Registration Abuse Policies Working Group
TRANSCRIPTION
Monday 12 October at 14:00 UTC

Note: The following is the output of transcribing from an audio recording of the Registration Abuse Policies Working Group meeting on Monday 12 October 2009, at 14:00 UTC. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but **should not be treated as an authoritative record. The audio is also available at:**
http://gnso.icann.org/calendar/index.html#oct
All recordings and transcriptions are posted on the GNSO calendar page:
http://gnso.icann.org/calendar/index.html#oct

Present for the teleconference:
Greg Aaron - Registry C. - Working Group Chair
James Bladel - Godaddy Registrar C.
George Kirikos - CBUC
Faisal Shah - IPC
Rod Rasmussen – individual
Robert Hutchinson
Martin Sutton – CBUC
Roland Perry - Individual
Philip Corwin – CBUC

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

Apologies:
Mike O'Connor - CBUC

Coordinator: This meeting is now being recorded.

Greg Aaron: Thank you. Well let's begin with roll call for those on the phone and on Adobe Connect. If at all possible please do try to join both.

Gisella Gruber-White: I'll do the roll call for you quickly. Greg, it's Gisella. Good morning, good afternoon to everyone. On today's call we have George Kirikos, Roland Perry, James Bladel, Greg Aaron, Martin Sutton, Faisal Shah, Rod Rasmussen, from staff we have Margie Milam, Glen

DeSaintgery, Marika Konings and myself Gisella Gruber-White. And we have apologies from Mike O'Connor. Thank you.

Greg Aaron: Thank you Gisella. All right well today's agenda is as follows, we're going to get some updates from our subgroups, cybersquatting, contracts and spam/phishing malware. We're then going to discuss the Seoul meeting. I'd like to get an idea of who's going to be there. And we have to provide an update to the council so we'll talk about that today.

Today I'd like to start by talking about the cybersquatting group. Two meetings ago we kind of discussed a way forward since there was little to no progress being made in this group. One of the questions that came up was, are we really talking about inadequacies of UDRP for example. So I want to either make some substantial process on this topic or stop talking about it because it's been going around in circles for a while.

James, you had evidenced some interest in the past in this group. What do you identify is the way forward?

James Bladel: Hi Greg. Since our last meeting we kind of decided that George Kirikos and I would go off on our own and see if we couldn't come back with something that was palatable to the group at large and if so we would check this box if it were and just move on.

So that's exactly what George and I have done since our last call. We met once via telephone and a couple of email exchanges since then. Where we are is that essentially that for defining cyber-squatting we should stick to the definition as outlined in Section 4(a) and 4(b) of the UDRP.

Now there are some - there was some discussion about borrowing from other areas as well. For example the - I believe it's the Anti-cybersquatting Consumer Protection Act, ACPA. There were some issues involved and borrowing from other legislation, first of all, it's jurisdictionally specific.

And secondly it seemed to be a bit unbalanced, for example, if we were going to borrow from one side of the definition we should also borrow from those areas that tried to outline what constitutes fair use or, you know, lack of bad faith. And George posted some sections from the ACPA to that effect on the list.

Finally I think the third point is that, you know, any - if we are going to point a finger and say that the UDRP needs to be updated, revised, refined or, you know, modified in any way then that needs to be a separate question that this group can discuss whether or not recommendation for a revised UDRP should be made and that should follow the prescribed PDP process as they currently exist rather than trying to piggyback it into a cybersquatting definition or anti-cybersquatting PDP.

So those were the three main points that George and I arrived at. And, George, please if I've left something out or misstated your position on something please jump in now.

George Kirikos: George here. That was perfect.

James Bladel: Okay. So, the three takeaways that we had Greg -- one, we should, unless we have a compelling reason -- we should stick with the UDRP definition of cybersquatting which is Section 4 of the UDRP policy.

Secondly, that any attempt to borrow from other language or other documents or other procedures or proceedings or legislation has to be balanced; it can't grab all of the components of UDRP - or I'm sorry, cybersquatting and then not grab the components of fair use or, you know, things that would not demonstrate that faith.

And then thirdly that any attempts to refine, reform or, you know, reconstruct the UDRP has to go through a separate process in its own right because there's a whole host of different interested parties besides those - just those on cybersquatting.

Greg Aaron: Okay. This is Greg. So as far as Number 3 is concerned the recommendation is if folks are interested in UDRP discussion it would obviously need its own PDP because that's a very complicated topic. Are you also saying that this group should not make a recommendation about UDRP?

James Bladel: My personal opinion Greg is that we should not. This is James speaking again. However leave that to the consensus of the group. I certainly could be in the minority on that - in that respect. But I feel that, you know, if we're starting off with an issues report going to council and requesting the PDP on its own merits as opposed to, you know, bundling it with existing efforts.

Greg Aaron: Okay, thank you that was very clear. Okay I'd like to open up James's comments to the larger group. Does anybody have any questions or comments? Fazal?

Faisal Shah: Yes, so James, let me just see if I understand; are you saying basically that we're just going to pull out small five and small six as evidence of that page in connection with the definition? Is that what we're talking about here?

James Bladel: Are you talking about the UDRP small five and small six or...

Faisal Shah: Well (unintelligible) and what I'm looking at here in terms of what we've put together, I guess, in our discussions. You know, we've had small one through small - or small one through small four that (unintelligible) faith and then small five and then small six are - come from the ACPA. Are we saying that in terms of how we're moving forward are we just pulling those two out as evidence of that faith and everything else pretty much is the way it stands right now?

I mean I guess I'm trying to figure out what the - where we're going from here.

James Bladel: Yes, Fazal, I think I remember you're referencing the email threads between yourself, myself and Mike Rodenbaugh from September. Is that...

Faisal Shah: Yes.

James Bladel: Okay let me pull that up real quickly here and reference those. I think that you are correct and I think that Mike made a pretty effective case that those elements are key into what's considered by a UDRP panel - panelists or a UDRP provider.

But I think that one of the questions that we had was whether the differing providers defined them consistently or there were room for interpretation within the different providers. So I’m just trying to pull that up and speak at the same time so I apologize if I'm rambling a bit here but I'm trying to kill for time.

But for the most part, yes, I think that if we're going to pull up those additional sections of the - of the ACPA or any other areas we should probably, one, make sure that they are, you know, very tightly and uniformly and consistently applied and I don't think that we can necessarily always say that with the UDRP providers.

And secondly, I think, George, if you want to post a link to the area also from the ACPA that balanced those three parameters; I think that those are also unnecessary (unintelligible) and those would kind of go hand in hand. So I don't know if that answers your question specifically but I think that once we started to go outside of the UDRP we had to be very careful that we were - that what we were bringing back into the definition was both uniformly applied and had its corresponding counterbalance.

Faisal Shah: Okay.

James Bladel: So I guess we didn't just throw them overboard, we looked at those as well and tried to find where they were linked to as well in other parts of the legislation. And I think George has that up now.

Faisal Shah: No, the only thing I was saying is what a, you know, examiner is looking at whether something is the cybersquatting domain name or not. But you look to whether or not the registrant has registered other names, you know, like for their own personal gain or for their own commercial gain, you know, like names that have to do with Nike and have to do with Yahoo and names that fit there that should not be used for their, you know, I guess their (unintelligible) for the intent - their intent of selling it back to the owner or whatnot.

So that - and I'm just (unintelligible), you know, in terms of (unintelligible) six, those are the kinds of - those are the things that we look at. And I, you know, I'm just trying to figure out if there - if you've got (unintelligible) ways of actually improving the sections as opposed to the - like you said, James, you know, just throwing it out.

Greg Aaron: This is Greg. I have a question. Are patterns of past behavior like that listed as criteria in the UDRP? I mean I guess they're used as evidence of bad faith right?

Faisal Shah: Right so it's not determinative, I mean, it's not something that they'd say, okay, absolutely this is what's going on. I mean, that's why, you know, those services that some of the companies provide like reversing with that provides all the WHOIS information regarding what other domain names are owned by particular registrants; that can be really important because it just shows that there is that pattern.

And they are, you know, accumulating domain names that clearly aren't names that they plan on using themselves (unintelligible) but these are names that they are going to use for personal gain by somehow trying to leverage them. So I guess to some extent, yes, I think that it is - there is a pattern that's looked at but it's not the thing that they look it, it's just one factor.

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

George Kirikos: Yes, I just wanted to point out that the existing UDRP actually does say provide that you have engaged in a pattern of such conduct in 3-2 demonstrating bad faith. So it is kind of already there it's just that, you know, taking the language from the UDRP - sorry, from the ACPA without any counterbalancing measures would be very problematic.

James Bladel: Okay.

George Kirikos: As I demonstrated in the link that I posted.

Greg Aaron: Okay. And I see James's hand.

James Bladel: Yes, and I think that, you know, Fazal and certainly open to other opinions on this but, you know, one of the things that George and I set out to do was to try to separate those elements that would clearly come down hard on the scales and cause someone to lose a UDRP versus those things that would constitute a very narrowing type definition of cybersquatting.

So for example if I went out and got a single - one single domain name that fit the parameters described here in the UDRP I would still be a cybersquatter, you know, even though I did not necessarily have, you know, a whole portfolio of domains that met that criteria.

And in the latter case, you know, that would certainly expedite my loss of those names through the UDRP but wouldn't necessarily add a whole lot of value to the definition. And I don't know if that makes sense; it's a pretty subtle distinction that we were trying to uphold.

Greg Aaron: Okay. Thank you James. This is Greg. So I have a question. I would like to drive this towards some sort of a resolution. What I've heard so far is that, you know, this whole issue of cybersquatting has been raised as a potential abuse.

The conversation does keep turning back to UDRP. Other than UDRP are there any recommendations that this group wants to make regarding cybersquatting? Let's put aside UDRP for a minute and we can come back to it as James and George have said that UDRP conversation may need to take a separate path.

But other than UDRP are there any recommendations that this group or anyone in the group wants to put forward regarding cybersquatting?

I'm not - James, is your hand up?

James Bladel: Yes, yes.

Greg Aaron: Okay.

James Bladel: New hand raise. And to answer your question, Greg, my personal opinion is that stepping away from this subgroup a little bit and speaking as an individual I believe that UDRP is a tool and probably the most appropriate tool from a policy perspective to address cybersquatting although registries and registrars may be doing things on their own as well.

But from a policy perspective the policy exists and it is appropriately applicable to cybersquatting. Now whether we want to discuss the efficacy of that tool and whether or not that tool needs to be sharpened or maintained or revised to keep track with, you know, current practices and things like that I think that that is definitely one of the recommendations that this group can make.

But I don't think that it's - at least from my perspective I don't see a large demand for a new set of tools.

Greg Aaron: Okay. So if I may, your statement is that UDRP is the tool that is used to deal with the issue? And the recommendations about its efficacy is, you know, something that could be possibly discussed. But you yourself are not recommending other (unintelligible).

James Bladel: I'm not -- yes, that's correct.

Greg Aaron: Okay. Martin?

Martin Sutton: Hi, thanks. Yes, I think that's a good point actually raised by James in terms of how efficient it is. I must admit personally I use it as a - the last resort really. I think the problem here is that there is masses of it out there troubling brand holders that we can't take every case to UDRP so some very rare occasions I'd even bother going to that expense.

So there is a massive abuse out there that exists which goes untreated. So I suppose I would like to see something else beyond UDRP listed as an area to explore. But I don't have the answer.

Greg Aaron: Okay.

James Bladel: Greg, could I - this is James - could I just respond to that really quickly or I can -

((Crosstalk))

James Bladel: Martin, I think you're correct but I think that that type of work can be achieved through any future revision of the UDRP if you're saying that, you know, as a last resort because it's too long, it's too expensive, it's too fuzzy and its outcome or things like that, I mean, those are things that could be cleaned up in a revision of the UDRP rather than creating a new policy. That's just my response to that.

Martin Sutton: That's fair enough, yes. No I agree with that.

Greg Aaron: Okay. I'm sorry, I guess - I think Fazal was next.

Faisal Shah: Yes actually I just wanted to echo what Martin was saying in fact you took the words out of my mouth. And I think the UDRP is expensive and it is - it falls short of being an effective remedy. And I think that, I mean, I think we have to talk a little bit, I mean, (unintelligible) should be, I mean, there'd have to be other tools or maybe there's ways of coming up with those tools.

And I don't know if this group - it's about coming up with those tools but recommending that maybe there's other ways of handling the cybersquatting problem in addition to making the UDRP more effective. So I'm kind of coming alongside Martin on this.

Greg Aaron: Okay. George?

George Kirikos: Yes, I'd like to echo what James said earlier and I'd also like to make a couple of other points that the amount of cybersquatting measured by the UDRP has tended to fall in the last few years if you look at it as a percentage of the names registered totally across all gTLDs; also if you look at it on an absolute basis I think the number actually fell last year and definitely has fallen this year.

Secondly people are free to pursue civil remedies like they don't necessarily need a special policy from ICANN in order to counter trademark infringement as long as the WHOIS is accurate. You know, there's courts around the world that can handle this and have handled it for, you know, Verizon, Dell, Disney, etcetera. There is no special need for a policy from ICANN when people do have alternatives.

For example if somebody's selling a counterfeit pair of Nike shoes on eBay or Craigslist we don't have an ICANN policy for that. People, you know, are free to take it to court and that should be the same for trademark infringement.

The solution should be more in the pattern of trying to make WHOIS more accurate in other words so that people can pursue those remedies themselves in a civil manner.

Greg Aaron: Okay. Anything else George?

George Kirikos: No that was it.

Greg Aaron: Okay. Martin, did you raise your hand again?

Martin Sutton: I did. If I may am I up in the queue?

Greg Aaron: Yes, please go ahead.

Martin Sutton: Okay. George, I do agree that point on the WHOIS side of things because I think that comes into the equation a lot more as we look through some of the abuse types and see this process. That would be an ideal area to explore separate to UDRP.

The only issue I have still got when we talk about this it's very simple to say yes there are mechanisms in place but the owness is always on the trademark holder. So the ease at which it allows itself to proliferate across the internet in terms of cybersquatting abuse it's uncontrollable for trademark holders.

You know, we can only pay attention to the highest risk elements because this isn't - these are not our day jobs. So just to put a balance on that, you know, fair enough there are mechanisms out there that we can utilize including UDRP. But the fact is people can get away with this activity and remain anonymous and pay nothing apart from $5 for a domain.

So I just think that's worth to bear in mind at this stage.

Greg Aaron: I see James's hand and George's hand. James did you want to comment?

James Bladel: Yes, just very quickly. I wanted to mention that as far as alternatives, you know, particularly when we're talking about incomplete or fraudulent WHOIS information there are policies existing for that as well as stipulations and requirements and registration agreements.

So, you know, perhaps in those types of situations it's best to work with the registrar or the registry to get those corrected or even ICANN compliance so that, you know, I agree with you that there are existing alternatives to that.

And I think that Martin raised a very astute point relative to, you know, the barriers to entry for someone who wants to commit this type of action is very low versus the cost spent and diligence required to prevent it.

And I think the same, Martin, the same equation also holds true for registrars as well. And it's - it goes back to the analogy versus the police department versus the fire department; are you out there patrolling looking for problems to, you know, prevent or deter those types of issues or do you build a cost-effective and, you know, rapid response mechanism so that when the problem is detected and reported you can clamp down on that very quickly?

And I think that, you know, when we start talking about things that are prevalent on the internet I tend to gravitate towards the fire department approach because I believe that, you know, in the long run that's what, you know, that's what serves the community. But - so that's my thinking there.

Greg Aaron: Thank you, James. George?

George Kirikos: Yes, I just wanted to follow up on that point about the barrier (unintelligible). And I agree with what James just said. Just some - the same can be said for other abuses too like spam; it doesn't cost anything at all for anybody to become a spammer and send out, you know, 10 million emails for a $1 or $2.

So that problem exists not just for trademark infringement but for all the other kinds of abuses as well. Typically they're taking advantage of the economies of scale offered by electronic communications.

And so to some extent, you know, trademark holders can worry about the issue of, you know, death by 1000 cuts that people can register thousands of variations of their marks. And I guess at some point they have to start doing a (unintelligible), you know, exactly how much traffic are these domains actually receiving.

And, you know, are they as big a worry as the, you know, set them out to be. In some cases they are like Verizon obviously.

James Bladel: Thank you.

George Kirikos: They say tens of millions of visitors a year by going after the typos of their names. But for other people it's probably a lot smaller than that. And also there are other means to go about it - to go about finding remedies rather than the courts. For example Google and Yahoo are the dominant pay-per-click providers.

People could obviously file their trademarks with Google and Yahoo and get the names turned off if they're being sent to pay-per-click (unintelligible) methods.

I guess the little bit more concerns they were when people do it for banks, for example and, you know, phishing of banking internet tools which, I guess it's Martin's background. But there you don't even necessarily have to do it with a trademark infringing name, you could do it with any domain name.

So it goes back to the broader question of phishing in that specific example. That's what I wanted to say. I guess we also have a few more people that joined the call according to the Adobe so we might want to introduce them.

Greg Aaron: Okay. Anyone else? Okay...

((Crosstalk))

Martin Sutton: ...but my hand up.

Greg Aaron: Okay, go ahead Martin.

Martin Sutton: Greg. Yes, I'll keep putting this on mute because I've got lots of background noise here. I think that, again, there's some good points there. On the phishing side I tend to forget about cybersquatting in terms of phishing. Phishing is very - is actually a lot more easier to identify, you know, the intention and deal with it. So those - there's very good methods of approaching that although perhaps not uniform across all the players across the globe.

My concerns are for instance where there are large numbers of domains that infringe on a brand like ours where we do not see much evidence of malicious activity. These are things that go under the radar so there could just be a very bland holding page on the site saying under construction.

But there's MX records set up. And you don't know what traffic they're trying to do on the back of that domain; it's all hidden. And when they start targeting individual users with faxes which then say well you can contact us by this telephone number or by this email address to build up a relationship these are - these are quite difficult to pick up.

And I would say again, you know, this is - it's very difficult then for end users, one to identify their being lured into a scam and secondly where to report it to and get something done about it. And we only pick up these randomly if you like.

So I think there's a problem where there's a - I agree that we have to do some cost benefit analysis and we certainly approach it in a way which says biggest risks let's deal with it and the rest of it we haven't got the resources or the time or the money to manage thousands upon thousands of variations across all the gTLDs and the ccTLDs.

And what my concern is that the end users are then affected by approaches which appear to be coming from a bank but we can't even pick them up on radars that we would traditionally use for phishing or malware and related scams.

So I just (unintelligible) that up again because it - I think, you know, we've spent quite a lot of time on definitions here but in practice there's lots going on out there that the UDRP for instance will not address. Certain other policies, the WHOIS, the emphasis on WHOIS earlier, you know, these are all good things and could end up helping all of these problematic behind the scenes issues that I frequently see. That's my lot.

Greg Aaron: Okay. Thank you Martin. I see George's hand.

George Kirikos: Yes. I just wanted to add - George here. I just wanted to add that, you know, there are a couple other ways that people can glance at a problem instead of just trademark infringement, you know, the banks can focus on better education of their customers, things like, you know, having a EVSSL certificates, things like that, that can educate their consumers on, you know, how to identify these frauds because I guess that's where the fraudsters are really taking advantage of people, they're going after the least educated consumers.

And, you know, they could spend, you know, we could limit it, for example, all the trademark infringement I mean in the world and then somebody could simply do it on a sub-domain. So, you know, it's how we get the best results for the amount that we invest in terms of trying to tackle these problems.

Greg Aaron: Thank you George. Fazal.

Faisal Shah: Yes I totally understand what George is saying but I think most of that, again, puts the burden back on the trademark holder and makes it either expensive or difficult or, you know, there's nothing, you know, I think we should be finding tools that are not as expensive that we can - that we can use to help trademark holders in connection with cybersquatting in addition to the UDRP because again like we have been talking about this time - this entire time it's really not that efficient.

And even stakeholder remedies that George has talked about are expensive as well. I mean, if we can take it from UDRP and we talk about, you know, expensive air, if you're talking about thousands of domains at, you know, $2500 a pop that could be pretty expensive for a particular company.

And then when you start - I was thinking about, you know, $10,000 for an ACPA action; that's even more expensive. And then maybe, you know, issues and costs in other countries. So I'm just thinking that here should be some other tools that are not quite as expensive and maybe more (acceptive) for brand holders in addition to the UDRP. And I guess that's why I keep trying - that's what I keep coming down to.

Greg Aaron: Okay. This is Greg. We're about 35 minutes into this conversation. And I would like to wrap it up for today. The discussion of this issue has been much more focused than it was earlier in the working group's life. What I need you guys to do is get on the Wiki and put down your positions.

If you have recommendations please draft those and put them in the Wiki. A lot of the discussion we've had has been around kind of what the issues in the background are. And I think we've gotten some good crystallization of what that is.

You've been discussing how the UDRP works well; sometimes how it doesn't work well. You've enumerated some cases where you don't think the UDRP is effective or perhaps not applicable. Those kinds of things need to go into the issue and background sections.

We must drive towards publication of an initial report. And I think the time for identifying the issues is now past. I think we've gotten to a point where we understand some of them.

If you're interested in this topic you've got to put something down on paper now. And I don't want to take time in the meetings because I think we've gotten through the issues.

I need volunteers to flush out those issue sections; we've already got a fair amount of material there, it needs to be shaped according to the last couple of conversations and some of the relevant threads.

I also want to see recommendations. If you suggest that we need additional tools to deal with cybersquatting please state that. If you believe that the UDRP is the appropriate tool please state that. If you have any other additional ideas please state those.

So I'm hearing interest from George, Martin, Fazal and James mainly. The four of you have been the most engaged in this topic. Can I rely on the four of you individually or together to put material down on paper and drive towards something we can publish?

James Bladel: Yes.

Faisal Shah: Yes.

Greg Aaron: Okay. Okay. I know that we have the ICANN meeting coming up and people's lives are starting to turn towards that but we need to attach a - kind of a timeline to this just so it's all on the tops of our minds.

What do you think is a reasonable time to have the issues, backgrounds and recommendations sections filled in so that the group can read through them and measure levels of consensus? How long is it going to take do you think?

We've got - ICANN basically the last week of this month. So do you think it would be around - let's see when's the meeting after ICANN? November 9. Do you think that's doable? That gives you the first week of November to recover from ICANN and do some touching up.

James Bladel: I think that's fine.

Greg Aaron: Okay. Okay so the goal is to have the issues, background and draft recommendations. And of course that means all of the recommendations that people want to put forward. They can be in tune with each other or they could be in conflict with each other or whatever. But then that gives us something on paper that the entire group can come through. We'll measure levels and we'll rewrite as necessary.

Okay awesome. Long time coming but I'm glad we're there. I'd like to move onto the next section, uniformity of contracts. What we discovered by going through the work that Berry and others have done is that there is no uniformity. But then the next question is well what does that mean? Is that a good thing or a bad thing?

The group's task has been to understand that if registration abuses are occurring that might be curtailed or better addressed if there was more uniformity. And the group is going to put some material on the Wiki and flush it out.

So let us go to the Wiki. And is there - Berry is not on the call today. Is there anyone - and Mike - Mikey had to give his regrets for today; he's in transit. Is there anyone else in that subgroup that can tell us about where the Wiki material is in terms of it's process? It doesn't seem to be flushed out.

James, do you know? I don't see that the Wiki has been filled in.

Marika Konings: This is Marika. There is a document posted. I'm trying to pull it up on the Adobe Connect in which Berry has summarized the last meeting of the sub-team. I think it's at the top of (unintelligible).

Greg Aaron: Okay, are you able to pull it up in Adobe?

Marika Konings: Give me two seconds.

Greg Aaron: Okay.

Marika Konings: It should be up now.

Greg Aaron: Okay great. Okay. So the sub-team says it will not have capability to make true recommendations relative to what abuse provisions are required. We would not be in the proper position to define what the minimum baseline should be.

And they say they want to discuss next steps and better understand the required effort at future meetings. We're missing some of the key participants from this group though.

James Bladel: Greg, this is James.

Greg Aaron: Yes.

James Bladel: Yes, just speak to that. This is centered primarily on Rod Rasmussen's message to the list. And I want to point out that you skipped over the part that says without sufficient data. And Rod outlined essentially an approach or a methodology on how that data might be obtained in an earlier meeting - or earlier email.

And so I think that this group is saying that yes we're agreeing with Rod that without that quantifiable data it would be difficult to make true recommendations on what the minimum baseline should be.

Greg Aaron: Okay, very good. And my skipping that section was completely inadvertent. Okay so anyway are we in a position to discuss this without Berry and Mikey on the call?

James Bladel: I'd rather have one or both of them.

Greg Aaron: I would also. All right I think the action item remains to put this material on the Wiki though. And we're going to need them in the next meeting.

I don't know offhand if they're planning to participate in the meeting at Seoul or not but we'll ask.

James Bladel: Both have indicated that they'll be - they won't be there in person but they'll be participating remotely.

Greg Aaron: Okay. Okay good. Thank you. Okay next one is - we'll have to pick that up next time. The next one is malware and botnets. I have put new material on the Wiki as I promised. And Marika, that's on the malware/botnet control Wiki.

Marika Konings: Okay, I think it took the wrong there. Just - I need a few second to...

Greg Aaron: Right, yes, we've got two separate topics; one is malware and botnets...

Marika Konings: Okay. All right.

Greg Aaron: ...and the other one's...

Marika Konings: All right if you can talk around it I'll get the other one up there.

Greg Aaron: ...spam/phishing/malware. One of the things that's been posted recently on the ICANN Website was called the ERSR which stands for expedited registry security request.

This came directly out of the experience with Conficker which was a big part of our malware and botnet discussion. Basically what happened was Conficker was a large-scale threat that uniquely leveraged thousands of domain names.

Initially in com, net, org, info and biz and .cn later it expanded to include about 100 other registries as well mostly ccTLDs. And basically what happened there was the registries in ICANN got together and said okay, yes, this is all something we're interested in dealing with; it's the right thing to do. Let's figure out a way to get it done and then we'll regroup.

And what people realized was that this kind of thing will probably happen again at some point; there will be a threat to the DNS or there'll be a threat that could fall on a particular TLD or registry that would require the registry to take some defensive action.

And we've - basically everybody said well we need to be prepared to have process for the next time that happens. So the ERSR is the result. And in the description I posted a link to it. And basically the ERSR says that if an issue like this comes up the registry can go to ICANN, report it and propose a mitigation effort.

And ICANN can choose to waive or modify relevant contractual language for the duration of that incident or whatever is needed to deal with that incident. In the case of Conficker that meant some registries wanted to register the relevant domain name so criminals could not register and use them.

So in some cases those registries registered those names in a holding account. Normally registries aren't allowed to register domain names for themselves of course so that was the waiver.

Other registries chose to do it different ways; some of them just blocked the names so they couldn't be registered which doesn’t exactly - that's kind of a more of a reserve name approach or a - it's not exactly a cessation of first come first serve but it sets aside some names that can't be put into the registry.

Other registries said what we'll do is let's let a white hat register those names and we will agree to waive the fees. And then ICANN should also waive the ICANN fees on those. So that was another contractual accommodation.

ERSR basically sets up a framework for the registry and ICANN's legal and security staff to review these proposals and then get them checked off on so there's process involved in it. So it's basically - and it's also fairly flexible; it doesn't say exactly how we're going to deal with things, that has to be figured out once you understand the threat that's come up.

So basically it's a framework for going forward. It's been proposed as something to be available to the existing TLDs. The ERSR has also been inserted into the new draft applicant guidebook for new TLDs. So the ICANN staff has proposed that all the new TLDs to come would also be able to avail themselves of this.

So first I want to ask if anybody has any questions about what the ERSR is and is designed to do? James, is that your hand?

James Bladel: Yes, a quick question, Greg, and I apologize, I've read this once but that was quite - I think when it first came out and so this may be covered somewhere in the document. But the question is is the ERSR designed to be a rapid stop gap measure and that if for example the situation or the impetus that caused the ERSR to be raised in the first place because a long-term or ongoing problem that it would be addressed through some other mechanism like an RSTEP or is it meant to be temporary?

Greg Aaron: Well it's designed I think it says for the duration of the incident. Now Conficker for example is an example of an ongoing incident in that Conficker's code continues to generate domain names and if you want to continue to block those that's an ongoing process.

And that's going to - it's going to depend on how long, you know, Conficker remains kind of out in the wild perhaps. Now but that said it's a fairly - it's a very well defined set of domain names. We know how many are involved and we know that they're kind of long random-looking domain names for the most part that nobody's going to want, you know.

So that's an ongoing one. Is - would a PDP be relevant to addressing Conficker specifically? I would suggest no because it's very, you know, it's a fairly limited issue - well defined issue. And now we have no idea what other kinds of things are going to happen in the future.

I think PDPs are most useful when there is a general and systemic question that comes up right? That's usually what our PDPs are about. Does that make sense?

James Bladel: I think so. I just - I - my only question relative to you ERSR would be whether or not this could be a backdoor for temporarily permanent changes. What I mean by that is something that, you know, is needed in a hurry and it's quickly addressed through ERSR but then because the duration of the incident goes for weeks and months to years it becomes, you know, a fixture on the landscape.

And I'm just trying to understand, you know, where that transition point goes from an emergency action to more formal actions like an (RSTEPer) or a PDP. And I don't have the answer I'm just asking that relative to ERSR.

Greg Aaron: I don't know if anybody knows yet because we don't have any good examples other than Conficker.

James Bladel: Yes.

Greg Aaron: I have to assume that if we get a log of similar events or if something gets really big then somebody would have the option of raising the issue and saying this is now become something that needs to be looked at, you know, more from a policy standpoint or what have you. I think that option would be open.

So anyway what's happened since we started our work in this group is this new thing has come about. I drafted a note about describing what ERSR is. And at this point I don't have any additional recommendations to be - to put into the malware and botnet control section.

I haven't heard from Rod yet but I don't have any because this would help me as a registry figure out how to deal with, you know, a large-scale issue, this would give me some options. So I'd like to hear if anybody else has any other recommendations to be slotted into this section.

And that's an open question now and for the next couple of weeks of course.

Rod Rasmussen: This is Rod, I heard my name used in vain there so I guess I'll pipe up. And maybe not vain but - and unfortunately I'm driving rather than in front of a computer so I can't raise my hand. The - and I think we had a little bit of an email exchange on this - I think this does, you know, the ERSR whatever it is - it's - I think it gets to the heart of the matter for large scale incidents.

So the only question I have remaining at this point is what do we do about small scale stuff. And does that fit in this category or not? This category was kind of created to address these large scale things like Conficker I think. And then we have another category that's the phishing/spam/etcetera which may be more germane to the small scale botnet stuff or not. We've got it labeled on here we have to figure out how we want to work that out.

But for example currently the botnet that's doing the avalanche attacks has got five (C&C) domain names attached to it and the code that's underneath it, two of which are registered, three are not. They all happen to be com I think. But anyways that's - and there's a, you know, there's some law enforcement saying hands off on those right now.

So, you know ,that's the kind of thing that how do you respond to that from a policy perspective versus an incident perspective. And then you've got all kinds of other botnets and things that being controlled by domain names or potentially controlled by domain names on a very much smaller scale; you don't need to have this process to, you know, warn lots of registries all concurrently of what's going on.

So that's an open area I think for us to figure out how we want to deal with that whether we deal with it in this topic area or the other one.

Greg Aaron: I agree actually. This is Greg. And that provides us a segue into the separate place where we were looking at other malicious conducts like phishing, malware and spam these smaller day to day kind of incidents that happen on the Internet all the time.

Rod Rasmussen: Yes, I think it's certainly appropriate to cover it there I just want to make sure we cover it and don't kind of skip it...

Greg Aaron: Yes.

Rod Rasmussen: ...because the natures of the two different things at the same, you know, just a scale issue.

Greg Aaron: Yes, I agree. My proposal is everybody take a look at what I've written on the Wiki in the malware/botnet area which kind of deals with these large scale threats that would - that are so large that they would require registry itself to respond and possibly get a contractual exemption to deal with it.

And then separately segue into the other area which is basically where we're looking at these kinds of malicious or criminal conducts like malware and phishing and so forth. And Rod's - I think you've touched upon an important question which is these are things that often have to do with domain names but the question is what's the role for policy making? What are the issues?

So let's segue into that then. Marika, are you able to bring up the malware/phishing/spam Wiki?

Marika Konings: The one that was just - you mean this one?

Greg Aaron: Yes. Okay we've got notes. Yes, it's pretty much the same what's on the Wiki and what's on that document. Okay. To recap the previous conversations there was some - I'm just going to read this, we just sketched out these abuse categories relate to the scope of the working group's activities and GNSO's policy making.

As these abuses occur after domain names registered some suggested that these abuse categories fall outside the scope of the working group as its focus is on registration abuse. Some suggested that only if you were able to determine at the time of registration that a domain name will be used for phishing, spam or malware it might be considered registration abuse.

Some argue that it will not be possible to determine at the time of registration whether it will be used for phishing, spam or malware while others pointed out that based on who is registering the domain name how this is being done, e.g. which name serves are being used - uses stolen credentials etcetera it might be possible.

The point was raised that a problem with assessing what a domain registration will be used for at the time of registration still requires speculation about future intent which can never be 100% accurate.

Some propose that there is the ability to accurately predict or accurately assess intent at the time of registration. I'm sorry, that if there is an ability to accurately predict or accurately assess intent at the time of registration it should be part of the recommendations made by the group relating to registration abuse.

The issue of false positives and how to deal with those is raised in this context. So the point there was - we're talking about registration abuse rather than use abuse and how those intersect. There's the issue of at the time of registration can you figure out whether it's going to be used for a malicious purpose or not.

It was pointed out that - in the next bullet that as a business practice many registries or registrars delete massive numbers of domain registrations that have never been used for phishing or spam - I'm sorry, phishing, malware, etcetera. When they discover that the person organization has registered these domains is actually using at least some of the domains for that purpose.

In these cases the registrant has already broken terms of service agreement. Another question would be whether or not ICANN should get involved in that process or whether this working group should make any recommendations to that end.

It's suggested that an ICANN approach might inject uniformity where flexibility is often required as it might tie the hands of registries and registrars and reduce or limit their options or how they can or cannot act in those situations.

It's suggested that best practices or minimum standards could be explored. The importance of due process is also noted. So if I may that bullet was about the fact that some registries and most registrars I think if not all already have some contractual language or terms of use about domain names.

And at this time they do use those to suspend domain names for these kinds of infringements. The question is whether there might be more uniformity in that or whether that uniformity might be a good thing or a bad thing.

Next bullet is someone noted that in certain instances legitimate domain name registrations are hijacked and used for purposes such as phishing, malware and spam. Any policy or recommendations should not impact those that are innocent bystanders - bystanders such as blocking future domain registrations.

In the case of phishing 80% of phishing domains are compromised or hacked with the legitimate registrant not being aware of those activities. The next bullet is taking into account the scope question for this working group to focus on registration process it's suggested that verification of users might be a potential approach to consider suitable for policy development.

Another issue is - that was suggested is systemic abuse by resellers which goes back to how registrars deal with various agents. It was pointed out that with regard to GNSO policy making these categories might be out of scope for GNSO policy development that other managers such as e.g. best practices could be possible outcomes.

Okay so those were the substantive comments that have been made so far. I have a question which is we've been calling this one phishing, spam and malware should we call this something that gets to the heart of it which is malicious conduct involving domain names or something like that? Is there any merit in that?

There might be things outside of phishing, spam and malware which are equally applicable for example. I'd like to throw that question out. Rod, do you have any opinion on that? Are we missing any bad activities for example?

Rod Rasmussen: Well I mean certainly things like, you know, the classic example everybody throws in there is child pornography. I guess the malicious use is in the eye of the beholder. You have, you know, all the issues that people bring up is what's illegal where in what jurisdictions.

I think if you call it malicious use and specify examples that are fairly universally agreed upon then you might be able to avoid those issues but if you kind of web this - get this semantics argument rolling if you'd just have a broad label.

((Crosstalk))

Rod Rasmussen: I don't know, I'm getting tired of semantics arguments.

Greg Aaron: Yes, well and we have those issues of jurisdiction when we're talking about malware or spam or anything else anyway.

Rod Rasmussen: Yes, absolutely.

Greg Aaron: I see Martin's hand.

Martin Sutton: Sorry I'm late to the mute button. Yes just to echo Rod's words there as well, I don't really want to go into lots of definition type processes. One thing - I just wonder if I put out a question here in terms of gTLDs there's this remark with regards to, you know, privately identifying domains that are likely to have the intent for abuse.

I just wonder whether that expands across all gTLDs so there's some proactive registries and registrars out there but across the gTLD space. I wonder if the same information is shared so if you do have somebody breaking the terms and conditions set out within your agreement whether that can then forfeit their registrations across any other gTLDs or potentially one to examine down the road.

Greg Aaron: Well that's an interesting question. Most of what happens now is according to whether someone has violated the terms of service or a contract. And the registrar may determine a particular registrant has done that. But can that be shared or should it be shared to other registrars or other registries? I mean I think that's up to the registrar.

And if I was an attorney I would, you know, and at a registrar I would want to make decisions based upon my own contract.

Martin Sutton: So does that go back to uniformity of contracts?

Greg Aaron: Well I'm not sure what you're asking. Should...

Martin Sutton: Well I'm just thinking about some of the fraudulent type activities. Ignore domain name space for the moment, I'm just thinking about frauds within the banking environment.

There's a lot of collaboration amongst other financial institutions. So we know what's going on, share - the new types of fraud that are going on. And where appropriate there's a certain level of data share and giving between a select group of players so that we can tackle for it effectively.

I'm just wondering in some of the particular circumstances that we're talking about where gTLDs are viewed as a good resource for us to conduct deployment of malware or phishing attacks and such like where there's some data elements within for instance WHOIS that are going to be the same and can be checked across all of the gTLDs whether there is some proactive work that can be done in that space.

So it cuts out more and at what level what's going on rather than wait for events to occur and all treated in their own separate way further down the line which is normally when end users are affected.

So I'm just trying to think here is, you know, building into some of the ideas where there are good practices already undertaken by some of the registries and registrars whether to extend that out so that for gTLDs where there is a contract with ICANN that there's something that could be built in there or looked at, investigated, whatever to think about best ways to share information and block out bad actors.

Greg Aaron: George.

George Kirikos: Yes I just wanted to follow up on - George Kirikos here - follow up on that idea from Martin. Was he kind of advocating like a risk-based approach where you can identify certain people or certain registrants as high risk kind of like you do in the insurance industry, you know, identifying people with, you know, preexisting conditions and charging them more and being able to classify people according to their risk. Is that kind of what you're advocating?

Martin Sutton: I think.

((Crosstalk))

George Kirikos: ...I can support if you allowed people to mitigate that risk for example by sharing, you know, doing the WHOIS verification and other things to kind of white list themselves or signal...

Martin Sutton: Yes.

George Kirikos: ...to the market that they are a good actor?

Martin Sutton: Yes, I think it's more where there is distinct evidence of foul play. So there is always a lead. It's probably not at the point of registration; there is some activity that takes place which reveals a bad actor. But some then some reverse WHOIS checking then reveals all the domains across gTLDs, and probably lots more ccTLDs but we'll ignore those for now.

Where there can be some methods built in to say okay once you've broken the terms and conditions for this type of category say, okay, phishing then all of your domains that you hold in your portfolio that we can identify are then suspended or some kind of action can be taken against those across all the gTLDs.

Greg Aaron: So - Martin this is Greg. So the idea would be once an individual proved to be a problem your question is can all their domain names be identified across the various TLDs and registrars that they use?

Martin Sutton: Yes.

Greg Aaron: And then have all of them take action against that party?

Martin Sutton: Yes. It's similar to me going to legal department saying can we put an injunction on somebody from ever using the Internet. I know it would very difficult to impose but there are ways that can - we can work through some of these.

But it just reveals to me some of the ways that we tackle fraud issue is through data sharing where we're able then to - as George alluded to, we can risk assess some of these or we can block them out depending on the severity and the proof.

So where we've got distinct types of threats we can work through some of those to - an idea where, you know, bad actor has been revealed; it's for this type of malicious behavior and therefore we can cross check against all of the gTLD domains that are held by that individual and take action against them all on block rather than, you know, all they'll do is just shift their business to all the other domains that they've got available to them.

Greg Aaron: Okay.

Martin Sutton: And there could be the potential for a black list as well but they'll always go under another name.

Greg Aaron: Thank you Martin. And I see that James had posted a note in the dialogue box and he said once we use the term conduct does that not imply post-registration or use - e.g. use issues? James, do you want to flush that out?

James Bladel: Briefly Greg. That going back to your proposed category definition for these issues you mentioned something, malicious conduct. And I thought that the, you know, that we should possibly stay away from the word conduct because that essentially comes down pretty heavily on the question of whether to not this is a registration abuse or a use abuse issue.

And anything that you move under the heading of conduct, you know, immediately settles that question.

Greg Aaron: Well isn't that one of the central issues that we're faced with a domain name - in these kinds of problems we're looking at phishing and malware and so - malware distribution and so forth, the domain name can be registered but it's not actually a problem until it's used.

The issue is is that in some cases I think we're worried about that the bad guy is definitely going to use it because he's proven that he is a bad actor before. So the question is are you - are you moving against this person because you have a pretty good idea that he's going to do something bad and why should we wait until it happens; is that really the issue?

James Bladel: Yes, if it is, Greg, I think that we want to state that - this is James speaking - if it is then we want to state that deliberately rather than just making a categorical statement. So that's...

Greg Aaron: Right, right, okay. Well this is good, we're getting down to the core of the issue I think we're trying to at least.

James Bladel: Right.

Greg Aaron: Well it's - it reminds me of that old joke where the guy goes into the doctor's office and he says, doctor it hurts when I do this and he hits himself on the head. And then the doctor says well don't do that.

You know, you know in some cases - in my experience you're pretty sure that a particular person may do something bad because they've done it before. And it's frustrating as a responder - I'll state this as my personal opinion - it's frustrating as a responder in certain cases where you know that somebody is going to do something bad with a domain name because of their past history.

And why then wait for them to do it? After that the damage has been done and users have been hurt. I will say that those cases where you're really sure are relatively few where you have a repeat offender. Rod can tell you about the avalanche gang for example of phishers who make very distinctive registrations and you know who's behind them and you know what they're going to do with them.

The question is should ICANN have a policy that addresses these are these cases already addressable I think? And is more uniformity needed or is there something we need to do to make things more clear or something like that? I think that's the issue with these kind of problems like phishing and malware distribution.

So what are your thoughts?

James Bladel: Are you directing that to James directly or the group at large?

Greg Aaron: Anybody.

James Bladel: Okay because Martin is head of me in the queue.

((Crosstalk))

Martin Sutton: Sorry, I'll let that one stand, sorry I'll take that down.

Greg Aaron: Okay. All right I see Margie's hand.

Margie Milam: Yes, actually it was a separate topic. We've been - it seems like we keep going back to this topic of whether we're allowed to look at use as part of the work of this group. And I thought, you know, from some of the presentations that I've made over the past that we're not limited to looking at only abuses only to registration.

The only thing that the charter really identified is that we weren't going to - at least we weren't worried about abuse that was solely related to use. But that doesn’t mean that you're not allowed to look at use. So I just wanted to, you know, at least address that topic; that we don't need to be that restrictive.

Greg Aaron: Yes, you're reminding us that use is a factor that may be considered.

Margie Milam: So it's not off limits it's just, you know, what the charter really clarified that we can't only look at use. You know, that it's solely related to use that's a separate topic.

Greg Aaron: Right. I think the other issue maybe in the back of the mind is that in the issues report the general counsel said it's out of scope for policy to address uses in a certain fashion. I'll have to go back to the exact language what they pointed out.

Margie Milam: Yes, and I guess we could take a look at that but I don't recall it being that restrictive. I think what we were trying to get at is we're not trying to, you know, this isn't meant to be purely content so if it's - use of the domain name that's purely content and it has nothing to do with the registration then that's probably off limits and we can certainly go back to the issues report and look at the language.

But that's, you know, that's not saying that we're not able to look at use at all which we've been talking about over the last ten minutes.

Greg Aaron: Okay thank you. James, I see your hand up still.

James Bladel: Yes, you know, I'll go ahead and take that down because I know we're getting close to time.

Greg Aaron: Yes, we are actually. All right well let's pick this issue up again in the next meeting which will be in Seoul. I think a lot of us will be participating remotely. Could I have a show of hands of who will be attending the Seoul meeting in person?

Rod Rasmussen: This is a virtual hand up from Rod.

Greg Aaron: Okay, Rod will be there, Margie, Marika, James...

((Crosstalk))

Greg Aaron: ...Fazal, Robert. I will not be there - George will not be there. I don't think Mikey is going to be there. So we'll have a few members at least.

((Crosstalk))

Roland Perry: That's another virtual hand up from Roland who's accidentally closed his browser.

Greg Aaron: Okay, so Roland you will be there in person?

Roland Perry: Yes I'll be in the meeting all week in person, yes.

Greg Aaron: Okay. All right so we'll have decent participation in person. Others including myself will join remotely. Since I'll be joining remotely Marika had said she would help with the logistics of recognizing speakers and so forth so we'll figure that out.

One of the things we have to do is present an update to council. And just this morning there was a note from Glen about an invitation to do that. So I have to read that invitation from Aubrey. I think what I'll probably end up doing this week is work with Marika to do a summary.

Marika, you had kindly offered your time to help put a slide deck together.

Marika Konings: Yes. Yes, correct and maybe just to add to that because one of the objectives of that update would be as well to brief some of the new council members on some of the work that's ongoing so it would be a bit as well of a more in depth explanation probably on, you know, what the objective of this working group is.

And I think some slides we'll still have some from some of the previous meetings so I can...

((Crosstalk))

Greg Aaron: Okay. Okay great. How many new members will be coming onto the council; do you know offhand?

Marika Konings: At least of course there's three new (NCG) appointees. There - one new non-comm member. I think there's two at least new in the other groups and I think some still need to confirm. So I think at least six, seven members that will be new.

Greg Aaron: Okay great. Okay well we'll work on that over the course of the next week or so. And why don't we keep people updated on the list about that. And the meeting time has been posted up for everybody and the room numbers. This time it's not first thing in the morning so thanks to the staff for obtaining a slightly more civilized time I guess.

Also this time slot does not interfere with the SSAC meeting which was the case for the last two meetings. So if you're interested in SSAC you can not have a conflict; that's good.

The format of the Seoul meeting is going to be pretty much the same as it was last time which was the first part will be continuation of our discussions amongst the members. We might decide to use the slide deck also as an orientation. And as in previous meetings then we open up to hear questions and feedback from the community so in the latter part of the meeting we'll do that and record any comments and questions that people have.

And I think that's about it. Are there any other things that we should think about for the meeting? Marika, the remote participation has been pretty good over the last couple of meetings. Do you know if we'll have video coverage of this in Adobe?

Marika Konings: Not that I am aware of. I know that was run in previous meetings as a test for some meetings but I don't think it has been - is going to be across the board yet. I don't - Glen, do you know - if Glen is still on the call. I think she might have dropped. But as far as I'm aware there's no video coverage for this meeting. I think we just have the Adobe Connect line and the telephone lines.

Greg Aaron: Okay. Okay cool. After Seoul then the next meeting will be November 9 and then 23rd which is the Monday before the US Thanksgiving holiday so we're locked in for our next three meetings. I haven't heard from anyone that there are any major conflicts as far as those three meetings.

So anyways as we come up at the end of the meeting we do have a few action items that we agreed to today; I'll write those up and send them out to the list. Especially we need to do work on the Wikis for uniformity of contracts and cybersquatting. And we will circle around to those at the Seoul meeting.

And does anybody have any last thoughts before we conclude for today? Going once, going twice. Okay if not we will adjourn and we'll have our next meeting in conjunction with Seoul. So thanks for your continued good work and hope to converse with you on the list before Seoul. Thank you.

Marika Konings: Thank you everyone.

((Crosstalk))

George Kirikos: Bye everyone.

Greg Aaron: Thank you. Take care.

Coordinator: Thank you. That does conclude today's conference call you may now disconnect.

Gisella Gruber-White: Thank you (Louise).

END