

**Registration Abuse Policies Working Group
TRANSCRIPTION
Monday 21 December at 15:00 UTC**

Note: The following is the output of transcribing from an audio recording of the Registration Abuse Policies Working Group meeting on Monday 21 December 2009, at 15:00 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-20091221.mp3>

On page:

<http://gnso.icann.org/calendar/index.html#dec>

Present for the teleconference:

Greg Aaron - Registry stakeholder group - Working Group Chair

James Bladel - Godaddy Registrar stakeholder group

Berry Cobb – CBUC

Mike O'Connor – CBUC

Rod Rasmussen – individual

Faisal Shah – IPC

Martin Sutton – CBUC

Philip Corwin – CBUC

ICANN Staff

Marika Konings

Apologies:

Margie Milam

Gisella Gruber-White

Operator: Excuse me the recordings have started.

Greg Aaron: Okay thank you.

This is Greg Aaron and this is our registration abuse policy working group for December 21, 2009; our last meeting of the year.

And why don't we begin with the roll call. Marika would you like to do the honors?

Marika Konings: Yes, no problem.

On the call today we have Mikey O'Connor, Berry Cobb, Faisal Shah, Greg Aaron, Rod Rasmussen, James Bladel, Phillip Corwin, and for staff we have myself Marika Konings. We have apologies from Margie Milam and Gisella Gruber-White will be late.

Greg Aaron: Okay thank you.

Well let's hop right into it. Today if at all possible we'd like to close out the last remaining of these topics that are to be discussed which are stolen or fraudulent credentials, sale of counterfeit goods, false affiliation, and unauthorized use of logo.

Oh and we have Martin Sutton joining us now.

Martin Sutton: Hi yes sorry for my lateness; stuck in the snow.

Greg Aaron: Okay thanks Martin.

All right so Rod if you would – this is your document that we see up on the screen. Would you like to walk us through? Now what we did last time is we kind of walked through some of the issues and you explained the broad strokes.

But maybe what we ought to do is concentrate on the latter part of the document which has some ideas or recommendations for discussion.

How does that sound?

Rod Rasmussen: Okay.

Greg Aaron: Do whatever you feel you need to do.

Rod Rasmussen: All right well we went over this last week – I thought it was fairly longwinded but I can – as usual. But I can certainly dig in here a bit as well. And we didn't see any discussion on the list so maybe we can get some of that going so we can flush out the actual placeholders that I had at the end here.

Just to recap for those who weren't on the call last week there were – I took the work credentials and broke it down into really what I saw as the three places that could apply to what we're talking about. Because credentials themselves are fairly broad topic area when you just look up the definition in the dictionary.

So we had what I consider kind of three categories in credentials in use of information technologies. Let's see here. We have the access control type of thing which is user name and password and things like that where you can get on and, you know, use it to get into some sort of system, you have cryptography which are cryptographic keys, et cetera.

And then you had identification – actually I'm sorry. I'm looking at the wrong – I'm looking at the Wikipedia. Here we go. Get my brain working here this morning.

Yeah so I had – so yeah that one was actually the definition from Wikipedia. So the three that I execute on was identity credentials which are, you know, things about a person. It gets into the things that establish a person's identity whether it's like a passport or your driver's license or things like that – your personal information.

Your access credentials which allow you to get into, you know, computer systems and things like that. And then financial credentials which are credit card and the like allow you access to money. So those are the three types of credentials. And then take a look at the various types of abuses we're seeing against those and how that applies to domain registrations.

And then what we didn't talk much about where I guess the – what we can do in the roles for policy and other things that we could talk about as far as mitigating those abuses of those different types of credentials within the domain registration process.

The – and really you get into looking at those from a model of how the registrar/registry actually works, what they accept as part of the registration process. You look at the ways that people can get a hold of their different credentials and then just use them later on.

And then, you know, try and applying that across a band – or a wide swath of different registration methodologies can be challenging. But I think there certainly are some commonalities and if nothing else baselines could be set as far as how – if you are dealing with certain types of credentials that are dealt with and best practices as to how to deal with them beyond that.

So I have put together kind of the end of that document a placeholder for looking at models from other industries whether that's the payment card industry or healthcare or other people who have to deal with personal information credentials, financial credentials, and access credentials.

I think there's certainly some room for improvement on all three of those areas given the widespread use of stolen credentials in the registration process today.

And then also what could be done as far as, you know, best practices and, you know, standards for protection for those types for credentials across the industry. And it's going to vary depending on what type of credentials we're talking about there.

Access credentials, you know, that's good password management and things like that. Financial credentials you're looking at what the option of standards that are fairly well publicized. It's a matter of, you know, actually doing them

for the most part and, you know, requesting, requiring, calling it a best practice, what have you that people follow those standards. There's standards and then there's the actual application and enforcement of those standards.

And then, you know, for PII type of things, you know, that's something that I think one of the things that we run into is that we're all talking about doing some sort of data sharing between entities and domain registration community to allow us to track down and prevent bad guys from doing things. That's been talked about in multiple forms.

But one of the questions is do our current agreements and policies, et cetera, even allow for that to occur or encourage it to occur? So all these other efforts are being talked about may be, you know, may run into some difficulties getting implemented if we don't have a framework for which in to work with, you know, data sharing, et cetera, across an industry. Because there's always concern about collusion and these other antitrust type of issues when you start talking about data sharing between elements. And I know we've run into that in various groups that are trying to set up data sharing agreements.

So can we codify that at some point so we can allow for that? So those are some of the ideas, et cetera, that are in there. I think at this point, you know, I've got some placeholders in there for talking about specific ideas but I don't have anything concrete. We need to figure to what we may or may not want to put into this section and get it written up.

Greg Aaron: All right thank you Rod. Thank you very much and thanks again for writing all of this up.

If I can my suggestion is first let's – it looked like there's several ideas in here, some of which might be for best practices, some of which seem - might be for

policy making. So let's try to figure out if they're any policy issues and then any best practice ideas.

So in – on that last page you have several things. Now which of those would be policy related? Under addressing use of stolen identity credentials there's an idea to provide a policy framework to allow information sharing between registrars of fraudulent domain registrations and registration attempts.

Okay. So let's open that up for discussion. My question is is a policy framework within ICANN needed or is it applicable? I'd like to open that up to the floor.

Mikey?

Mikey O'Connor: Hi Greg this is Mikey. I think the question and Rod you're going to probably want to chime in on this.

One of the reasons you may need a policy framework is to clarify some of the anti-collusion legal stuff. So that information can be shared between business entities in a way that doesn't expose them to the liability that they might otherwise be exposed to in a fair trade sort of context.

I know that in the PCI industry – I can't remember if there's law or regulation about this. But it allows otherwise competitors who would be accused of colluding to share certain kinds of information between themselves. And Rod again you're way more current and closer on this one but I think that might be the reason that that's in there.

Rod Rasmussen: That would be – that's why it's in there but I am not a lawyer nor do I play one on TV. But I do pontificate at parties.

So...

Greg Aaron: Okay. I see James's hand if you're done Mikey.

Mikey O'Connor: Yeah I'm all done.

Greg Aaron: Okay. Over to you James.

James Bladel: Thanks Greg. This is James and apologize if I'm not coming through very clearly but I think that Mikey raised a good point. You have to ensure that your I's are dotted and T's are crossed relative to making sure that there's no underhanded information sharing or, you know, collusion going on.

But I think that the – one of the best ways to do that is to ensure that you have a third party that is acting as an intermediary to collect and distribute all the data sharing, especially when it's narrowly specified as being information that's relative to fraud or criminal abuse or something like that.

I don't know that that means that necessarily ICANN is the only organization that can step in and fill that need. You know, we have a couple of other organizations that could be equally suited to step in and be the centralized trade association or clearinghouse for that type of information.

Hello?

Oh I thought I lost you guys.

Greg Aaron: Okay.

Got a couple of hands. Let me go to Berry first because he hasn't spoken yet.

Berry Cobb: Well for the moment I guess I just have a question. When we use the word like a policy framework versus the idea pervious where it just talked about the dissemination of best practices each of them is really talking about the sharing and dissemination of information.

So I'm just – my question is is what does the policy framework part of this idea make different than just the sharing of best practices? And I guess specifically the question is is does this framework allow for a fast track of new policies to be developed to combat stolen identity credentials or if that could just get a little clarification there.

And/or an example of something like that that may exist today within ICANN.

Greg Aaron: Let's see. Let's go to Rod and then Mikey.

I see their hands up.

Rod Rasmussen: Okay this is Rod again. Yeah Berry I think that the idea here and actually it gets to James's point as well I think is that there's two back to back ideas here within that stolen credentials area.

One is this policy framework and the other is the data clearinghouse. I think those almost have to go hand in hand in that if you're going to have some party, you know, third party or what have you, you know, that's gathering and sharing this information that you have to have within the community that's doing that sharing some sort of a framework for how that works. And how that, you know, protects and identifies the people who are sharing that information.

I think that, you know, within the ICANN world I mean we might just want to take a look at how the whole thing's set up in the first place, is that there's access and policies set up so that, you know, people share access to a central route, you know, zone files to be able to add and enter things in. The registrars all share access to a central registry, for example.

I think that's painting kind of a broad stroke but in order to make sure that there's not – that people will actually - will play this is what we run into in an

abuse world is people don't want to do things because they don't think they're protected when it comes to information sharing.

And they would like to but they, you know, there's somebody saying, "Oh no you can't do that because we don't have the legal authority to do that or we may potentially somehow expose ourselves to risk. So given that we don't want to do it."

So codifying things in a way that says you're okay to do that from a central resource is usually very helpful in getting people to cooperate that, you know, that want to cooperate but they have some sort of - something holding them back from a risk management perspective.

Greg Aaron: Okay. Thank you.

Okay and then I see Mikey's hand.

Mikey O'Connor: Thanks Greg this is Mikey.

Just to piggyback on what Rod just said. I think the policy framework on information sharing is really just as he described it. It's sort of the rules of the road and who's liable for what and what are the boundaries of what can and cannot be shared. What can we do to indemnify folks that are sharing the information?

And then to James's point I sort of agree. I don't think that ICANN is probably the right organization to actually host this service. I think that's pretty far outside of ICANN's mission and charter.

But I think that ICANN is a pretty good place to put this policy framework in place and start the conversations between the people that need to participate. You know, I think we're going to run into a really similar discussion in the route zone working group that we're on.

How's this going to work? What are the rules for the road? Who's responsible for what? And I think ICANN is actually a pretty good place to hammer out that understanding even though I don't think it's a good place to actually provide the service that may emerge out of that.

Greg Aaron: Okay thank you Mikey. This is Greg. I'd like to share some perspective from the ecosystem out there that kind of deals with these issues.

Right now registries and registrars do share information about malicious uses of domain names with each other. And they do that in some various forums. You know, they're security groups and mailing lists where people are saying okay we're got a problem on this domain name. Can the responsible registrar take care of it for example.

And then there're groups like RISG which is a group of registries, registrars, and some security companies who have been working on data exchange program again to point out places where phishing and malware are occurring; affiliates and internet identity – Go Daddy and MarkMonitor amongst others are in that group.

And they got together not under ICANN auspices but because they want to share information. I think with – I've never had a registrar share credit card information with me in my security work because they say they can't do that for security and confidentiality purposes.

What I hear from them is that's just a legal issue. I'm wondering – there isn't therefore an indemnification aspect to it but that would be I think between parties and I don't know if that's an ICANN issue. (Unintelligible).

Now they're also some third party organizations out there that facilitate this kind of thing. For instance there's an organization called (Asoka).

And that's a third party where companies can basically share information and do credit card checking. For example the registrars who have joined that and the problem they're trying to solve is that fraudsters are using stolen credit cards to create new domain names to do bad things with. And so I know some registrars have joined that as a way of improving their fraud checking on the cards.

So my question personally is is this more of an issue between parties? I think there's that indemnification question but I don't know if that's an issue that should be solved within ICANN.

So that's my perspective.

Martin's raised his hand.

Martin Sutton: Thanks Greg. Just to keep checking here I mean we've probably head on to specific information when you (unintelligible) credit cards there. I would say that it doesn't necessarily have to be those particular elements if that were deemed a problem should it be.

But certainly phone numbers, emails, contact information, et cetera that regularly appears on who is – could potentially be a useful thing to share. If there are concerns through say data protection security issues if the purpose for the data sharing is to prevent crime there are a number of areas that are able to assist that data sharing facilitation because the purpose is a legitimate purpose.

So we probably don't need to at this stage get head up too much on what detail can or cannot be shared. It's more problem are we going to solve, how big is that problem, and what are those data elements that will do the best in terms of combating the fraudulent activities?

So I just wanted to raise a couple of points there.

Greg Aaron: I'm sorry this is Greg. I was on mute.

I think Rod's next and then Mikey.

Rod Rasmussen: Thanks Greg. This is Rod. I was about to see if you were still around.

The – and just I want to follow up on Martin's point there and I think one of the areas we've run into, you know, varying regulations and thoughts of what can and can't be shared is in the area of IP addresses and very specific stuff that is going on as part of the registration process.

Where again it'd be nice to have some rules of the road or, you know, some – here's what we know we can do to work some of these practicalities out with – on those various efforts that are going on. And, you know, the RISG effort and a couple of other are out there very – being very specific about helping - not only just enable those to work, but to help encourage other members of the community who we may not see showing up at some of these meetings to be able to say well we actually have created this ability to share this information.

And have, you know, through various, you know, processes, external (unintelligible), what have you have these in place. ICANN of course, you know, can help codify these things as far as being able to, you know, this is a accepted practice, this is a proper thing to do, whatever you want to – whatever terminology you'd like to use is very helpful in dealing with the registrars who, you know, are not – are a little recalcitrant when it comes to trying to get them to participate in antifraud measures.

When there is a – when ICANN does make a pronouncement about something dealing with that it's amazing how much more cooperative they are in dealing with issues rather than just falling back and saying, "We can't do anything."

So that's one of the reasons for actually just putting some things in place. And, you know, at this point we're just talking about ideas here; not actually trying to develop any policy. But, you know, what would that look like and how would that be helpful? Because I think that's what I'm trying to concentrate on there.

Greg Aaron: Thank you. Okay and I think Mikey is next in the queue.

Mikey O'Connor: Thanks Greg it's Mikey again. I think that the reason that I – at least in this pre-PDP phase lobby for a policy discussion about this is because I think that it's all the things that we've been talking about.

You know, I can't – is the central place where these particular stakeholder groups get together? And it may be a simple matter of a policy group saying, "Well this other group is really already doing exactly the right thing." But I doubt it.

I think that there's – when it's (unintelligible) kinds of relationships between subgroups of the ICANN constituency we run the risk of missing opportunities to broaden the reach of those things. And we also leave people uninformed and unmotivated to participate.

So I think I'm continuing the lobby for a recommendation that at least we take a policy look at it. I agree with Rod. I don't think we've got cycles of the time or the charter to actually formulate that policy but I think it's a worthy discussion.

Greg Aaron: So Mikey – this is Greg. What would the – how would we encapsulate the policy questions that needs to be explored?

Mikey O'Connor: I'm going to be a guy and make stuff up. But others feel free to chime in. I think one of the policy discussions is to what extent should participation in these kinds of activities be required of registrars and registries.

I think another is what kinds of participation are we expecting both in terms of the legal relationships and in terms of the technical relationships.

I think another policy discussion is the one about collusion and setting up a legal framework to protect the entities' ability to share information without fear of legal repercussion.

And I think another is – it's probably not necessarily a policy discussion but a best practices discussion about the preferred form of the entity that the information is shared through (unintelligible) separate organization from ICANN – my guess would be probably yes. Is it a non-profit, is it a for profit if it's jointly owned by registrars and registries and others, et cetera, et cetera.

I think that ICANN is a great forum for that kind of discussion and, you know, those four bullets would at least get it kicked off.

Greg Aaron: Thank you Mikey.

And I think it also raises a charter conundrum for us. Because this group has been charged with figuring out whether those things are in scope or out of scope.

Would we be kicking the can down the road to say there should be a policy effort to figure out if this is in scope or out of scope for ICANN to do?

Mikey?

Mikey O'Connor: I think we have to kick this one down the road a little bit given the amount of time we have left. I think we can sharpen the issue. And I wouldn't be that

uncomfortable putting it forward under the umbrella of saying that it's at least a discussion in this end scope for ICANN even if the outcome of the discussion is no policy for now.

But I don't (unintelligible) given the fact that we need to get a preliminary report out basically within a month I don't think we can much beyond what we're doing here – (unintelligible) pile but (unintelligible) answer the question.

Greg Aaron: Okay Rod why don't you go next.

Rod Rasmussen: Yeah I was just going to say that I think – at least I hope that the discussion we're having is – would fall within scope. And if we're talking about facilitating data sharing that will be part of the registration process to curtail abuse. So we may have already answered the question of scope or not but then the – it's more of an implementation question as to how you would, you know, how and if you need policy and then how and if, you know, you do various best practices or things like that to facilitate this type of activity.

But I think that the idea here is that we've got issues surrounding the registration process itself and policy around data sharing of information and the like. I think we can hopefully be able to agree we've got something within the scope of what we're talking about. And it's really a matter of what we're saying needs to be looked into further is – and that which coincides with the rest of the things we're doing we've got questions about, you know, actual how do you do it.

Greg Aaron: This is Greg. I had raised my hand. I'll – I'm speaking of course just as an individual member right now. But I'm not sure if this is in scope or not.

I don't think we can say that it is in scope. I think that's perhaps an open question for now.

Now Mikey also just raises a practical question which is we're – got to put our report out in February. Now our report is going to be an initial report though and one of the ideas of the initial report is the – then get constituencies to comment and you get comment also from anyone else in the community to then inform a final report.

And the final report is what GNSO council then take the actions on, right? So they don't – they're not going to really take any recommendations until we've gone through the whole thing.

So it sounds like we've got an issue that we're still wrestling with as far as the scope question. It's fair to continue this discussion over the next few months perhaps.

What we could do is say, you know, this is a vector that's being used. It's in the registration process. There are some issues that we haven't come to consensus on yet at least. And, you know, continue it that way.

Rod?

Rod Rasmussen: I just wanted to try and get an idea of where the group stands on, you know, whether we've got something in scope here or not. I'm, you know, I don't know whether I'm in the majority or the minority or am seeing something that seems to me so obvious that it's frustrating for me that others don't.

So I'm trying to understand what is the question of scope and where the group is. I'm – if we're going to spend some time working on this we may as well figure out where we are so you might want to request that we figure out where we stand and what needs to be done one way or the other to make this either happen or go away.

Greg Aaron: Very fair.

Let's figure out how to frame this then so we can do our hand raising and such and take a straw poll.

We have a couple of ideas before us. One is is there something within policy scope? Now when we're talking about policy scope we're talking about binding policy. So that is policy that would be required of registries and/or registrars.

Then there's also the – separately there's another realm of non-binding stuff and that would include best practices and so forth.

Now so what is the policy issue? Are we saying that policies around the sharing or use of stolen credentials is within ICANN's scope to make binding policy on? Is that an appropriate way of phrasing the question?

Again that's is making binding policy upon the use or sharing of credential information within scope – within ICANN policy scope?

Does that sound right or should we rephrase? Mikey?

Mikey O'Connor: I'm not going to come up – this is Mikey. I'm not going to come up with rephrasing yet but I think one of the issues that we're sort of tiptoeing around is sort of a sequence question.

In a way it's hard to know whether ICANN should make a binding policy until we know the sort of practical implementation of the things they're going to make policy about.

So for example it may take an iteration of figuring out how to do the sharing and how to organize it before we can say this is such a good thing that everybody ought to participate at least at this minimum level.

You know, I think I would be nervous about saying participation is required in a policy context before I knew what the thing people were participating in was going to look like.

And so I think that perhaps the thing that's in scope for ICANN is in the context of providing leadership on this issue. We have Rod, a fellow who spends his whole life basically in this environment saying, "ICANN you are the most obvious people to have this conversation and figure – and at least take a leadership role in figuring this out. ICANN you may or may not have to make specific policies." But it's certainly within their scope as an organization to organize this conversation and to facilitate it.

Now I'm sort of putting Rod's – words in Rod's mouth when I do that. But I think that I'm a lot more comfortable with a pretty broad definition of the scope question than a really narrow one.

It may turn out that actual legal context of sharing information may be outside of ICANN's scope but...

Greg Aaron: So what I'm hearing from you Mikey is that you don't know if it's in ICANN's scope to impose policies here yet.

Mikey O'Connor: Yes. That's exactly right.

And that's – I have doubts as well. I mean for me it's – there is the question of ICANN is a good place to discuss these things but that might end up being best practices.

At the same time my view is we have to ask is ICANN the right place to make policy on these things? It might be the most obvious place but it still might not be the best place or the right place.

So that's kind of just where I am.

Greg Aaron: All right so let's go back to the phrasing question. Sounds like we don't know yet actually.

I'm saying I don't know and I have doubts about whether ICANN can make policy in this area. Mikey's expressed that he doesn't know yet at least.

Are we – can we say with any confidence then that this is within scope? We have to leave it as an open question.

Mikey O'Connor: This is Mikey without his hand raised – sorry.

If you said that is the question of information sharing between registrars and registries an arena of ICANN – within scope for ICANN policy making? I would say absolutely yes. (Unintelligible) is the perfect example of information sharing between registrars and registries. We already have lots and lots of policies on that.

And so I don't have any doubts on that front. What I'm not quite so comfortable with is the degree to which certain kinds of information sharing would need to be required in policy until the definition of that information sharing was a lot clearer. And that's the sequencing question I got.

Greg Aaron: Okay.

So how do we move forward?

This is an area that needs more exploration. It sounds like we have a consensus on that. But we don't know all of the policy implications. There's also the possibility that this kind of stuff might not be a policy – a binding policy kind of an issue but they're all those other possibilities like best practices and so forth.

Berry Cobb: Can we agree...?

Greg Aaron: I'm sorry. Go ahead?

Berry Cobb: It's Berry, I'm sorry. I'm not in front to raise my hand. Real quick I'm just curious hypothetically let's say we all agreed that there should be policy made around this particular topic and we make a recommendation as a team and move forward with it.

You know, what happens if it's not within scope? They would just deny the recommendation and then move forward. So I guess my question is what harm do we have by making a good recommendation that, you know, X number of level of effort needs to be done around this topic and then let the powers – kicking the can down the road so to speak and let the powers that be make that determination for us.

Greg Aaron: Yeah I think they're two issues nested in there. You're right – the council ultimately decides what course it wants to take to authorize a PDP or an issues report or what have you.

I think it's an issue for the individual members of the group to decide whether they want to state that there are policy issues – definitely.

I think that's up to each member to decide whether they can take that step.

I see Marika's hand.

Marika Konings: Yeah this is Marika. Just to Berry's point indeed, you know, if the council would take the recommendation forward and say well let's explore what is possible in the product and development process the first step would be an issue of support (unintelligible) of which one of the elements is the advice from the general council whether it's in scope or not. And it normally provides some guidance as well, you know, where possible like which parts might for

example be suitable for consensus policy development and which areas might not be in scope.

So further work would also be done regardless of the recommendations that this group makes and, you know, affecting that against the bylaw requirements.

Greg Aaron: Okay. Thank you Marika.

Rod I still see your hand raised. Would you like to go ahead?

Rod Rasmussen: Yeah Greg thanks. This is Rod.

The – I was going to say I think that one of the big problems we're running into here is we've got a – kind of a high level concept and a few particular ideas that aren't very well fleshed out as far as addressing things.

So it might be good just to put a placeholder in for this at this point and for, you know, perhaps we have a subgroup which I'll volunteer to be part of to flesh these out a little bit more so we can maybe have some more concrete things that get us to a point where people feel more comfortable one way other other being able to say yeah, that belongs or no, that's really something that, you know, you can – it doesn't belong in our discussion here as we've done with several other issues.

It's just a thought for moving us forward practically here.

Greg Aaron: Thank you Rod.

That will give us a little more meat to sink our teeth into.

And I mean that sounds good to me if that sounds good to everybody else.

Anybody else who would like to help Rod with that?

Mikey O'Connor: This is Mikey. I'll join.

Martin Sutton: This is Martin. I'll join and help flesh out anything there, Rod.

Greg Aaron: Okay, all right. I'll take that as an action item for – to be done offline and posted up to the group as Rod and Mikey and Martin on tap to do that. Okay. Excellent.

So thanks in advance for that.

If possible I'd like to then – since we have an action item on that I would like to move on to the next topic since we're a little more than halfway through this meeting if that's okay with everyone.

The next item is sale of counterfeit goods. This is a proposed abuse but it was proposed back when we were compiling our initial list. I forget exactly who had proposed it. Does anyone recall?

Okay. Let's find that on our sheets. Just a second.

Man: (Unintelligible).

Greg Aaron; Is it under false affiliation?

Man: It's just called counterfeit by itself.

Man: There's another one on the very last – Page 5. The very top of Page 5 in the document. I just found the search function by the way. It's very cool.

Greg Aaron: Yeah. So we have counterfeit which is websites used to sell counterfeit goods – the impacted party being consumers. And then did you see another one which applied?

Man: No that was the one I found.

Greg Aaron: I think that's it, okay.

So sale of counterfeit goods on websites. Is this a registration abuse?

James has raised his hand and then Mikey.

James Bladel: Hi Greg you anticipated my statement I think with your question that I don't believe this is at all related to the registration process and this is a use function (unintelligible) site.

Thanks.

Greg Aaron: Thank you. Mikey?

Mikey O'Connor: This is Mikey. I'd chime in on that. It just seems very much like a use question rather than a registration question.

Greg Aaron: Okay.

Martin and then Rod.

Martin Sutton: Yeah I'll basically say the same thing. I would like to just question out and probably James might be able to enlighten us. I saw some recent news articles; Go Daddy did quite a bit of work on this that there's a specific policy that you've got drafted into your registrant agreement I think it is with regards to counterfeit drugs being sold.

I mean again that's probably content and use rather than registration. But is there anything useful to draw out from that from what you experienced so far?

James Bladel: This is James speaking. I'll respond to Martin. I don't have any firsthand information on that. I'd have to check and see if that's where that's actually been inserted. I'm guessing it would be probably into our universal terms of service for hosting.

And it's also something that we've worked with in conjunction with our legislative groups here in Washington, DC to get this added into various online criminal statutes so of course that would be US only.

Martin Sutton: And then I suppose a point from that would be if that's relevant to the registrant of a domain name mustn't use it in a particular way. Is there anything that we could draw from that which is relevant to either users best practice or introduce for all gTLD registrar agreements with registrants?

James Bladel: Again I'll have to get back to you on that but right now I'm thinking that that's more targeted to our hosting terms of use rather than our registration terms of use.

Martin Sutton: Okay thanks, okay.

Greg Aaron: Okay. And I see (unintelligible) checkmark and then Rod has his hand up.

Rod Rasmussen: Thanks Greg. This is Rod.

The – James I think that it also applies to your domain registration side as well. I think that's in response to illegal pharma stuff and I think it's the (Ryan Hade) Act in the US if I recall correctly so you might want to check on that part of it as well.

And I would say again we've come up to another issue where it would – it looks typically like a use case issue rather than a registration issue. The – but like many other things the scale and the methodologies that the people who are doing these kind of things are using, you know, got all kinds of other abuses we've talked about over the months where you've got large, you know, hundreds, thousands of domains being registered on an automated basis (unintelligible) to support these kind of activities gets the same question – begs the same question. Again are there, you know, are there things that are being done on such a scale that the registration side of the equation comes into play.

You know, as far as the individual abuses go absolutely I think it's an abuse case. It's when it gets to scale and it starts to affect, you know, large swaths of the internet and users on the internet that you start looking at well gee is there something we can do on the registration side of this?

So I just bring that up because it's again another example of what kind of misuse the people are putting the domains name system to in general out there.

Greg Aaron: Yeah. This is Greg. I'll go and then Mikey's raised his hand.

With these use issues I don't think scale is a matter. ICANN in general is responsible for the overall health of the DNS and those activities don't impede the general function in the DNS. They're a big problem and they cause hungry consumers and so forth. But there's not a technical issue that is making the DNS break down. I don't think scale is a consideration. I think it's mainly an abuse issue.

Now there's absolutely an interesting angle here I think best practices. I think this is an example of something where maybe one or more registrars have put that in their registration of use terms of service because they don't want to be associated with that kind of stuff. And that's kind of a moral stance.

It's probably also a business stance because if people are doing that kind of thing it creates a lot of issues. And you want to just – you don't want those business issues of having to hand off as abuse complaints and (unintelligible) complaints and that kind of thing.

So I think registries and registrars should be allowed to put things like that in their terms of service but I'm not sure that ICANN should be able to mandate it because it again is a use issue.

Mikey why don't you go ahead.

Mikey O'Connor: Thanks Greg. This is Mikey. I guess I have a question for Rod and maybe you too Greg. And that is if you determine the intent to register a domain name can use it in this way.

And that's I think what I'm hearing and what I think the both of you are saying. Then all of a sudden my mind changes because if you could determine at registration that a person is registering a name in order to do counterfeit goods – especially counterfeit pharma but almost any kind – then all of a sudden I'm quite cheerful saying sure this is a registration abuse.

Is there any chance that that's possible?

Greg Aaron: Let's see I see Rod's hand.

Rod Rasmussen: Mikey in some cases yeah it's a lot like the same people who are doing this are doing malware, doing phishing, doing the same types of organizations, the same types of setups are being used. At least, you know, in today's world if you get a string of 1,000 registrations and they all happen to use the same name servers as the ones you filled yesterday that happen to have all been registered.

Typically fraudulently, you know, stolen credentials are all pointing to the fake tag ware or however you pronounce it – watch site or what have you. It's the same stuff. It's just a different flavor of the same stuff.

And some of it, you know, this is where we kind of run into some interesting dilemmas in that you've got, you know, phishing and malware and things that are illegal everywhere, versus this kind of stuff that's not necessarily illegal everywhere but it's using the same techniques and the same kinds of methodologies for setting them up, oftentimes with the same exact infrastructure providers behind them.

So yes you can determine a lot of it. You can't determine all of it so, you know, there's always that thorny issue as to, you know, how are you going to make a policy that can capture and encompass everything if you're going to make policy?

But yes certainly you can find a lot of these things. I would, you know, I don't think we have it listed through fake job sites in here too for lack of a better place to put it. But those are, you know, you've got your pharma stuff, your luxury goods, your software, you know, piracy's– piracy on the list – I forget.

And then, you know, your fake job recruiting site that are typically turned into money mules and things like that that all use the same kinds of techniques often with (fast flex) and the like. So it's all kind of intermingled.

Greg Aaron: Thank you Rod. This is Greg; I raised my hand.

I agree with Rod that – and I'm going to speak as a responder to (unintelligible) and complaints and sites and domain names that have these kinds of problems with them.

Sometimes you can establish to a pretty high degree of certainty – especially when you kind of have a repeat offender who's working on a known

infrastructure or is, you know, you have a batch of domain names and you're able to see problems associated and prove problems associated with certain – with some of those domains, you know, the whole batch for example.

I also agree with Rod. Sometimes you cannot determine intent beforehand. And that's a - gets into a really tricky legal area.

I think this all comes back to a topic that we've discussed before which is are you going to require a contracted party to do something about a domain name that may have illegal activity associated with it?

I think – I am hearing that everyone thinks it's a use issue but I think it comes back to these issues of can you force people to shut down domain names and that kind of thing? And, you know, and we've kind of outlined the indemnification issue that goes along with that and we'll be putting some material into the initial report about that.

I think again this is a kind of illegal activity. It's in that respect it shares the same issues with malware distribution and phishing and all those other things.

I'd like reaction to that.

Anybody? Mikey and then James.

Mikey O'Connor: This is Mikey. I agree (unintelligible) this is a huge list of bad things being one of them; false affiliation and so on being another.

And I'm still comfortable with those being in the use case. The only thing that I'm intrigued with is the notion that if you could determine the intent at registration time to do any one of these bad things the way we've been just discussing I'd be okay with putting some policy or best practice in place to help registrars and registries combat that behavior.

But other than that I agree with the use case per se.

Greg Aaron: Thank you. James?

James Bladel: Hi Greg this is James and I just wanted to kind of chime in on a little bit of a response of what Rod was mentioning. And I keep coming back to this difference between a registrar and a hosting firm and many registrars are also offer hosting services.

But I think that the point I'm trying to make is that the difference between a registrar operation and a hosting operation is the difference between suspicion of intent and evidence of intent.

So, you know, you may look at a registration of a domain name and say that looks a little suspicious. But only when someone looks on the website and actually tries to deceptively or illegally solicit business across that website does the suspicion, you know, become something that can be proven.

And I think that one good thought experiment that might be useful in helping us draw these lines between use and registration abuses is that if we were to (unintelligible) imagine a registrar that had no web hosting operations. And simply just offered the registration of a name; you had to provide your own DNS services and hosting services. And how little discretion they would have in terms of intervening in some of these cases. I think that's a good thought experiment to help us draw the line between registration abuse and use abuse.

And when I think about can possibly result from ICANN policy that's how I'm picturing the impact on a registrar that has no hosting operations. So I'm on some cold medicine right now. I hope that makes sense but it's the idea that we continue to step over that line somewhat – or blur that distinction

somewhat, you know, freely. But I think that we need to keep that in mind as we discuss these topics.

Greg Aaron: Okay. Anything else James?

James Bladel: I think that's it.

Greg Aaron: Okay. So I'd like to make a proposal. Is there general agreement that this is mainly a use issue? Can I get a quick pulse check on that? Do you agree it's mainly a use issue you can use the checkmark. If not use the X.

Okay so we've got checks from myself, Berry, Faisal, James, Martin, Mikey, Phillip. Only one who hadn't voted is Rod.

Rod Rasmussen: Put a check down for me. I'm dealing with kids at the moment.

Greg Aaron: Okay so there is unanimous consensus it's really a use issue.

I have a proposal. In the report we've got a number of these kind of bad criminal things and that takes in this malware and a couple of other things.

I would propose that we discuss this topic in that context because they all share some similar policy issues and they could also be discussed – they could have similarities for best practices.

And I'm happy to also try to volunteer to draft some of that. We have some material on the Wiki about malware and botnet so we're going to need some – we need to write some techs about the – basically the criminal stuff and what intersections if any it has with policy.

So I'll have – I'm happy to volunteer to do that because I've been thinking (unintelligible) day. I'm happy to have anybody join me. We certainly need some material for this stuff in the initial report.

So if anybody'd like to join me I'm working on that. Please do let me know.

Mikey?

Mikey O'Connor: I didn't mean to do that but I'll join you.

Greg Aaron: Okay you're off the hook.

Mikey O'Connor: I'm not on cold medicine. I've got no excuse at all.

Greg Aaron: Okay. Thank you. All right.

So I think unless anybody else has anything else that covers sale of counterfeit goods. Our last issue is false affiliation and unauthorized use of logo.

So on our little spreadsheet we said false affiliation is a website that is falsely purporting to be an affiliate or brand and the consumer is to be harmed there. Unauthorized or improper use of brand or logo on the website can harm the brand owner.

So I guess again the first question we always ask is what are the policy dimensions and is this a use issue? So open that up for discussion. I think Martin is first and then Mikey and then Faisal.

Martin Sutton: Wow. I'm impressed to beat Mikey to the post there. But usage and that's all I'll say. Thanks.

Mikey O'Connor: Yeah I'm with Martin.

Faisal Shah: I guess it's my turn?

Greg Aaron: Yes go ahead (unintelligible).

Faisal Shah: I think that's right. I think it is usage. I think there's a couple of things I guess with false affiliation, you know, that the old, you know, putting in trademarks and metatags and whatnot I think that's part of it. And then actually usage within the website itself, you know, using a logo and displaying the logo within the actual page.

I think both – when you look at both of those it's probably both usage as opposed to registration.

Greg Aaron: Okay. And by the way in these definitions it doesn't say the brand name and the domain name because I guess that would be a cyber squatting issue. This is just what's on the website as far as I understand. Is that everyone's understanding what this is?

Faisal Shah: Yeah that's what I understand.

Greg Aaron: Okay.

James is next.

James Bladel: Yeah Greg actually that was exactly what I was going to say was the difference between having a distinctive string in the domain name versus having some logos or names on the website and that clearly puts us just over to the use side of the bench.

Greg Aaron: Okay. Thanks.

This is Greg. I'd also raised my hand. Yeah it seems to be a use issue, especially since cyber squatting has been discussed.

It also seems to me to be a dispute between two parties rather than necessarily a criminal thing. This seems to be more trademark infringement, that kind of thing. So that's for me an issue between two parties for them to figure it out.

Anyone else have any comments?

Faisal Shah: Hey Greg this is Faisal. Just something that would go is – just gets taken out completely or just go within the cyber squatting category.

Greg Aaron: I think our cyber squatting definition has to do with what's in the domain name string.

Faisal Shah: Okay.

Greg Aaron: Mikey?

Mikey O'Connor: Yeah this is Mikey. I was just going to chime in. This could go in along with all the other criminal stuff I suppose. But it's in some – I think your point is well taken Greg that in many cases this isn't necessarily criminal. It's a civil dispute.

So I don't know. I mean it could go in that chunk of the report that you and I just volunteered to write as an example I suppose.

Greg Aaron: I'm personally thinking – this is Greg – that it's not a criminal thing. Because when you're using somebody else's logo or that kind of stuff it seems to be a criminal – not a criminal but a civil thing. It's between the two parties. It's not something that you would ever get your district attorney to draw charges up on.

Mikey O'Connor: Yeah I think that's right.

Greg Aaron: Martin?

Martin Sutton: Yeah I think that's just important to recognize. We've got the important element of crime, et cetera sort of phishing for instance or the malware where there may be use of brand and domain names, et cetera, or within emails, within site content which takes it to that next level which is, you know, fraud.

This is simple brand issue elements I think here where, you know, you have to observe, respond as you see fit and that's down to brand owners.

There's no loops in here that would be worth pursuing I don't feel through any policy or best practice sharing within the sort of ICANN community as a whole.

I would suggest that we just mark this as out of scope, you know, looked at on which date but decided as out of scope.

Greg Aaron: Okay. So Martin's made a proposal to say this one's out of scope. Does everyone agree with that or have a different opinion? You can hit your checkboxes if you agree with Martin.

We have checkboxes from Berry, James, Martin, Mikey, Rod, and myself.

Faisal Shah: I agree as well. Somehow I got muted off but put me down as yes.

Greg Aaron: Okay so we're putting Faisal down for checkmark and the only person who hasn't voted is Phil. But looks like absent that we've got some consensus that it's out of scope. So we'll note such.

And that brings us to the end of the proposed abuses so congratulations. We've had a long list we've gotten through. We have met our goal for this meeting. So thanks everyone.

We are running a little short on time. We have about ten minutes left. I'd like to take that time to talk about the path forward. We do still have some work to do on cyber squatting, uniform year contracts but we can take those up next time.

Last week Marika and I were talking about the mechanics of putting an initial report draft together. And Marika we had all agreed would be at some point the kind of the keeper of the documents.

She also knows how to put it into the correct format which includes, you know, kind of a standard outline for these GNSO type papers with an executive summary and then discussion of various issues, recommendations, and appendices for additional materials.

These documents also have line numbers so as we go through we can refer each other to line numbers as we're getting into the process.

So Marika and I had talked and we were thinking that we're going to take all the material off the Wikis and she's going to start slotting it into draft documents. And we will have a draft to start working from in January.

So what this means practically is that we will stop using the Wikis for drafting. We're going to take whatever material is there and plop it down in the appropriate spots.

Marika is going to try to put material in proper spots. So she may need to rearrange some material or kind of standardize format a bit for readability. But her goal is always to preserve the intent and any important language of course.

So hopefully around January 4 which is our next meeting or shortly thereafter we'll have a rough draft. It'll be very rough. And there are some spots where we still need to do some work. But at least for the first time we will kind of

have a view of our whole thing and we're going to need to take January to fill in those spots where we think we still need to do work.

So does anybody have any questions about the process that we'll be undertaking in January?

Okay.

What I envision is there will certainly be spots that we're going to have to call attention to in our January meetings. We're going to have to do some intense editing. Marika will keep the master document but I am anticipating that a lot of us will need to do markups of various kinds. Not only pieces that we still have to write but also pieces where you suggest changes.

By late January we want to have that draft in much better shape so that means we will have to do some work offline. And then use the online meetings to work through any language that we feel really needs help. We also have to use some January meetings to figure out kind of where we stand. We have (unintelligible) or do we have (unintelligible) edits.

Marika did you – I see your hand raised. Why don't you go ahead.

Marika Konings: Yeah this is Marika. I just wanted to mention that we're in the process of looking at a better online tool that will allow for like live editing of documents (unintelligible) working group. But I think it might be helpful as well for this group.

Because in Adobe Connect we cannot do that. We can show documents and you can write notes but you can actually not do live editing. So if we have that in place that might be something that this group might want to make use of as well so they can collaborate on editing the documents during the meeting.

Greg Aaron: Okay thank you.

So to look at our timeline that's there on screen January 4 is hopefully the deadline of any other stuff that we need to write. There's major stuff. We want to try to get it done by then. That'll then give everybody in the group a chance to read it and make edits over the next few weeks.

Then have meetings on January 11, 18, and 25. By late January I'm hoping we have basically a master list in that document of all the recommendations that we might make. Those could be recommendations for all kinds of things.

At that point we may put up a poll using an online polling function and put up recommendations and maybe other sections of text up there. And this would be an opportunity for everybody to weigh in on whether, you know, they're comfortable with those or want to suggest additional changes. It's basically a temperature taking in late January to kind of figure out whether we've got consensus on some things or not or areas in which we need to have some final discussion and see if we can get to a consensus on various points.

Then shortly after that hopefully we'll have final drafted recommendations and we will have to then go through another polling process to tally up the levels of support. So in all of these working groups we have to basically give people a chance to say whether they agree or disagree, if they don't they can right up a minority opinion and we can figure out where all the members fall.

But consensus measuring – maybe voting isn't always the right term but that's kind of what it is.

We have to attach people's names to those opinions in the initial report. And then say whether it's a unanimous consensus or not, et cetera.

So then that's got to happen early February and the draft has to be finalized and posted out to the secretariat no later than February 12.

And then we go to the ICANN meeting in Kenya and then Marika I have a question. Once we publish the initial report when does a public comment period begin? Does it happen then or do we wait until after the Kenya meeting and the council's had a chance to read the report?

Marika Konings: Normally it opens straight away. But as for a meeting in Kenya and I think there's agreement that, you know, public comment period shouldn't start during an ICANN meeting. I think we could easily find out. Just (unintelligible).

Greg Aaron: Okay so do you think a comment period would begin in February or early March after Kenya?

Marika Konings: Probably March after Kenya unless we really want to start it beforehand and have it out in the public.

Greg Aaron: Okay, got it, okay.

And how long does the public comment period usually last again?

Is it 45 days?

Hello?

Did we lose Marika or can anyone else hear me?

Man: I can hear you.

Man: I'll bet Marika's phone did the hour and a half thing.

Greg Aaron: Okay.

Man: Dropped her off the call.

Greg Aaron: Okay, all right. Well that's okay. So we can follow up on that later.

So anyway I have us at 27 after the hour. So that's what we'll be up to in January and February.

Today represents kind of a major achievement for us. So I think it's a wonderful way to close out the year. And I'd like to thank everybody for closing out that list.

Certainly everyone have a wonderful holidays; some of you have already begun your holiday season. And really enjoy yourselves and have a great new years. We will pick up in early January.

Man: Thanks Greg.

Man: Great job.

Man: Thanks Greg.

Man: Thank you.

Man: Thank you.

Man: Thank you everybody. Take care.

Greg Aaron: Take care.

END