

And that might be the same case for you know domain abuse in general. While there is a large amount of abuse that takes place, relative to the amount of non-abuse that takes place, perhaps you know the best practices need to take into account that relative balance.

I just wanted to toss that out.

Greg Aaron: Okay, thank you George. Mikey is next.

Mike O'Connor: This is sort of in response to Margie's comment. I think we need to distinguish between ICANN scope and the scope issue of this particular working group.

I'm mostly narrowing the scope of this working group for fear that they'll otherwise bite off a task that's too big to complete.

So I just wanted to zero in a little bit on that, that most of my comments aren't about ICANN scope at all, they're really just about the scope of this working group.

Greg Aaron: And James?

James Bladel: Yes, and my response was also to Margie's points relative to scope. I just wanted to point out that in my perspective that when we start talking about different types of spam, phishing and malware we're encroaching a little bit on use and content.

And therefore I think it's a little dangerous to - or trying to put policy around those activities because they could be expanded into other areas of use in content.

And I think that you know if they were completely and wholly contained within the process of provisioning and registering domain names that would be a little more clear cut.

But since they involve elements of how that domain is used, I think that's where the red flags at least for me start to go up as far as scope.

Greg Aaron: Okay. Anyone else?

Rod Rasmussen: This is Rod, I expected comments on a few - a lot of the concept that have come up here, and I'd just like to say the discussion here just kind of proves that we need to talk about it more.

But beyond that I want to make sure that people aren't misconstruing my desire to tackle these issues as a way of sneaking in - getting registration or taking on the entire issue through the registration abuse policy group.

I really want to focus on those areas that abuse of the registration process itself. So that is you know I think there's two very germane areas there. One is the use of credentials, stolen credentials, etcetera.

And that comes back to verification of users. There's plenty of good examples in the real world where policy gets set by a group, let's say it's the banking industry saying you must know your customer before you can assign an account, that kind of thing.

Then the other area is systemic abuse by typically resellers. Again this is an area that's probably a policy area as far as how registrars deal with their various agents.

Now that may or may not need some sort of modification but again those are the two areas I see as being very germane to this group. The use of - the broad scale use of domain names for phishing and malware and all that is kind of the - that touches on lots of areas I think are outside of the scope of this working group.

So I'm not trying to say that we should take this all on but really focus on those areas where we can actually have some leverage in the process.

And absolutely I think that the compromised domain issue is a big one. I think that we do have a problem where people are suspending domain names that are innocent.

So I would argue that one of the things we can do is help clarify those issues so that people aren't doing that, but that may very well fall outside of the scope of this group because that is a usage issue largely, unless you're suspending something based on what is already done.

So those are my comments.

Greg Aaron: Okay, thank you Rod. We are coming up at the end of our meeting time, about 28 after, so this has been a dive into the issue. I think it's been really constructive.

Sounds like we're still feeling out kind of what the issues are here and so I would propose two things. One is continue this conversation in the next call for sure.

Now we have scheduled an offline conversation for a sub group of people. What's going to be the purpose of that call? Is it to continue this discussion or I should we continue this discussion in the larger group?

So actually I wasn't - I had forgotten or didn't know that there was going to be a subgroup call arranged, so my question is what's the purpose of that call and what's the agenda?

Or should we continue this conversation amongst the larger group?

Mike O'Connor: This is Mikey, as another member of that call, I think that given - I was participating in the call with sort of the same point of view that you were Greg, I couldn't remember why we were getting on the call but I felt like I was being a good scout.

So why don’t we - unless somebody can more accurately remember, why don’t we just have this continue in the large group for now and postpone that subgroup formation?

Greg Aaron: Is that suggestion okay with the other folks? It’s okay with me. I think we’re still as a bigger group wrestling with the major scope issues that these problems present to us. Any objections holding off on that subgroup call?

Okay, hearing none, let’s all - Gisella let’s hold off on having that call and let’s continue to put spam, phishing, malware on the topic of the agenda for the next working group meeting.

Marika, we’ll definitely need a Wiki for this topic. Do we already have one?

Marika Konings: Yes, we do I think and it’s in the forum that is the other one.

Greg Aaron: Okay awesome. Okay, that will be ready when we need it then. Mikey?

Mike O’Connor: I guess my thought was that it would be very neat if somebody could sketch out the outlines of the conversation we just had on that Wiki as sort of a homework assignment for next time so that we can sort of start from where we are now rather than starting from zero again.

Because I thought - I agree Greg, I thought today’s conversation was very good and it would be neat to have it summarized.

Greg Aaron: Marika, once the transcripts comes out, would it be possible for you to pull out the relevant sections?

Marika Konings: Yes, no problem.

Greg Aaron: Kind of a skeleton? That would be great.

Marika Konings: Okay.

Greg Aaron: Nothing terribly fancy but we want to get the skeleton of that conversation and the major issues down on paper so we can continue to go through them.

So if you would be able to do that in the next two weeks that would be greatly appreciated. Okay, awesome.

So that was the - I think a very directed and very rich discussion. So thank you for your thoughtfulness. We'll continue it next meeting. We have a few action items I've noted so I'll send those up to the list.

And our next let's see, next meeting would therefore be Monday the 14th, is that correct? September 14.

Mike O'Connor: That's what I've got, Mikey here.

Greg Aaron: Okay. By incredible coincidence I will be at the German anti-spam summit that day in Frankfurt. So I will check my availability to join into the call that day.

If there's a problem where I'm not able to get in, I kindly ask if Mikey would mind filling in for me if I'm not able to fulfill my duties that day. Would that be okay Mikey?

Mike O'Connor: Yes, that's fine, I can do that.

Greg Aaron: Okay wonderful, thank you. Okay, I guess that's it for today and thanks so much again for the rich discussion and we'll talk again in two weeks.

Mike O'Connor: Thanks Greg, great call.

Greg Aaron: Thank you everyone, take care.

Mike O’Connor: Thanks, bye bye.

END