Registration Abuse Policies Working Group
TRANSCRIPTION
Monday 07 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 07 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-20091207.mp3
On page:
http://gnso.icann.org/calendar/index.html#dec

All recordings and transcriptions are posted on the GNSO calendar 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
Robert Hutchinson – CBUC
Martin Sutton – CBUC

ICANN Staff
Margie Milam
Marika Konings
Glen de Saint Gery

Apologies:
none

Greg Aaron: Okay. This is the RAP meeting for - excuse me, and we'll go ahead, now that we've got the recording going, why don't we take a roll call.

Gisella Gruber-White: I'll do that for you, Greg. Good morning and good afternoon to everyone. On today's call, we call James Bladel, Mikey O'Connor, Faisal Shah, Greg Aaron, Berry Cobb , Martin Sutton, Rod Rasmussen. From staff we have Marika Konings, Margie Milam, and myself, Gisella Gruber-White. And if I could please remind everyone to state their name when speaking. Over to you Greg.

Greg Aaron: Thank you, Gisella. Our agenda for today is to continue through the remaining issues for discussion, and then we'll move on to material we have on cybersquatting and uniformity of contracts. We will then review the schedule of our meetings leading up to publication of our initial report in the ICANN meeting in Kenya.

So first item on the agenda was offensive site/gripe site. The action item from the last meeting was that Faisal was going to draft some material for our consideration. So, Faisal, I don't recall seeing anything. Do we have some material?

Faisal Shah: You know, I don't - I didn't recall there was any draft something. I did do some research and talked to some people, and I could put something together based on that. But basically, I think it boils down to the fact that, you know, we talked a little bit about (unintelligible) between the free speech and whether offensive names, you know, even tied to brand holders for example would fall in the cybersquatting.

You know, after looking at it and talking to a lot of the brand holders, I think it does fall within cybersquatting to some degree, but I think there is a distinction. And I think the distinction has to be made that I've seen, maybe that - and maybe this is kind a where I might have been falling down last time or coming out last time, and that was that maybe what we're talking about here is purely just offensive words. For example, the Carlin-7 words and whether or not, maybe those names are of a type that just need to be, maybe even reserved as opposed to being allowed to be registered.

So, for example, dot US registry, and I took a look at some of the words, you know, the seven words, and it looks like they don't allow you to register those names. And maybe offensive words, maybe the seven words, you know, the Carlin 7 offensive words/dirty words, are perhaps fall outside the cybersquatting and maybe should be given different consideration than

maybe a name that actually even attaches to something else. Even though I think a name, even a dirty word that attaches to even something that is even more inflammatory is a problem. I'm not sure how we get around the whole cybersquat, you know, whether it falls within cybersquatting or not, I think it probably would get pushed there. So anyway that's kind of my thoughts on this issue.

Greg Aaron: So I have a question Faisal, this is Greg, it sounds like as far as if there's an abusive sense like you're proposing that there are two parties that are harmed, one of which is the brand owner, but the other, if there are seven dirty words, it seems to indicate there is a special harm about those, and somebody else is getting harmed - anyone who comes across them or sees them.

Faisal Shah: Actually, you know, I think I would put those in two separate categories. I think that's right, I think probably the more inflammatory category is just the seven dirty words that are offensive I'm not sure how we would get around putting a dirty word along with a brand and somewhat expect that it's not going to fall within the cybersquatting issues.

Greg Aaron: Okay, Martin had raised his hand and then James.

Martin Sutton: Thanks. I've been wrestling with this one in terms of how practical is it to segregate these types of domain names that are registered. One thought that occurs to me is that if you have any way of blocking explicit terms, the offending parties will actually just go to more easier names that people will get tracked into search engines so that results of searches come up higher. This is kind of like a swing of runabouts.

But is somebody is putting an expletive plus brand into a search engine, then they are presumably after something, whereas if they just put the brand in, they are probably expecting results suitable to that brand. So I kind of feel that these are lower risk whenever I've looked at offensive Websites,

because it is where people expect some unusual results, they're not expecting something from a well known brand.

So I personally would probably put the (tart) list under cybersquatting, and where that gives me grief then is the fact that there is potential consumer harm, brand owner harm and ineffective UDRP, really, because I wouldn't take anything like that to UDRP, I would try and just outside original. So I'm having trouble really thinking about practical ways. Even when you're talking about listing certain expletives as a blacklist, because then you're probably going to get some different languages, as well, as they come onboard and a different audience.

Greg Aaron: Okay. James?

James Bladel: Yeah, thanks, Greg. This is James speaking. And I think Martin made a couple of points that are noteworthy. And I just wanted to put out for discussion to the group, that we keep using the term words, but these are in fact text strings. And string can behave differently than words, because you can combine or attach these strings together and they can form words, because consumers in different languages are looking at the combination of a string to try to see if there is a word meaning in there.

There are a couple of famous examples that I won't bring up here where someone has very innocently tried to put together words in the center of that long string, they are recognizable either expletives or brands.

I'm also concerned a little bit with the idea of, as Martin said, that you know trying to keep ahead, not only of the different languages, but also the evolution, the continuous evolution of slangs and other types of pejoratives that might pop up over time.

And finally, you know, those are so easily gained by perhaps removing or substituting hyphens for vowels that the intent is understood pretty readily, but the idea of a black list is thwarted.

So I just wanted to put out the challenge of this problem and recommend once again that if there is a detectable brand and it seems to be intentional and being used in that (save), you know, I think we have a tool, imperfect as it may be, we have the UDRP that we can bring to bear on those situations and the other ones - I think that we start to go down the path of cleaning up the internet and I'm not sure that is something we want to be undertaking.

Greg Aaron: Thank you. Next is Mikey.

Mikey O'Connor: Thanks, Greg. This is Mikey. I just want to reiterate the concern that I've got that basically revolves around free speech, which is that anti-corporate or anti-brand speech is protected speech, and I think we're getting very close to that when we start talking about this. So I'm just stating again on the record that I'm against it. I'm fine with cybersquatting but I'm very uncomfortable indeed with legislating speech on the internet.

Martin Sutton: Martin here. Yeah, I think that's a good point. I kind of missed that on my list of items there Mikey. It in fact is a good place for brand owners to go to. So I often use some of those rank signs, because within there is sometimes hidden some valuable messages, which we take action on, either to correct something for a consume or within a system search, sometimes there are some little gems in there that actually work well for us. It's a shame that customers don't feel inclined to come to us first of all to talk through the issue, but sometimes it's easier just to have a bit of a rant.

And if consumers navigate themselves to those sites, they've navigated themselves there for a reason. They want to rant. And I'm quite happy with that. I don't want us to go down the route of trying to curtain free speech. I think where there is an issue where there are people taking branded

domains, adding some terms to that, and it doesn't matter in that context, but monetizing it so that they're peeling away at the back of brand owner's benefit.

And who gets harmed is not just the brand owner, normally it is the consumer in some way or another. And behind all of that, you've got registry, registrar and ICANN community, and the registrant, not really feeling any problem at all. It's all targeted in the brand owner and the consumers. And this is probably where I go back to the point that perhaps it should be parked under cybersquatting, but still with that caveat that it's ineffective for the mass problem of cybersquatting. It's ineffective.

Mikey O'Connor: Yeah, and this is Mikey. Just a follow-up on Martin's point. I agree entirely with that, and that's why I am so keen on using the sort of well trod paths of cybersquatting and UDRP and address this. I think when we get into the speech half, you know, legislating with words or even in (unintelligible) sometimes. I think we stray far away from usable tools, and that's really where I get uncomfortable.

But in terms of cybersquatting where a brand owner is being harmed and also the unsuspecting consumer is being harmed, I'm there 100%.

Greg Aaron: Okay. This is Greg. I'm going to go to Faisal and then I'm going to take the four first seconds. Faisal, go ahead.

Faisal Shah: Yeah, when I told them I agree with Martin, I just I made one distinction, and Mikey's talking about free speech, and I think that's right, but I guess the issue is really (unintelligible) word, I mean (unintelligible) versus, you know, some offensive. Again, I keep going back to the 7 dirty words with George Carlin, you know, putting that with a brand, which then I think maybe it's not so much gripe side, as it is something else.

But putting that aside for just a moment, because I think you do have an overlay of free speech, as Mikey is talking about and I totally get that, but what happens when you take an expletive plus Jerry's Kids, you know, or some other organization that is not a brand holder and now there is a different conduit to it, and maybe, what is the reason for that.

So I guess I just want to make the point, that I understand the gripe sites, I understand free speech. The question then comes in to what you - you know, you have these offensive words but what's the use of these offensive words in certain context. And maybe there's been one registry at dot US that said, look, we're just pulling out all those words.

I'm just throwing it out like to put it in the context of how we should be looking at it.

Greg Aaron: Okay. This is Greg. I mean US is an interesting example, because it's not an ICANN regulated TLD it's a CCTLD. It's one of the things that is structured from its government. And I don't know if New Star has to comb every domain name string to pull out or flag certain strings. I know that maybe they registered just those seven names, I don't know exactly how it works.

Martin Sutton: Hey, Greg, this is Martin. I might have just went (unintelligible), I don't know either.

Greg Aaron: Yeah, but anyway, but that's by-the-by. My two cents is I read an interesting article on domain names this morning, it was from an intellectual property attorney, and he actually the problem for him is that the UDRP decisions in this area are inconsistent and may not be evenly applied.

So it strikes me as one of those items that gets maybe slotted under UDRP, which is here's another example of something that might be examined by a UDRP working group.

Also, one more thing, which is I'm becoming increasingly aware of how close February is. We had some discussion on this topic last meeting, we've had some more now. I'm going to propose that we close discussion. What we really need is some background text and proposed recommendations. In other words, something in writing. So that's where we really need to go now that we've had some oral discussion.

Do I have a volunteer to write material by the next meeting?

Man: This is all regarding offensive words, right. That's what we're talking about this section?

Greg Aaron: Yeah, yeah. Offensive sites and gripe sites. So we need background material, which briefly explains the issue, briefly explains what we discussed and then comes up with draft recommendations. And then we can all add material, etc.

Man: Hey, Greg, if there's a way you could send me that article, I'd like to take a look at it too.

Greg Aaron: Yeah, I'll send it around. I send those links.

Martin Sutton: Martin here. I'd be happy to one up with you on that one.

Man: Okay, I'll put it together and send it to you and you can take a look at it.

Martin Sutton: Okay.

Greg Aaron: Okay. Can you deliver that to the group no later than Friday afternoon, so we have it for our next Monday meeting.

Man: I'll do that.

Greg Aaron: Awesome. Excellent. Thank you. All right. We shall move on then. Fake renewal notices. Mikey O'Connor had taken the lead on this one. So, Mikey, over to you.

Mikey O'Connor: Thanks Greg. This is Mikey. Thanks, Marika for getting the draft that James and I put together up in front of us. I'll just run us through this super quickly.

The first part is the definition that it's in our working papers right now. And then what we did is we summarized the conversation that we had last time and listed three sort of desired actions by the bad guys. One is to get an unnecessary fee or slam somebody into a different registrar without due notification, and then finally the pertaining credentials on domain on (unintelligible) codes to actually steal the name.

And I think that in general it's the middle result, this is really just a slamming kind of activity most of the time, but these were the three things that we talked about.

One of the questions that Greg posed in the call, was well, "What's the issue to ICANN?" And again, much of this is just summarizing the conversation that we had last time. We came up with three. One is that an inter-registrar transfer type of issue, sort of a deceptive practice. There could conceivably be a domain high-tech kind of thing. And the third is in almost every case, probably an abuse of the WHOIS system obtaining contact information inappropriately through WHOIS.

One of the questions that we raised on the call was, "Was well what's ICANN's role in all this?" And again, we concluded there are really two. If the perpetrator is a registrar or a reseller, then ICANN policy applies to them through the RAP or other consensus policy. If the perpetrator is not a registrar, ICANN still has a role, but it falls more into the inter-register transfer, hijacking or WHOIS abuse kinds of policy.

And then towards the end of our conversation we started discussing what we as the RAP, registration abuse policies working group ought to do about this. And we came up with several options. One would be to refer it to the RIA working group, if enforcement tools need to be added to the RAP. Another would be to refer this issue to the WHOIS working groups, because one of the things that doesn't seem to be clear is what the sanctions are for abuse of WHOIS.

It's against consensus policy and shows up in the RAP, but it is not clear who actually has to enforce it or who gets to enforce it. Another would be to refer it to the RRTP working group for the discussion around urgent return. And another was to refer it to the post-expiration domain name recovery working group when it touched on high-teching. And then the final option would be to simply keep this issue in a lump and refer it to the proposed (PDP) that we're going to suggest, the Registration Abuse (PDP), as a way to sort of keep the issue all in a bundle.

The concern that was expressed last time was that if we sent it off to the other working groups, we run the risk of it getting lost in the shuffle and perhaps because the old story of the blind people taking a look at an elephant. We are in fact in a way blinding people by doing this, because we give it very specific facets to be discussed by a whole bunch of different working groups, and it might be a good idea to keep it all in one place.

So I think the primary conversation today is probably to see where we fall amongst the disposition alternatives. I'll bring us back to that in a minute.

But then James and I went off and took a look at the Domain Registry of America. There was an interesting post on a blog that posted one of the letters that are now being sent by Domain Registry of America. And so we just wrote a little case study. I won't drag you all the way through, it just sort of puts in - you know, gives us an example of something to look at.

What they basically did is they send an email to the hapless domain registrant saying that they have attempted a domain transfer, which they probably have and the transfer has failed, because the registrant has no interest in transferring the name. So then they send the notice that says that it's failed, and then give the registrant the steps to make a transfer. If the registrant is naïve or just befuddled by this very technical sounding/official sounding email, they might be duped into transferring their name from their current registrar to Domain Registry of America.

Now DROA is in fact either a registrar or affiliated with a registrar named, Name Juice or Brand and Gray Internet Services. And thus they fall into that category of registrar or reseller and are presumably subject to enforcement actions from ICANN.

And so it may simply be that the tools are already there. I mean, if you read through this there are several apparent infractions that have to be investigated. Probably the most significant one is (unintelligible) of WHOIS. You know, it may just be that ICANN already has the tools that it needs to address this, and if this is a generalizable case there may simply need to be different enforcement actions.

So that concludes my report. I think that maybe what we do is having sort of a general discussion for a few minutes and then hone in suggested disposition and if we could come to consensus on that, I think we're pretty much ready to go.

Greg Aaron: First, thank you, Mikey and James for working on this. And the material presented by the way is going to be easy to insert into a draft of a report. So that's also very helpful. Thank you for that. I do see Marika's hand raised.

Marika Konings: Yes, this is Marika. I just have a question. You provide an example here of one registrar that is known to use these practices. My question is there any indication of how many complaints or actual cases of people falling for the

fake renewal notices actually happen. I mean, if (unintelligible) for example has sees how many people are coming back going well we didn't know, and we were tricked into this.

And have we checked with compliance to see if this an issue where many complaints are received which might give his mother a better indication as to what those complaints specifically are and identifying which category then, those that specifically fit or whether we see that indeed all those different areas might by applicable and worth pursuing.

Man: James, you want to take this one.

James Bladel: You want me to be a guide. Thanks, Marika, and I'm sure, although I haven't discussed this with our teams, I'm sure it's something with deal with on a continuous basis with spikes in activity whenever there is another wave of these messages would be filling out, similar to fraud or spam attempts.

One think that Mikey and I did discuss, and I don't know if it's supposed to be (unintelligible) called out here earlier, or may not be part of the DROA case study. But a lot of times these messages will not necessarily take a form of a request or instructions on how to transfer, but they will initiate contact via a fake past due invoice and threaten things like, you know, credit action or legal action against the registrant if they don't follow these stops.

So I think the method of communication and the style of communication, the way it's initiated, also plays a role here, because it can really use scare tactics to try to get these folks to remove the locks and cough up the authorization codes.

Greg Aaron: This is Greg. I've heard of Domain registry of America. This has been going on for a while to my understanding. Do we have examples of those kinds of letters or messages to registrants?

James Bladel: Mikey has an email here, but I think it would be interesting to also if we could scan some of the snail mail letters that they have sent that looked like the overdue invoices.

Mikey O'Connor: Now this is Mikey. I get them, but they come, at least to me, in a sporadic way. I'd be happy to save the next one that comes if one comes before the...

Man: I'm betting Google could easily provide us with one.

Rod Rasmussen: This is Rod, I'm not on the computer, but I could probably wallpaper my office with the number that we get all the time, so, I'm sure I can find one and scan one if you want an example.

Man: I agree with James. This case study was a pretty narrowly drawn one, and it was mostly because it was (PROA) was a topic of conversation on our last call, but I think it's a good idea to get examples of their forms of this activity. So it's not just narrowly cast at just one, because for sure I've seen those letter and they are quite intimating the first time you get them. I've also started getting them in foreign languages, which means I have to then translate them and translation is often rough and then that makes it even more intimidating. And so I'm sure there are lots of variations of this that we include in a packet.

Greg Aaron: Okay. This is Greg. I think Marika's and Faisal's hands are up, but those might be old.

Marika Konings: No, I just raised my hand again. Marika. Just briefly I quickly exchanged some instant messages with a colleague in the compliance team, and he actually indicated that he's not aware or he hasn't received any complaints in relation to this issue. But I guess that might not say much because maybe people don't, you know, complain about the actual fake renewal notice, but it might be, you know, a considered a hijacking of their domain name or other

issues, but on the fake renewal notice itself, apparently we don't seem to receive many specific complaints of such.

Man: That's interesting. I think that's an interesting question to add to the pot. Because just from the folks on this call, I know that this goes on a lot and it's interesting that nobody complains to ICANN about it.

Marika Konings: Well nobody, I mean, it was just, he said he wasn't aware of it, but I'll ask him if he can check and have a look, because they do track the complaints and see if they can provide some further details, if there are any. So I'll follow-up on that one.

Man: There is a great deal of discussion about Domain Registry of America on the various genuses of email archives going back to 2005, according to Google. I mean I see (Bob Connelly) for example talking about how this group has been - this is a quote, "...deceiving people for years. We've been a primary target. The FTC issues an order against them, etc., etc." Probably if we dig, I would assume there have been complaints.

Marika Konings: This is Mikey again. There have certainly been complaints to the FTC, because of the final injunction. It's interesting to me that ICANN is perhaps not perceived to be the right place to make that complaint, and I think it's a failing on our part. We should be receiving these.

Greg Aaron: Yeah, I've seen a lot of discussion about it. Like here is a conversation between (Chance Mitchell) and (Bruce Tonken) about it. I think what we should certainly do is let see, as we said, if we can get more examples of these letters, these posted letters. I'm assuming there would be some posted publicly, and maybe if we also have some individual letters. I would be surprised frankly if nobody had every complained about them to ICANN.

Marika Konings: Just to note, I'm not talking here in a historic sense, it's more about current complaints. So, I didn't ask the question if people previously or in the past

complained about this kind of behavior, so he might not be aware of that. So I will follow-up and try to find out whether, you know, this was an issue in the past and not anymore, or whether we're still receiving complaints or we never have received complaints. It might help inform us during the discussion.

Greg Aaron: Okay.

Martin Sutton: Martin here. Just quickly, I just did a Google search, just of fake renewal notices for domain names and there are quite a few registrars that have got warning and contact information if they need to report anything. So I'm just wondering if it's worth searching out from half a handful of registrars what sort of levels of complaints they get in directly and whether they feed those through or could feed those through. I think (unintelligible) but yeah, there are quite a few straightaway on the search results on Google.

Man: And the Net Register is also on there. It's a great letter there.

Martin Sutton: So there are some examples, but we probably haven't got any idea from that the quantity, and might be just as well to see input from a handful of large registrars for instance, just to see if they get much forwarded onto them.

Greg Aaron: Yeah. I see some evidence that at some point (DROA) was a reseller and registrars actually had to drop them as a reseller. So that's under the question of, you know, that's an issue if you have a problem with the reseller, should the issue get escalated to the registrar. Is the registrar responsible for what his resellers are doing, or is that the place to address it.

So Mikey, you had suggested that we think about these questions and try to come to some sort of a consensus. Would you like to continue to lead that discussion?

Marika Konings: Sure, Greg. This is a Mikey. If you roll back up just in front of the case study part of our little write up is where the list of disposition options is. And my

preference at this stage of the game is to keep this in a clump rather than split off the individual pieces of it and hand them off to other groups. I think this falls into the registration of a domain name and thus constitutes registration abuse.

So I think it would fit okay in the charter of PDP if we were to recommend it. And to sort of those two things that at least make me look to the last option rather than handing it off to others, but I think that's the conversation that we need to have now and once that's done, then take a consensus of the group as to where we're at.

Do you actually want me to run the conversation and look at Adobe Connect and stuff, Greg.

Greg Aaron: Yeah, if you want.

Mikey O'Connor: Martin's got his hand up. Go ahead, Martin.

Martin Sutton: Oh, sorry, that's an old one.

Mikey O'Connor: That's a left over. Anybody else got feelings about this that they want to throw out there or is my summary so good that everybody is in agreement.

Greg Aaron: Mikey, this is Greg. I have another option, which would be to put all those options out that you list under the dispositions and ask the council which way they want to go. That would be another way to do it.

Mikey O'Connor: Okay. I think if we were to do that, I would still like to put some editorial bias around that recommendation. Because we will have taken a harder look at it than the council will, so we might want to give them the list with the one that we favor if we can come to this. We've done that before. In fact we did it at (IRTP) a few times.

Greg Aaron: Okay.

Mikey O'Connor: That might be a way to do that. Because I agree, it would be good to give them a full array of choices, but at the same time I think they're probably looking to us, if we thought about it, to give them a suggestion. (Bob)? Oh, (Bob) is agreeing, I think. Sorry. My eyes are failing. Any other comments on this or are we ready to sort of take a sense on the group? I think we're done here Greg.

I think maybe the consensus of the group, if I can restate it, is we'll provide the list of options with a recommendation from us that we include it in the proposed (RAPPDP). And I'd be happy to take this draft back and run one more time through the mill and add on the results of this part of the conversation and come back next time with a draft.

Greg Aaron: And to clarify. There might not be just one (RAPPDP). If this was a discreet topic it might become a done (DDP). Because a (PDP) needs to have a very specific topic, rather than incorporating several. So the language, which Marika can help us with would be on that last bullet. Either you refer the various questions to other existing efforts or the recommendation will be that the council asks for an issues report, I guess, or however we're going to phrase it. And as we discussed last time, an issues report becomes the first step in a PDP process, if that's what the council wants.

Mikey O'Connor: Yeah. That works for me. I can take that action.

Greg Aaron: Okay.

Mikey O'Connor: Okay.

Greg Aaron: Awesome. Excellent work. Thank you.

Mikey O'Connor: Shuck thanks.

Greg Aaron: So I think one of the things that will happen is we've got good material here, we'll be able to pick this up, place it in a draft and an initial report and everybody will have a chance to read through that again at that point. But it sounds like a lot of this will just move over intact and that's great.

Okay, if nothing else on fake renewal notices, the next item is WHOIS access. I posted a note, as per our last meeting, asking the ICANN complaints department some questions about material they may have published in the past, and whether they have any statistics on access, and whether they have monitoring on who has accessibility.

And Marika, I know that you touched base with the complaints staff. Do you have any more information.

Marika Konings: Yes. This is Marika. They will get back to try to provide us with as much information as possible prior to the next meeting of the RP working group next week.

Greg Aaron: Okay, by next week? Okay. That's great. Thank you. And please express our thanks to them as they work on that.

Marika Konings: I will.

Greg Aaron: Okay. So it sounds like we'll get some more material during the course of the week and we'll take a look at that and come back to it.

The next item is domain pasting and kiting. We had a substantive discussion about that in previous meetings and Marika was going back and she had pointed out that we've got actually several different definitions. So we have some material upon on the screen now. And Marika, would you like to walk through that.

Marika Konings: This is Marika. Actually the material that's up is what Mikey and James edited. I think it's more detailed than what I shared. I just provided information on what was done in the context of the domain pasting working group, and I think this note provides more background. So it's probably better if it's Mikey or James that maybe run through this one.

Greg Aaron: Okay.

Mikey O'Connor: This is Mikey. The originator of the hallucinatory homework assignment, which I dragged James through, because we were sharing a Midwestern hallucinations and I don't know what we were thinking. Anyway, James, feel free to chime in any old time. What we came up with is in the first section sort of a summary of kind of a murky evolution of the term, domain kiting, which we just sort of tried to put a little historical background together.

And the next is the actual length of the various references, so there is a link to (Bob Carson)'s blog where I think that he was actually the first to use kiting, although in his blog post he was really referring more towards what we now call pasting.

Wikipedia then went ahead and came up with a post almost immediately after that and this next section is the current version of that post on the original one.

Message Labs chimed in a couple of weeks later back in 2006 with the notion of a disposable domain, so we really have three terms now on the table, and I also put the link in for the issues report on domain pasting, which has a section describing domain kiting in it. Finally, our definition is from the current working papers.

And then the next section, which is on the third page I think, it possible clarification. So we came up with three. First is domain pasting, domain kiting

and disposable domain. And then sort of in the same vein as the last little section, possible things we could do as a working group.

One would be to refine those definitions a bit, although I think there actually not too bad, they're just sometimes confused. And then the rest is summarizing the call, really. One thing that we thought on the call we might want to do is check with other working groups and see if there is definitions that we could use, and I tried to pull some of that out. And then the last thing that came up on the call was maybe do some research and see how widespread domain kiting actually is as a problem.

Greg mentioned on the call that he had taken a look at one of his registry data bases and hadn't found much, but it might be a good idea to broaden that research and perhaps form (unintelligible).

And then if in fact there is kiting going on, which is very much an open question right now, the final thought would be to perhaps use the accessibility policy as a way to address this.

So I think the questions in front of the group really are again right here at the end: What sort of things do we want to do as a working group. Greg, do you want me to do the call thing a good or do you want to run.

Greg Aaron: Well it looks like we have a couple of commenters first. We have James and then Marika.

James Bladel: This is James and I just wanted to extend my thanks and congrats to Mikey. He pulled this together almost like the last one and it was a second set of eyeballs going over it afterwards.

I wanted to point out that we did identify three rough categories of what we're characterizing under the umbrella of (AGP) abuse, pasting, kiting and disposable domain issue, which I have a lot of questions about, since I'm

fairly new from my perspective. But I should point out, or I think it's worth discussing whether or not existing excessive deletes policy covers all three examples. Because it essentially puts the registrar financially on the hook for any excessive deletes, regardless of whether it's coming from pasting, kiting or disposable domain.

Greg Aaron: I can tell you that it does cover it. The excess deletions policy doesn't distinguish widening of deleted or what they were being used for, it was just were they deleted in the add grace period. If so, and you exceed your minimum, then your registrar does get dinged for it.

Man: And if you had a lot of kiting then every time re-registered it every four days that would count against your excess deletions.

Man: Just to break in on this, I think the tricky bit would be if somebody was kiting across registrars. You know, they could spread that pain across a lot of different registrars. I think the place that we need to go to find out whether the kiting part is happening is the registry. And there, I don't think that the (AGP) would necessarily touch this as they hopped across 20 or 30 registries, and admittedly it would be a logistical nightmare, but you could conceivably avoid the HP abuse provisions by...

Greg Aaron: This is Greg. I mean I can look at it again pretty easily and then (unintelligible) info registry and tell if it's happened there.

Man: I think that would be very useful. And what would be really useful is if we could enlist (VeriSign) to take a look at that com real quick, because clearly if it's going to happen anywhere, that's the place. I don't know how amenable they would be to that, but...

Greg Aaron: I also see Marika's hand raised.

Marika Konings: Yeah, I actually was just going to make the point that, James and Greg, you made as well, that this seems to fall under the current (AGP) policy. And I also wanted to know if we were expecting an update to (unintelligible) policy I think next week or two weeks or so, I know it's in the process of being developed, so it might provide some further information on the policy and its effectiveness.

Mikey O'Connor: Marika, this is Mikey, is there any chance that we could influence that report in the remaining two weeks to have somebody take a look at some of the other registries, especially dot com (unintelligible).

Marika Konings: I think the report specifically looks at domain (unintelligible) and the (AGP). I don't think at this point this group could influence the outcome, but I don't think there is anything preventing this group to comment or make suggestions as to how the next version might include certain information that this group might feel is currently lacking.

Man: Okay, thanks.

Greg Aaron: Okay. All right. Well I'll mark that down as an item and Marika will bring us more news as info becomes available. Strike (unintelligible) I think we've now got some industry, kind of the industry standard definition of nailed down. Pasting has become the choice term and we understand that kiting is different. So I think the definition of the word is actually pretty straight forward and we've got it nailed down. Would anyone really disagree?

Okay. And if you'd like, what I can do, is I'll check in the dot info registry this week to see if we had any examples for what that's worth. That would be one registry.

Does anybody recommend any additional actions?

Mikey O'Connor: This is Mikey. Actually, Marika I think just came up with perhaps the one that we would want to recommend, which is that if the (AGP) working group is sort of monitoring the situation on an ongoing basis, perhaps what we want to do is suggest a minor expansion of their current monitoring to include kiting.

Marika Konings: Mikey, just to correct something. It's not the (AGP) working group that's doing that, it's actually ICANN staff that receives monthly reports from the different registries in which they provide data on the leads that have occurred over the course of that period.

So it's ICANN staff that is gathering that information and compiling the report. I think part of one of the requirements under the new policy I think is every three or six months an update needs to be provided to the GNSO Com so that they can actually assess how effective the policy is. So the comment it might still be relevant, but it's actually not (AGP) working group that is doing that work.

Mikey O'Connor: This is Mikey again. Then the definition of the data that is being collected is probably imbedded in the policy. Correct? In which case we might have to go so far as to recommend a slight change in the policy or is the definition loose enough that the staff could simply expand their data collection efforts without a change in policy.

Marika Konings: I would need to look into that, because actually I'm not that familiar with the policy as it was developed, so I can check on that to see, you know, what information is included there and how it was defined or staff assessment to decide which information might be better than another. I can look into that. I don't know, Greg, do you have further information, you know the registries are providing this kind of information to, you might have some more details on that.

Greg Aaron: Well, I have to provide ICANN reports every month and they list all the deletions and grace period by registrar and that information gets posted on

the ICANN Website with all the other registries reports. But why they're being deleted or for what reason, I don't have any insight into that.

Mikey O'Connor: Greg, this is Mikey again. Do you have to provide the actual domain names that get deleted or just the summary.

Greg Aaron: Just the summary.

Mikey O'Connor: So if we were to try to track down kiting, the data the staff gets today wouldn't contain...

Greg Aaron: It wouldn't tell you.

Mikey O'Connor: So never mind. Sorry about that.

Greg Aaron: Okay. All right. So anyway, the document that we have up on the screen right now actually contains excellent material. I think that would be ported over into the initial report draft, as well. Do we need any additional discussion of it at this time. Like I said, I'll go and try to do some kiting research this week in my registry. But do we want to move on in the meantime to the next topic?

Okay. Not hearing any other opinions, so if not, what I'd like to do is move onto the stolen or fraudulent credentials.

The issue here is basically criminals using stolen credit cards and identities to sign up domain names. As we discussed last time, this is a way of looking at the malicious conduct issue. And the question was, I think from the last meeting, I think first question is it in policy making scope. We know that criminals do this, they do it every day. But the question is is it something that I can do something about? Is it within policy making scope? What are some of the issues involved? What came up last time was can you make registrars adhere to certain credit card validation processes for example.

I want Rod to weigh in on this one, because he's been interested in the topic. I also see James' hand raised. James, you want to go ahead?

James Bladel: Yeah, Greg, thanks. This is James. And I just wanted to weigh in on it, but this is entirely outside the scope of ICANN policy. You know, credit card validation and monitoring stolen credentials and thinks like that nature are going to be imposed and enforced by the bank or the other credit card merchant account for other relationships that a registrar may have outside of ICANN.

While certainly I agree that this is a problem, I think that it effects different models of registrar businesses different ways, The question assumes that there is a registrar that has retail oriented market focus and is accepting credit cards with a default method of payment, when in fact the registrar could be a guy with a roadside tollbooth accepting shiny beads in exchange for domain registration. I mean it really presumes quite a bit of other registrar business models and business practices to suggest this is somehow within the scope of ICANN policy.

Again, not saying this isn't a problem, just inappropriate for this particular venue.

Greg Aaron: Okay. Thank you. I see Mikey's hand raised.

Mikey O'Connor: I'm looking at the document that's in front of us and it says, use of stolen of fraudulent credentials at the bottom of Page 2, and I'm wondering if we've gotten ourselves sidetracked on the credit card issue. It doesn't say credit card credentials, it says credentials, which could mean stolen account credentials at the registrar. And I'm just curious if we've got a definitive word on that or am I looking at the wrong place.

Because I think James is right. In terms of the business process of collecting money and credit cards, that is pretty variable across a lot of different

business models. But I think that to the extent that it's stolen credentials from a registrar that's being used to facilitate is likely hijacking. But that is within the scope. But I'm just not sure what those - it's an awfully short bullet, so I need re-education on that, I guess.

James Bladel: And Mikey, just real quickly, this is James, I would say that my objection was in terms of scope was to either of those being included within an ICANN policy. Just because the stolen credentials presumes that the registrar is operating some sort of a domain control panel, when in fact maybe their interaction with customers is via (unintelligible) or phone or possibly even a dedicated client that clients download and it's all in their machine.

So it just assumes too much and it's delved a little too deeply into the internal workings of registrar and it doesn't necessarily take into account all the variety that is out there in the registrar ecosystem.

Mikey O'Connor: This is Mikey again. Just to push back gently on that second point. Now I can remember when we did this all by email and it seems to me that you can steal somebody's credentials irrespective of the mechanism by which the credentials are being used to validate the transaction. And that to the extend that's what our definition is all about, I'm not sure I buy that last argument.

Again, I'm not sure I feel terribly strongly about this, because it's illegal and it may not need ICANN policy, but I'm not sure that I've got a good sense of what we meant when we wrote that bullet down.

Greg Aaron: This is Greg. Maybe one way of saying is that there is the stolen credit card issue, stolen identity being used to register domain. Mikey, I think you're also raising issue of somebody getting into somebody else's registration account as a registrar.

Mikey O'Connor: Or not. It could be that it's not - to give credit to James' point, that's one way to do it, but in the old days there weren't accounts at registrars, they were just

emails that went back and forth and if you could present the right credential, you could steal it.

Greg Aaron: But to me it represents either it's a hijacking issue, which has other solutions, or it's a data breech issue at a provider. But I don't know if that's a scope for ICANN to get involved in either.

Mikey O'Connor: Yeah, I agree. So I don't' want to belabor this one. This is not one that's real high on my hit parade, but I just wasn't clear what exactly we were trying to go after. Presumably this list came from people who put things on the list. It does sound like the person who put this on the list is on the call, would begin saying well, this is what I meant. Does anyone remember why this one got on the list.

Man: Perhaps issues report.

Martin Sutton: It's Martin here. Well what we did in the outset was just to list as many different types of issues for domains, registration of abuse that was recognized. So there was a lot listed down in the first instance. But with a caveat that as we go through it, we've got to decide whether they actually form part of the scope of this team or not. And it was better to put more on there and whittle them down rather than forget some.

I mean, thinking back on this particular one, we see a lot of issues in terms of domains registered using fraudulent or stolen credentials, because this goes back to WHOIS issues, it goes back to the point that most of the fraud or unwanted activities on the internet are going to be hidden behind stolen credentials.

Now I'll probably labor on this point again, but if you look at the situation, this is where consumers get harmed. If there is a brand involved, and it doesn't have to be in this particular case, there is potential for brand owner harm, as well, but the primary one here is consumer harm.

Behind the scenes, there are volumes of these domains registered where the registry registrar take no responsibility for like, apart from say in their policies this is what you should use for legitimate purposes, etc., etc. But there is so much activity that just allows us to go on. Where if there was prescreening or simple mechanisms that may be unwanted I would imagine by this sort of registry-registrar community, that would actually insure that who is actually registering a domain is who they saw they are and they are using credit cards for instance that belong to them. There may be a process which takes a few days before the main name goes live.

So I know some of those have been cited in the past. So I think that's where the use of stolen fraudulent credentials came from in the past.

Greg Aaron: Yes, and it's the vector by which a lot of undesirable activity takes place. The harm of course also is not only to consumers but also to the institutions that they have to absorb some of those losses, is that correct?

Martin Sutton: I would expect so. So perhaps there is an issue here. You know, for registrars in particular, where there is a cost of doing business here that on its own may not be a particular huge problem the registrar, but altogether in the registrar community it could be a quantitative problem. I'm not sure how much of that information is shared, if at all between registrars.

Because I'm assuming the domain is once they are recognized as problematic and whatever activity was running on the back of it has been switched off. These domains just float around again waiting for people to either pick them up through automatic methods or just to delete off at some stage.

Mikey O'Connor: This is Mikey. Martin has dragged my needle up a little bit with his comments. I'm fairly ambivalent about this one, but I would hate to just dismiss it out of hand, I guess, but it seems like, the point that's being made here is a really

good one, which is if everybody is aware that it's going on and nobody is really doing anything about it. And a lot of people are being harmed, as well, then that's the topic for the conversation.

James Bladel: Mikey, this is James. Sorry Greg.

Greg Aaron: I was going to recognize you. Go ahead.

James Bladel: Yeah, I just have issue with the idea of nobody is doing anything about it. You know, as you may have imagined, we have a very large and dedicated staff working on this 24/7, and that is of course at our cost.

I have no idea what the traffic level is in these types of incidents, but I know that the feasibility of making each of these somehow governed by an ICANN policy and getting ICANN involvement in some of the positions, it has to be really in minutes, according to our procedures, is probably un realistic.

You know registrars have to be very mindful of this if they are going to offer registrations and accepts credit cards as a meth of payment. If they do not, their banks or their Websites or probably their customers' attorneys will make sure they are not a registrar for very much longer.

I don't really know that this is - I mean for example, one of the most common or frequent ways to reach a registrar is to steal someone's free email account credentials and Yahoo and Google and then to request a password change.

This is a very simple process, however, I don't necessarily hear a lot of calls for, you know, ICANN needs to get involves in how Google manages their internal password controls or Yahoo. So I'm just kind of pointing this out here that this is a problem, it is something that I think registrars take very seriously and at their own costs. Like major investments to thwart and control these issues. But turning them into anything that is either monitored or requires

involvement by ICANN I think is going down the wrong path and doesn't lead us closure to a solution, just complicates the matter.

Martin Sutton: This is Martin here. And I probably agree to a lot of what you said there, although I would point out that within this, it doesn't necessarily mean policy changes, it may be recommending best practice or minimum standards perhaps. And you may well surpass what minimum standard could be potentially recommended. I'm not sure.

I'm just trying to make sure that we don't lose sight of the fact that this is probably a big problem, but because it's all bitten down into little chunks between registrars, between registries, it may not appear a big headache, but the community at large and ultimately the consumers, they're the ones effected the most. We probably just chip away at things just to manage the cost levels and the risks as best we can. But I'm just wondering if there is more potential work to be done in this space. I would suspect that because of the low value linked to domains that most of this stuff just gets washed away as the cost of doing business. It doesn't get recognized as fraud.

If there is a problem with a domain name that has been registered with a stolen card or whatever, this probably just goes down as charge backs, either through to the registrar or to the issuing banks. I think it's a very difficult one to get an idea of the scale, because there is no real information that we can tap into on a collective basis.

James Bladel: Mikey's ahead of me, but I would like to respond to Martin when you get a chance.

Mikey O'Connor: Why don't you go ahead James and then I'll throw another one out there.

James Bladel: Martin, you're absolutely right. This is an issue and this is something that the registrar and internet users and the company, again we are very committed to working through. There are a variety of other groups that we are involved in

that have made this area its primary focus, full force, information sharing. And for the development of best practices and coordination of different efforts across the spectrum of registries and registrars, I think I noticed a couple of votes on this particular call are also involved in those groups, as well.

So my strong reluctance to even discuss this issue within the form of an ICANN meeting, is not and shouldn't be seen as any, you know, discounting or dismissal of the scope of the problem, it's just it is something that we are very focused on addressing through other forms and other venues.

Mikey O'Connor: This is Mikey. That's actually what I was going to mention that as this conversation progresses, I was reminded especially the conversations in (IRTP) and post-expiree domain name recovery. We have been talking about that, and I'm not sure that means we can't speak about it here.

I think what it means is we would want to speak in such a way that amplifies and reinforces what's going on in those other working groups so that we aren't putting its banner in the works. But that's a different posture than out of scope for ICANN altogether. And so I'm warming up to the idea that we at a minimum out to do something along the lines of referring this to some of the other working groups.

The trick here is that both (IRTP) and post-expiree have slightly different focuses. (IRTP) will only look at it if it's a transfer of cross-registrars and post expiree domain name recovery will only look at it after the domain has expired.

And so it's a problem, especially if we're expanding the term credentials beyond credit cards, making it credit cards and account credentials at the registrar, I'm thinking that this is something that we can talk about.

Rod Rasmussen: Can I get a word in here. This is Rod. Unfortunately, this meeting has been timed for me, and I've been only to listen to the last 20 minutes in my drop off schedule of kids and all that.

Credentials, just to respond to Mike's last comment here, has chosen very carefully to not exclude things besides credit cards. In other words it's much more than credit cards. Credentials is legal for access credentials in particular or anything that can be used. Credentials have legal meaning and they can mean lots of things as credit cards. In this context, to explore some of those, you've got credit cards, you've got account credentials, and you've got email addresses and email accounts that are being used for various reasons. You've got identities themselves. You've got a lot of victims of identity theft involved in these kinds of registrations, so there are lots of different aspects here. So I think we've gotten maybe a little focused on one aspect of this whole issue.

And I would propose - I've got a lot to say in this, way too much to say in the next nine minutes. Let me put together some terms around this. But I think where the ICANN policy for ICANN involvement is not running a program saying we're going to screen credit cards for registrars. I think ICANN has a lot of ability to do things and helping with framing the problem, setting minimum stands, making sure that the issues are understood by all registrars and people involved in the registration process, not just those who are really doing a lot already.

Where we find the most problems are in people who aren't the ones on these calls from these meetings, but ICANN as a central body has a real sway in how those companies/organizations run their operations in the end. And there's a big hammer that could be used there if there are people who are basically just not paying attention to who is registering what to what purpose. That's my quick two cents.

Greg Aaron: Okay, Rod, it sounds like you're volunteering to write text for the group to consider.

Rod Rasmussen: Yes, absolutely.

Greg Aaron: Okay. Do you think you'll be able to deliver that this week.

Rod Rasmussen: Yeah, I'll endeavor to get that done this weekend.

Greg Aaron: Okay. Awesome. We have about eight minutes left. Let's take that as an action item and that will go up on this list. When it does, we should also of course feel free to discuss other lists, as well. All right if we have anything that's left, what I'd like to do is go back to our agenda and we're going to have to skip over cybersquatting and uniforming of contracts for now.

However, discussion of those topics is available on the lists. Berry had set up a draft of uniformity of contracts, background and recommendations. I set some personal comments up on that the middle of last week, so that's up.

I would suggest if you have not yet read those, please do so during the course of the week, that's important material I would like to see everyone's comment on the current status of those drafts.

Of course time is getting short for our initial report, if you don't comment now, we're going to have very limited time for you to comment in the future. I would like you go get you substantial comment out sooner rather than labor. So please comment on those documents on the list.

Speaking of schedule, of our remaining meetings, we have one meeting December 14, the next meeting after that will be December 21, which is the week of Christmas.

I'd like to poll you guys as to whether or not we should have a meeting that week or whether it's possible given your vacation schedules. So if you could, go to Adobe. And if you can make a December 21 meeting, please put a checkmark up there.

Rod Rasmussen: Consider this a checkmark for me there, Greg, this is Rod.

Greg Aaron: Okay. Okay we've got Greg, Marika, Berry, (Bob), James, Mikey, Martin and myself could do it. So that's almost everybody. So let's pencil one in for December 21. I'm glad at least most of us can make it. I think we're probably going to need that time. So let's pencil that in. Then we've got four meetings in January. January 4th is penciled in as a deadline for all text.

Okay, so we've discussed many topics over the months. The goal is that we have text which includes an overview background and draft recommendations for each of those topics.

January 4, is the point where we think Marika takes all that and does it into an initial report document. Then what we're going to have to do is go through that document and make additional edits and tweaks, and we have to have it processed to discuss the recommendations specifically.

What we have to do is kind of figure out where we all stand, how close or how far apart the opinions are on those recommendations. You know, walk them through, see if we can jell into consensus on as many as possible. And then at some point in January we will have to go back through and measure levels of consensus again.

Basically, we have a deadline of 02/12/09. In order for anything to be discussed at the ICANN meeting in Nairobi, Kenya in early March. Everything needs to be received by ICANN and posted no later than the 15th, which is a Monday. So if we're going to have our initial report done like we promised, we

really have to have it done and sent into ICANN on February 12, that's our drop dead date.

So what I have right now is four meetings to go through the initial report. We may have some - you know, Marika and I have been discussing some ways to do some polling off-line, especially on the recommendations to measure where we are initially and then do a final tallying of the levels of support and get everybody's name stamped. So we'll need to do some of that in meeting, we'll do some of it probably in a poll format, which will let you look at everything also at your leisure off the conference calls.

So I think we're coming down to the nitty-gritty here. If we want some text on something, it really needs to be written within the next four weeks. And again, January 4th deadline hopefully is not an initial drafting of something, it's something that's been put out there at least for the group to comment on, like we've been doing with uniformity of contracts.

So we're coming down on the nitty-gritty. We're running out of time to discuss issues. We are coming into a time where we need to discuss the specifics of what we are going to say in the report.

So, again, this is where the rubber hits the road. We need text to be developed. If text is not developed on a topic then it may not make it into the report.

So that's kind of where we stand on the schedule. Does anybody have any questions about what's going to be happening over the next two months? Marika, do I see your hand up.

Marika Konings: Yeah, this is Marika. I just had a question related to our previous discussion on having a call on the 21st of December. I just want to know if I can give that meeting as a deadline to the compliance team on the WHOIS issue, so they

have a little bit more time. My initial assumption was that next week would be our last call before the Christmas holiday. Would that be okay?

Greg Aaron: I would like to keep the ICANN staff on the schedule they agreed to, if possible. Once we get the material, we still have to digest it, see if we have any follow-up questions and then discuss in the group what it actually means.

Marika Konings: Okay. I'll leave it on the 14th.

Greg Aaron: That would be great. Any other questions or comments? All right, well that sets our meetings through mid-February. Thank you for your discussions today on these topics. As always, I'll send out the action items for follow-up this week. Thanks again for a good discussion. And if no other comments, we'll close the call and reconvene next week. Thank you.

Mikey O'Connor: Thanks, Greg.

Martin Sutton: Thanks, Greg.

Greg Aaron: Thank you everyone, have a good week.

END