## GNSO
## Inter-Registrar Transfer Policy B Brainstorming session in Sydney on
## Sunday 21 June 2009 at 08:00-9:30 local time in Sydney

**Note:** The following is the output of transcribing from an audio recording of the Inter-Registrar Transfer Policy B Brainstorming session in Sydney on 21 June 2009. 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-irtp-b-20090621.mp3
http://gnso.icann.org/calendar/index.html#july
Mike Rodenbaugh
Jim Baskin
Marilyn Cade
Gretchen Olive
James Bladel
Graham Chynoweth
Tim Ruiz
Raed Alfayez - Saudi Nic
Mark Klein
Jeremy Hitchcock
Tony Harris
Chris Wright
Michael Young
Joe Cady
Olga Cavalli
Jeff Eckhaus
Rudolph Garos
Ibrahim Mohamed
Remote participation:
Barbara Steele
Mike O'Connor

Staff:
Marika Konings, William McKelligott, Olof Nordling, Mike Zupke, Margie Milam, Dave Piscitelllo, Glen de saint Gery


Marika Konings**:**    As it says, this is a brainstorming session.  The idea is really to have a very open discussion, people being able to share ideas, experiences, suggestions for possible solutions that this group might be looking at.  Just to place this is context, this is not a policy development process yet.  The Council is expected to vote on this issue coming Wednesday, and I think the expectation is that it will be adopted – hasn't been much discussion or objection to these issues, as they have come from a review, I think, that started in 2005.

So, the idea is to record all the points made here and pass them on to the working group once they get started and make sure that that finds its way in the report. And of course, I hope that all of you here are willing, as well, to participate and sign up for the working group. You can tell me or **Glen** after the meeting if you're not on the mailing list yet, to be added.

So, my idea would be, unless there are any objections, just to run through the issues report and its main findings, and then basically stop at each – there are five issues that are covered in this Part B, and basically then stop on each of these issues and get people's input. I mean, one issue is related to a report of SSAC, so very grateful to see that Dave is here and Jeremy, so hopefully, they can give some input here.

There were some comments in the issues report that were made, for example, by GoDaddy. I'm hoping as well that James can shed some light on that.

And, I think it will be very helpful as well to see as some of these issues were reported in 2005, to see whether they're actually still relevant or whether there are any changes or whether there are any elements this group will need to take into account when they start looking at these issues.

Man:                    Marika, would you do the favor of just kind of running through what the five issues are real quick (2:02 unintelligible)?

Marika Konings:    Yes, we're coming up on that. And I don't know, maybe we should do a quick tour of the top (2:09 unintelligible) at least know who's in the room. So, well Mike, maybe you can start on that side and just…

Mike **Rodenbaugh**:    Sure. I'm Mike Rodenbaugh, GNS Council from a business constituency.

William McKelligott:    William McKelligott, ICANN contractual complaints.

Olof Nordling:    Olof Nordling, ICANN staff.

Mike Zupke:    Mike Zupke, ICANN staff.

Margie Milam:    Margie Milam, ICANN staff.

Glen de Saint Géry:    Glen de Saint Géry, ICANN staff.

**Rudolf Garos**: Rudolf Garro from **Noru.** I'm with **Zampac** Net. We're looking after (2:55 unintelligible).

**Ibrahim Mohamed** Hi. I'm Mohamed from Comores. I'm just gathering information about this whole event. Thanks.

James **Bladel**: James Bladel from GoDaddy.

Jeremy Hitchcock: Jeremy Hitchcock from Dynamic Network Services.

Dave Piscitello: Dave Piscitello, ICANN staff.

Woman: (3:18 Unintelligible)

Man: (Unintelligible)

Marika Konings: Feel free to come and sit here at the table, because we have plenty of space, and then you have a microphone as well to contribute.

So, just for those…

: I'm sorry Marika. Is there anyone on the phone or is there remote access to…

Marika Konings: There is remote access, but I haven't heard. Is there anyone on the phone?

Woman: (3:43 Unintelligible)

Marika Konings: No one yet.

(Crosstalk)

Barbara: Barbara Steele here.

Marika Konings: Hey Barbara. Can you hear us well?

Barbara: It's a little bit soft, but if I listen closely, yes.

Marika Konings: Okay. The presentation is up as well in the Adobe Connect room that Glen sent around yesterday, the council room. So, if you want to log in, you can see the presentation there as well.

Mike O'Connor:     Marika, this is Mike O'Connor, can you hear me?

Marika Konings:    Yes.  Hey Mike.

Mike O'Connor:     The Adobe Connect room isn't letting me in.  (4:24 unintelligible)

Marika Konings:    You have to go to the one that Glen sent yesterday.  We initially sent out another address, but it's the one that Glen sent out yesterday to the IRTP mailing list.  It's, I think, GNSO Council.

Mike O'Connor:     Barbara, can you see it?

Barbara:           You know what…I don't see (4:37  unintelligible) email.

Mike O'Connor:     Yes.  I'm looking at our most recent one.  It's not a big deal Marika.  I wouldn't worry about it.

Woman:             It was sent yesterday, Mike.

Mike O'Connor:     (4:47 Unintelligible).

Marika Konings:    Okay.  Well, I'll have it open so I'll see you appearing.

So, just for those of you that are new to this issue, the Inter Registrar Transfer Policy was adopted in 2004 and is a consensus policy that basically sets out how domain name holders can transfer domain names between registrars.

When this policy was adopted, the group immediately decided as well that it would be a good idea to carry out a review to determine whether the policy was working as it was supposed to be, whether there were any elements that were missing, or whether there were any areas that were unclear or not used as they were supposed to or intended to.

So, an overall review was carried out and a working group identified a whole list of issues that they deemed were suitable for improvement or clarification, and those were divided into one PDP on denial, the reasons for denials of a transfer that has already been wrapped up.  And then there were five other IRTP PDP's identified of which one has already been wrapped up as well on IRTP Part A, which was looking at some new issues related to IRTP.

On this last one, the Part B, the Council decided that trying to move up the speed a bit and take advantage of putting some similar issues together, they put three issues from the Set B that was identified by this transfer working group, and some identified under Set C, together into one IRTP Part B. And the issues in this one are mainly looking at undoing transfers and issues relating to a registrar lock status.

So, the issues report on this was submitted to the GNSO Council on the 15th of May, and they had some initial discussions on that in their previous meeting, and as I said before, they're expected to vote on whether to initiate a PDP at the public meeting on Wednesday.

So, this is just very briefly just an overview of all the issues that are covered in this PDP. We'll now go into each of these in more detail, but you can have a quick read so you get a feel for the issues that are covered here.

So, if we then move into the first one, which is on the urgent return resolution of a domain name. Basically, the question here is should there be an expedited handling process for fraud situations be developed.

A staff report that was published in 2005 that basically looked at all of the comments received and input received from the community provided some suggestions that there might be a need to develop an expedited handling process, or looking at automatically returning names that are subject to a dispute, return them to the original registrar until the dispute action had been resolved, or automatically rolling back a name service to what they originally were.

Then there was also discussing the SSAC hijacking report. I think maybe it's better to turn it over to Dave to give a little bit of feedback what that report recommended, and maybe start a discussion from there. I've listed here as well, because in the report we did cover – some issues are obvious that will need to be taken into account if indeed the group would agree that this is an area where an expedited process would need to be developed, taking into account that there is a transfer resolution, dispute resolution process in place. But I think that many deemed that that takes too long, and in those cases, in hijacking cases, the damage might be too great, that there is a need for urgent return.

There are some questions that will need to be considered like what is the actual extent of the problem, does that warrant a new policy or a new dispute resolution process, how do you ensure a fair process, who would be the

decision maker, who determines whether it's a fraudulent transfer or not, or are there any market solutions or best practices that actually already deal with this issue. So, that's something that needs to be taken into account.

So maybe Dave, if you can tell us a little bit more about the SSAC report on this issue.

Dave Piscitello:    The SSAC report is actually from 2005, and I think the terrain has certainly changed quite a bit in four years. The primary purpose of the report was to respond to domain name hijackings that had become fairly noteworthy and fairly frequent in situations where a registrar account was used and compromised by an attacker, and the attacker sought to transfer a domain, as opposed to the kind of attacks that are going on today, where the attacker actually wants to make you sell the domain in more of a stealthy manner or more of a malicious manner.

So what we tried to do in that report, and what we're continuing to do with the report that we distributed to the registrar constituency earlier this week, I guess late last week, is identify measures that registrars can take to improve authentication methods, improve ways to verify that a transaction is actually authorized by the appropriate legitimate registrant of a domain. And in the hijacking report, we broke up a number of recommendations that we identified to registrants who could take measures on their own to try to protect themselves from the unauthorized transfer of a domain. And then we also mentioned a number of recommendations that we had made to registrars.

Now, sort of anecdotal evidence suggests that a fair number of registrars had actually implemented some of these, but I don't think it's accurate to say that all the registrars have implemented all of them. I don't know how deeply you want me to go into this, but that really is the summary of what we did.

Marika Konings:    Well, I would be especially interested to hear a bit more about – because in the report you talk about having an emergency procedure, and you discuss some elements that this procedure could, should, might have such – I listed them here - like an emergency action channel, I think, as more of the 24/7 phone number you can call, the policy that would need to go with that, and the public awareness campaign.

Dave Piscitello:    Well, these are fairly common kinds of points of contact that are needed for a number of purposes, not just inter registrar transfer. And, I think the goal here is that there is some way for a registrant to contact his registrar in a very

clear and unambiguous manner, there's some way for him to notify of an abuse, in this case an unauthorized transfer. And upon having that notice placed with the registrar, the registrar would start some kind of auditing capability where the complainant could have some kind of tracking number or some kind of authorization that indicates that he's in the queue, he's going to be taken care of, that there's a record that starts the investigation that the registrar would actually perform or conduct to determine whether or not the claim is legitimate.

And if the claim's legitimate, then the question is how rapidly can the registrar rectify or remedy the unauthorized transfer. One of the important aspects of that is that if the community identifies a very clear set of criteria to a registrant, the kind of documentation that he must present to make a credible claim, like any other claim, like an insurance claim in a car accident, he's more likely to have better response if he provides as much exact detail as possible. So, accurate Whois information, an indication of when the party actually registered the domain, proof of purchase or proof of completion of the transaction are all components of that. And once the registrar has that information, he can look at it and determine whether or not this is a credible case. It looks like the guy paid for it, it looks like the guy actually registered it on this date, it doesn't look like any party that he authorized attempted the transfer, and I'm going to start an investigation. At that point, the registrars should act appropriately to say this is probably an asset that organization or individual, the purpose here is to try to accelerate the process of restoring the name to the complainant.

Marika Konings:    So, a question that would come to my mind is then who is in the end, or who should be the decision maker on whether a transfer is deemed fraudulent.

Dave Piscitello:    I think that's a very hard question, because there are different circumstances that probably beg different answers. If it's a situation where the information is not sufficiently clear, or there is some sort of intellectual property dispute or the paper trail, so to speak, is not particularly clear, I mean, I could imagine a situation where a registrar might want to reach out to someone else and say, I don't know how to make this decision. But, I'm not a registrar.

There are some clear cut cases, I'm sure, and that's the easy path. The harder cases are where there is a legitimate dispute as to whether or not the transaction was approved or not. The other cases I can think that come to mind that are hard are situations where an organization believes that it registered a domain, but in fact, someone in IT who no longer is a party to that organization, registered in his own name, and before he left, altered the

contact information so that it was his personal address, personal residence, personal phone.

Those are much more challenging disputes, and I can understand that a registrar would find a certain amount of difficulty in pulling the trigger and saying, this was Dupont.com or this was ATT.com, and you really aren't an officer of the company, and I question whether it belongs to you. But then maybe there are other cases that are not so clear where it's Joesbargainbasement.org, and the guy's name is Joe and the company was Joes Bargain Basement. So, it's not very clear.

Marika Konings:    The question, and it's maybe a question I'd like to ask to James then, would it make sense to have a policy? Or, as the cases are so diverse, would it be easier or more effective to indeed look at registrars, how they deal with it, and give them the leeway of saying, well, look at it case by case, and you still have, of course, the dispute resolution procedure that people can enter to. But, if there is really a need for a quick resolution and then for the real obvious cases, isn't that already being done in a registrar between registrar manner, or…?

James:    Yes, and I just want to say Dave's absolutely correct that there's a very high volume of transfer disputes like this, and we can take maybe 75%, maybe 80%, I don't know what the exact figures are, and say these are very clear cut and there's a – it's very intuitive what we need to do here. The remainder, though, I think requires a more in-depth investigation, understanding the different parties involved, the sequence of the events, and sometimes even looking into outside factors if there was a split between two principles in a small business or something like that.

And, I think as a whole, we should be very cautious when we weigh it into here with policy, because what we're going to do is we may bring some consistency to this area, but we also take away a lot of discretion and latitude. And I believe that most of the very major registrars are acting in good faith and trying to sort this whole thing out, and trying to make sure that the rightful individuals have their registrations returned to them.

I did want to point out though that we possibly could look at existing policy, particularly with the TDRP and how that's working, how effective that might be, whether or not any improvements or enhancements or clarifications or consistencies could be implemented in the existing policy, like the TDRP. Because, I think that that tool perhaps is maybe underutilized, maybe it's not trusted, maybe it's applied inconsistently. So, rather than trying to impose

different standards all over the place, I think we should take the standards we have and put them under a microscope, and see if we're getting the outputs from them that we were expecting.

Marika Konings: Dave, Mike. Just to remind, if you can just say your name just for the record for the people that are listening to the recording afterwards.

Dave Piscitello: This is Dave Piscitello again. You asked a question that is actually not one of those three, and one of the things that I think could be useful for a working group, pre-PDP working group or whatever, to do is develop a matrix of the scenarios. And as you say, there probably are 80% that are fairly clear cut where you have an agreement between the originating registrar and the receiving registrar where you have sufficient documentation, where you have a clear paper trail, and those are easy.

Then, if you go through and you look at the possible scenarios, there might be a scenario where the two registrars disagree as to the quality of the data, the parties disagree as to the quality of the data. And if you tease out those, it might be useful to then follow what you were saying, James, and look and see whether the existing TDRP accommodates each of those cells in the matrix. So, that would require a little bit of rigor, but it might be useful to execute.

Even if you do look at the TDRP, and it looks like it's satisfying almost all of the cases, I still think that having an emergency action channel is probably valuable, and it's probably something that would merit consideration in policy.

And I do think that public awareness is probably valuable, because we have so many more domain registrants now and people are continuing to increase their appreciation of the asset value to their organization or to themselves of the domains they register. So, I think that that would be useful because you give people an awareness of what they can do, and it's also useful because it creates the appearance for the registrar community that they are interested in customer care and they are reaching out and trying to be proactive and helping people in situations where there might be a problem.

Mike Rodenbaugh: It's Mike Rodenbaugh. I agree with James on this one. This seems to me to be an area we really do need to be cautious with, because you could really open up a huge can of worms where almost every domain transfer could be questioned just by a simple allegation of fraud. And I'm also not really aware of a large problem here personally, so I'd love to get some statistic and understand. I mean, is this something that people complained

to ICANN about a lot anymore or to registrars, because personally, I don't hear it.

I do hear plenty of cases where the IT guy or the web host or the web designer got the domain in the first instance, but you're not talking about fraudulent transfer there. You're talking about legitimate transfer at the outset, and then later, the company realizes, oops, we should have registered that in our name not in that guy's name. But again, that's not a fraudulent transfer, so not something we're really talking about here.

So, I don't know. Do we have any data now or maybe that should really be the first step on this one.

Marika Konings: Well, maybe a question to ask to William and Mike, well, maybe James as well, how often do you come across these kind of cases? Does ICANN get a lot of complaints? Does the compliance team get many complaints specifically relate to this, or is this an area where you would need to investigate a little bit more, you might be able to come back to the group on that?

Man: Yes. So the contractual complaints.

Woman: Sir, say your name.

William McKelligott: Yes, William McKelligott. So, the contractual complaints team regularly receives complaints from the community about transfer disputes. I could probably find statistics for this group.

The ones that I have dealt with have been primarily related to transfers involving resellers, It's kind of varies here. I don't know if Mike had anything on that.

Mike Zupke: Yes. So this is Mike Zupke. So, I don't look at the complaints as closely as I used to. That's kind of been shifted to the compliance area, but I think that the genuine hijacking complaints have probably reduced since the implementation of auth codes across all GTLD's. That doesn't diminish the fact that when it does happen to somebody it's really significant to them, and there, I think, are often cases where a registrar says there's not enough evidence for us to try and undo the claimed damage that was done.

So, I think that the thing that the thing we hear from people who do have this problem is often that they feel there should be a process that they could

invoke rather than relying on their registrar to invoke a process to a disputed transfer.

Man:        Addressing your question Mike, I don't know that we have statistics on each of the types of categories or the buckets that these might fall into, but I know that it's probably in the order of hundreds or possibly even thousands a month of incidents where we're trying to kick off an investigation and figure out what happened during a transfer. And regardless of the actual number, there's a couple of high-profile cases, some involving ICANN contracted parties and some involving ICANN themselves losing control through an unauthorized transfer, losing control of their DNS.

So, I think it is still an issue. I mean, not being around for the original 2005 report I don't know if it's improved, but certainly, it seems to be an ongoing challenge.

Mohamed:    Thank you. I'm Mohamed (24:39 unintelligible). I just want to add a couple of comments on this. I'm not really sure about how this (unintelligible) who's collecting them, but I just want to give you a different perspective from the community.

Because I'm from North African, Middle Eastern parts of Africa, the major issue is when the name or the domain name expires, the next day it's gone, and there is a lag. Sometimes, people forget to renew their domain names and it causes a lot of problems for a lot of businesses, and it's puts off a lot of people also using the Internet.

There would say, look, I can't register my company's name, because after I start everything, and then the next day, it might go somewhere to Hong Kong or somewhere else and I can never get it again. So, I'm not really sure whether that will add anything to the discussion, but (25:24 unintelligible) know the process, then what to do, who do you talk to and when you go to ICANN.com, it's huge. It's like the U.N. It's very difficult to find information and to actually know who do you talk to and so on.

So for example, GoDaddy, to their credit, sometimes, they add value by saying we can cover you for another week or month or something, but you have to buy insurance policy or something, and that works, because sometimes people forget the exact date, and then at least they have some time to catch up and to renew their domain name.

So, that's really – we did a quick research some time ago, six months ago in the UAE and a few other countries.  Huge problem, because not only people lose their domain name, but sometimes, other people register their company's name is advance.  So, if you're XYZ and you want to register, all of the sudden XYZ is gone and there's nothing you can do.  And then people just say, well forget it.  I'll call myself XYZ123 or something, or even forget about the whole idea and say it's not worth it.  This is chaos.

So, it's sort of my take on it.

Marika Konings:   On the issue of expiration, I can maybe invite you to come to a workshop that we're organizing on Wednesday that's going to specifically look at the expiration of domain names and what happens during that process, or that part of the domain name life cycle, because there are indeed some issues, as you mentioned, where there have been complaints or questions raised.  So, that's a separate process that has started as well, so please come to that meeting and hopefully we'll hear more on that.

Coming back to one point that Mike made, because I'm not sure whether – I think it's an issue that comes up as well in one of the later PDP's related to the TDRP, because as I understand for the moment, it's only registrars that can actually launch a procedure.  And, one of the questions that I think that's being raised in one of the other issues but that might be relevant here is, as some of you mentioned, that that might be an area that this group might look at is whether it should be possible for registrants to launch a complaint.  It's an idea that might be considered.

I mean, I don't (27:39 unintelligible) level of TDRP, but from some of the materials I've read, I've understood that it's actually very little used.  I don't know if anyone has any information on that or experience.  I mean, sorry James.

Man:   Yes.  You know, I think that's a valid question.  The issue is, is trying to kind of balance that with the way that registrars try to work with each other.  So, I think one of the reasons that there aren't a lot of disputes actually filed is because I know GoDaddy for example, we try to have relationships with all of the other registrars, as many as we can.  And so, when we have a problem, the first thing we'll do is contact that other registrar.  We try to work things out.  And probably, 90 plus percent of the time, we're able to do that just to work it out between ourselves, and so, the dispute mechanism isn't needed.

So, I think that's a valid question. Should registrants be able to initiate that? We want to consider that. We don't want to create a huge onslaught of disputes, because the process that registrars have kind of worked out among themselves gets circumvented, because it goes straight to a dispute. When in that reality it might be able to get handled quicker and with less mess between the registrars.

So, I think that's a good question, because I think that's – we've seen that where there are some registrars who don't make that very easy for registrants to know that there is a dispute resolution system, and if you can't get things resolved, that there's another avenue. So, there might be something there we could do, but I wouldn't want to just circumvent the registrars all together.

Margie:        Yes, I just wanted to follow up on something Tim said, and Mike can probably comment on this. But the registrars have, though ICANN, put in contacts for transfer disputes, right Mike? Isn't there in the radar system where you actually identify an internal contact purely for transfer disputes. So, a lot of the stuff gets, just like Tim says, gets resolved behind the scenes quickly through those contacts. I just don't know if that's changed the experience of some of these hijackings recently or if it's affected it, but I know that that is a system that seems to work informally.

Mike Zupke:   Yes. So, this is Mike. Just, kind of as a little bit of background on how that works, ICANN has always maintained a list of transfer contacts at all registrars and they're allowed to voluntarily provide that information to us. We treat that as confidential information that's shared only with registrars and registries. It's supposed to be sort of an express channel for registrars to use. And so, what Margie's referring to now is that we've sort of automated that process of collecting the data and making it available through the web interface that registrars have, which I don't know if that's made it more usable for registrars or not, but that's kind of the system that she's talking about.

Marika Konings: So maybe last comment before we move on to the next issues, because we still have four other issues to cover as well.

Man:          Yes. I was just going to add to that as well by saying that the TDRP is a time consuming process or can be compared to something that's a little bit more expedited, I think, when you're dealing with a claim of hijacking. You know, you're looking at hours of reaction time, and just getting that process started could be longer than that. So, it really cuts down on that window.

Marika Konings:    Any final comments on this issue?

Man:               Actually, I just have a question.  Does an incorrect suspension of a domain fall into the category of something that would be urgently returned?  So, if somebody has a false positive in identifying a domain as a phish domain or as a spam domain or a **fast flux** domain, and it's suspended, is there is a separate process that falls outside this process of most registrars?  This is perhaps an aside, but I was just curious.

Marika Konings:    I think people might have to come back to that one.

Man:               Yes, can we?

Man:               (32:03 Unintelligible)

Marika Konings:    Okay.  Maybe we can then continue to the next issue, which raises a question on whether there should be additional provisions for undoing inappropriate transfers.

                   So, the IRTP is clear that the registrant can overrule the admin contact but how this is implemented is currently at the discretion of the registrar.  Some of the comments received during the different public comments periods indicated that the return of inappropriate transfer is considered to be difficult, the process seems unclear as it's left to the registrar to define how this is done.  I guess, there are different practices used.

                   This is an issue that also came up in the IRTP Part A working group who also recommended that the appropriateness of a policy change that would prevent a registrant from reversing a transfer after it has been completed and authorized by the admin contact should be considered.

                   So, I copied here a comment that was actually put in by GoDaddy on this issue and you can read online, and I'm hoping that Tim and/or James would share a little bit more information on this.  So basically, saying as well that there's a lot of unclarity in this area, and they've raised a question as well, is this the intent of the policy or is this indeed an area that needs further work.

                   So, who would like to comment?  Mike.

Mike:              First of all, not really grasping why this is all that much different from the previous issue and why they wouldn't be dealt with in much the same way, if we're assuming we're going to deal with it.

Marika Konings:   As I understand, part of this issue that you have with the registrant can overrule the admin contact.  So in certain cases, understand that once the admin contact has approved and has all gone through the whole process, it has been transferred, then the registrant suddenly stands up and "Oh, I didn't authorize it.  Please roll it back."  I understand that causes a lot of problems and a lot of delays.

Man:   Sure.  But basically, they're just saying it was a fraudulent transfer from the admin contact.  Is that correct?

Marika Konings:   Tim?

Tim:   Yes.  I mean, that's basically true, but the difference is, is that the registrar that took the change or the gaining registrar will say we followed the process according to the policy, the admin contact did approve it, and so they do want to correct it.  But then, we run into that issue usually where the registrar wants to be indemnified.  And I know GoDaddy has been – we take that position as well.

So, if we're going to reverse what we saw as a good transfer, because the registrant overrides it, then we just want to be indemnified from any possible action that might take place after that as a result.  In other words, we don't want to admit yes, this was a fraudulent transfer and we were a party to it. It's a different situation.

And so that raises some issues, because some registrars are okay with indemnifying under that circumstance, some aren't.  It just depends on the registrar.  So it does raise a little bit different issue, because it was actually technically a good transfer at the outset.

Man:   So here, yes, what you're basically you're asking is for the registrants to indemnify you in the event the admin contact comes back and says it was legit whereas, in the first case, you would really want the gaining registrar or the – yes – the losing registrar would want indemnification, right?

But I don't – I mean, indemnity is a whole other issue.  I don't know that we really developed policy around that, around registrars indemnifying one another, right?  Never done that before anyway.

Tim:   This is Tim again.  Yes, true, and I don't think that's necessarily what we're suggesting, but is there some policy change that's needed or clarification that

will allow registrars to take care of that situation without expecting that kind of thing?  Do we need to look at whether or not the registrant is the only one that can actually approve a transfer or if they're going appoint an administrative contact as a transfer authority, then that's not revocable.  I think that's the kind of question that we're actually raising.

Marika Konings:  If I recall well, I think something that was discussed in the IRTP Part A working group as well, was saying well, we don't want to take away the right for the registrant to object in a certain window of time.  But, once the transfer has been completed and fully authorized, maybe then it needs to be looked at that it cannot be rolled back, if indeed it has been properly approved by the admin contact.  And that was one of the areas that was discussed.

Barbara:  This is Barbara.  Getting back to one of our comments (37:11 unintelligible) registry (unintelligible) and I will say that from our perspective, one of the things that (unintelligible) registrars (unintelligible) for our review based on the registrants objecting is they provided an affidavit from the registrant (unintelligible) identity and all that (unintelligible).  I don't recall (unintelligible) indemnification from the registrant or not, but may be something to consider.

Marika Konings:  Any other comments or questions?  James.

James:  Just to add to this, going back to the IRTP A PDP is that the registrant contact information, especially unless we're talking about a thick registry, is an invisible entity to the gaining registrar until that time.  So, not only is it this person that can or this contact that can override the administrative contact, but it also doesn't really leave them any recourse to contact that person.

Jeremy Hitchcock: This is Jeremy Hitchcock.  Just another concept on the whole administrative contact is that registrars are always validating who the actual entity that owns the domain name through proxy, through some sort of web interface, through some sort of email password combination, and it's that itself has some issues for verifying that an actual contact is the person who is in the Whois information is the person that actually registered the domain name.  And so, there's always this not a mismatch all the time, but certainly, whoever's in Whois as the admin contact, as the owner of the domain name, is sometimes different and authenticated by the registrar through a different means or through some sort of secondary token.

Marika Konings:  Any other comments, questions?  No?  Then I propose we move on to…

Man:                 (39:20 Unintelligible) same thing again though, it'd be really helpful before we start digging into possible alternatives is to understand the scope of the problem.  Getting stats around this again would be really useful to see if this is still a problem four years after these comments were taken.

Marika Konings:      Barbara, would you be in a position to share some data on how frequent this occurs?

Barbara:             I don't have my papers right now, but (39:45 unintelligible).

Marika Konings:      Okay.  That would be great, and I think we'll look as well from the compliance department and the services department at ICANN to see if we can pull up some data there as well, because I think it would be…

Barbara:             (39:55 Unintelligible) overall the number of transfer disputes (unintelligible), which is (unintelligible) at this point.

Marika Konings:      Okay.  Thanks.

                     So moving on to the next issue, which raises the question of whether there should be special provisions for a change of registrant (**40:20 unintelligible)** change of a registrar.  So, the IRTP does not currently deal with changes of registrant, which often figures in hijacking cases.  Some of the comments received indicated the liability for foreign transfers currently lies with the losing registrar, and some registrars, therefore, have taken preventative measures such as optional transfer prohibition periods following a change of registrant.

                     Some time ago, ICANN did clarify that a registrant to change the Whois information is not a valid basis for denying a transfer request, as some complaints had been received in relation to that.  Some registrants consider such measures unnecessarily restrictive, so the fact that if they change Whois data, they cannot transfer the name out for a certain amount of time.

                     I think this is one of the areas where the question should be asked how much of an issue this still is, because I think the clarification that most provided by ICANN has, I think, at least taken away the mandatory nature by which some registrars applied this procedure.  And as I understand, this has now changed into an option where the registrant, when they change the Whois information details, they can actually opt in to two months or three months – I don't know what the standard is – prohibition period for a transfer.

So, the question there as well is, is this still an area?  Are there still complaints received?  Do registrants still feel that they should be able to change that even if they've opted in at that stage?  So, I would like to open the floor for comments, questions.  Kind of again looking to Tim and James, what is the practice at GoDaddy.  How do you deal with that?  Do you feel this is an area that would require special provisions?

James:          Let me just clarify something.  I think at least with GoDaddy, I think most registrars I'm aware of, it's not optional.  It's mandatory where if you change your Whois information, you cannot transfer for 60 days.  You don't get the option to opt in or out of that.  It's absolutely mandatory.

I think there's an issue there with some registrars about disclosing that fact.  It's not disclosed predominately and some registrants don't realize that that's happening, and that they're stuck with their registrar for another two months, when in fact, they want to move it to their own registrar after a transfer.

Marika Konings:   Tim.

Tim:            We've refined our process over the years as issues have risen, complaints, concerns of ICANN and others.  But, the way we deal with it right now is that we look at it as if a domain name is changing hands from one registrant to another, it's a different situation.  It's not really something that we're required to support in our RAA.  Updates to the Whois is one thing.  A completely new registrant is a whole different thing.

And so, one thing is we want to make sure that we have a registration agreement in place with the new registrant.  So, we have a process that you go through if you're going to do that, that both the losing registrant and the gaining registrant is made aware of the fact that this is a service that we're going to provide to you.  We provide it free under the condition that once completed, the domain name, you agree that you won't transfer the domain name for 60 days.

And then we explain if that's not going to work for you, the option is transfer the domain name first and then complete the change of ownership at the new registrar.  And so, if they complete the process, they've been fully informed and then the domain name is held locked for 60 days.

We make exceptions to that.  I mean, if that happens and someone calls and it's an issue, we do some due diligence, make sure things are cool, and then we'll quite often lift that restriction and let them transfer the domain name.

So that's kind of the way we handle it. I know it's probably handled differently by other registrars. But, that is key to us because that's been – we've seen in the past that it's probably the first thing that happens before a hijacking attempt is that that Whois information is changed.

In fact, the way we do it now, it's – there has to be an actual change of registrant. I mean, at one time we were preventing it even if you – if anything with the transfer authority changed, any of the contacts, so if the email address of the admin contact changed or if the email address that we keep on file that isn't public of the registrant changed, we would do it then as well. We've stopped doing that. We think that's opened up a window of opportunity for hijacking, unfortunately. But, I think it's something that needs to be looked at, because it precedes attempts to hijack very, very often, and I think even the current report from the SSAC has kind of recognized that fact as well.

Marika Konings: Any other…Mike?

Mike: I do think that's really the problem is GoDaddy does properly notify people of this, but like Tim said, all the registrars are kind of different, and this maybe is one area where there ought to be a consistent standard, firm rules.

Marika Konings: So, Mike, William, is this an area where ICANN gets a lot of complaints? Are you aware or can you look into that and maybe share it with the group at a later stage if you don't have it off hand?

Mike: Yes. So I can say – this is Mike – we get considerably fewer complaints than we did since the advisory was posted. I think that a lot of registrars have been able to look at that and try to conform their procedures accordingly.

I understand from what Tim is saying that they've got certain procedures in place. They want to create an electronic paper trail of changes of registrants. That's generally in the interest of protecting their customers. So, I think, though, if there's a sense that that's not a desirable thing, then the advisory doesn't solve that problem. I think that should be clear. And, I'm not saying that what they're doing is a problem, but if that's the sense that what they're doing is still not acceptable, then something besides the advisory would be necessary.

But also, I think it's worth looking at the thing that Tim mentioned, whether it changes to, for example, administrative contact email address should

perhaps trigger some sort of a delay in transferability, and I'm not saying that's necessarily right, but I think it's something that should be looked at by the community.

Marika Konings:     Dave?

Dave Piscitello:     This is Dave again.  The wording of the third bullet where it says "the information is not a valid basis for denying a transfer request" sort of tickled something in intrusion-detection corner of my brain, which is that it's always dangerous to use one marker to declare something as being a positive case, because you're only relying on that as the distinguishing factor for a true positive versus a false positive.

One of the situations that I know has happened to me on several occasions with transferring registrations is that the transfers occur close to the time when somebody is about to renew, and the cost is something that they want to just actually avoid.  For example, if you are supporting a not-for-profit Website and that not-for-profit wants to actually move the site, and this has happened to me on a couple of occasions, what we've done is we've essentially gone through the process of I registered the domain, and got people set up on a web server, and then their web service got a little bit more than I wanted to handle as a volunteer, and they decided to upload it to GoDaddy, as an example.  And so, my goal was to simply get the domain name into the new contact and new registrant's identity.

So, one of the things you might consider is that you could think of additional parameters that you might use.  And, if contact information is being changed within a certain number of days of a renewal event, maybe that's not quite as clear cut a case as a transfer that occurs any other time of the year when information is modified.

These are just off the top of my head notions, but one of the things that I'm suggesting is that maybe you don't want to only rely on one factor to prohibit it, but think of other factors that would also help you distinguish between a hijacking case and just a fortunate or unfortunate sequence of events.

Marika Konings:     Margie?

Margie:     I just wanted to follow up on what Dave was saying, because there are a lot of legitimate reasons for a registrant change before a transfer.  Like, a secondary sale of a domain name, what would typically happen is you'd have a buyer who purchases the name, then they want to move it to their registrar.

So, there's a lot of legitimate reasons for why that might happen, and you want to make sure that you're not somehow preventing those legitimate situations.

Marika Konings: James?

James: Agreed Margie, but going back to what Tim was saying, there really isn't a mechanism for that sale or I think an obligation for registrars to police that commercial market. Whereas, there is with IRTP, this is just specifically on the transfer. So exchanging - if you and I, for example, were going to buy and sell domain names and we both had accounts at GoDaddy, then this would not ever come up as an issue. It's the fact that those things are trying to occur simultaneously or trying to attach something to an existing policy that is causing some of the confusion.

I also wanted to touch on something Dave said earlier relative to the SSAC report that's not out yet. Is that correct? I've been chatting with Jeremy, SSAC 40.

(Crosstalk)

Dave Piscitello: This is Dave again. I think it's fine for you to talk about the report. I mean, it's not published, primarily because we wanted to share it with the registrars and give you an opportunity to have this kind of discussion. So, by all means, if there's something that you want to talk about, let's do it.

James: Well, I don't want to steal too much of its thunder, but…

Dave Piscitello: The goals is to not have thunder, it's to have agreement.

James: There's an excellent point in there about having multiple points of contact relative to a registration, and not necessarily having all or nothing global transfer authority, or Whois change authority, or any other types of operations that you can perform on a registration, but having perhaps tiered or limited or restricted authority for some contacts, and then having administrative authority for other contacts. And I think that when we're talking about a change of registrant prior to a transfer, what we're talking about from an intrusion detection, is we're talking about a brand new account on a mainframe, let's say, that's seconds old having root level authority. And I don't know that any IT or CISO would go for that in the world.

So really, that's what we're talking about is something that's brand new. And one of the ideas I think that was even touched on in your report is the idea that think of that 60-day or 45-day or 10-day cooling off period as a way to age the account, to get an idea for what purpose it was, maybe even allow for a authorization window by one of the existing accounts or contacts on that registration to say that it's legitimate or not.

So, I think that using that example, if you had someone that came onto your network, created a brand new account, and as soon as they hit the submit button, they had root access to everything that you had. I think most people would see the problems there.

Marika Konings: Yes. I think Dave will definitely have you back on the working group when that report is out to share a bit more on that if you don't mind. So, when that SSAC report comes out, maybe you would like to join the working group again for a session to explain a bit how that might work. So, great.

Any other comments or questions on this particular issue?

So then, moving onto the next one. I think the next two are very closely related, so I'll quickly run through both of them, and I think then we can open the discussion. They're both related to the registrar lock status, and Question D is whether there should be standards or best practices be implemented regarding the use of registrar lock status, what may, may not be used, when it should or should not be applied.

The different public comment periods indicated that there are many variations in which the use of lock status occurs. Registrars have different practices. This seems to have added a level of complexity. A lot of registrants do not understand or are confused about how they can actually unlock their domain names.

So, the consideration should be given whether there's a need for greater standardization of locking and unlocking functions, or whether there should be more precise definitions in the IRTP on the appropriate use of lock status.

So, closely related to that is the last issue on clarification of Denial Reason Number 7, which basically states that a domain name was already in lock status provided that the registrar provides a readily accessible and reasonable means for the registered name holder to remove the lock status. So, as said, the practices vary, so registrants often don't know how to do this,

and again, should there be greater standardization to this mechanism, a more precise definition.

This issue was already discussed in a previous PDP on denials, but I think, and I'm going to turn to Olof to share a little bit more on that, but I think it was deemed that it required more time and discussion to solve this issue, that it was decided to pass it on.  Again, as it is closely linked to the previous question.  I think the group might want to consider taking both of those together and addressing those.

So Olof, if you can maybe tell us a little bit more about what has already been discussed in relation to this issue and what the group found at that stage, that would be great.  Thanks.

Olof Nordling:     Absolutely.  Olof Nordling, and once upon a time, there was a PDP…

On clarification of denial reasons, two out of four, we achieved clarifications of, and those have been changed, but two were left over, and this is one of them.  Well, if you look at the denial reason, I mean, in this drafting group, which addressed it, looked very much at the part, which says "a readily accessible and reasonable means", and that was sort of the core provision. It's pretty rubbery, and the question was could that be more specific or better defined.

And it was discussed at some length, and the more we discussed it, the more realized that the reasons and use of register lock varied between registrars.  And actually, to be more specific, and especially in that particular time frame, (57:10 unintelligible) come with some kind of clarification of it, wasn't really doable, and could have adverse effects making it, well, in some cases, unnecessarily difficult, and in other cases, taking away the existing options that the registrars have, or for the registrants to opt in for particular security prohibitions.

So, well, the advice:  The recommendation was really to link this (57:45 unintelligible) dodge it from the perspective of that particular drafting group, and recommend that it was addressed together with this wider issue of the use of register lock.

So, while Tim and others maybe you can expand if needed on the work in the previous working group, which concluded its work just around a year ago from that.  But that's essentially, the conclusion was well, this is more than a

clarification that's needed, and it better be addressed together with other discussions about register lock status as such.

Thanks.

Marika Konings: Tim, please go ahead.

Tim: I think that's pretty much it. That original PDP group or the original group where this was discussed was only asked to look at clarifications of some specific reasons for denial, and as Olof said, we just felt that this required probably something more than just a clarification.

For example, a number of registrars, they apply a lock, sort of an internal lock. It's not something that shows up when you do a Whois on a registry, so it might not even look like the name's locked at the registry potentially. Yet, the registrar has it sort of locked internally. So, that's something registrants may or may not be aware of. And then some registrars do that as a default when the domain name is registered. Some offer services around that kind of a lock where a registrant can opt in for additional security, additional measures need to be taken before any changes can be made to the domain name, that kind of thing.

So, it's just a wide range of issues surrounding why there's these various lock status, and that we felt it was more of a policy issue than it was just a clarification. So that's kind of why it was moved into here.

Marika Konings: Maybe a follow-up question to you then; what would be a potential solution or what do you think this group should be looking at? Is that more defining what lock status can be used for or obliging registrar to use a different name for other locks they might use that are not the one defined in the IRTP, or…?

Tim: Well, just from my perspective, I think what the issue is, is the registrant being aware of what's happening so that they're aware of the state of the domain name. They're aware of what they need to do when they want to transfer the domain name, and I don't think that's necessarily always the case.

They may not really understand what the registrar himself has done to the domain name or what is affecting it. And they may not always be clear how to unlock. I mean, even at GoDaddy, we'll get questions about how to unlock the domain name, yet, if you log into your account, it's a simple link to unlock

it. So, we're always looking at well, how can we better inform registrants about that process.

So, I think that, to me, is the key issue is just make sure registrants are aware that they know what's necessary in order to make modifications to their name or to transfer it. I don't think that's necessarily always the case.

Marika Konings: Mike, William, is this an area where we get a lot of complaints at ICANN, people being confused on how to do this?

William McKelligott: So, this is William McKelligott. I would agree with you, with Tim. Primarily, the registrants are a bit unaware of why their domain name is in lock status or what that implies or how to get it unlocked. And again, primarily, the type of complaints that I have dealt with have involved resellers, which I think adds another wrinkle into the story, because many times, these resellers become advocates for the registrants, and we're talking about several hundred or thousands of domains that they want to help transfer to another registrar.

So, it'd be kind of a variation of this, but I would agree that there is some type of lack of clarity, what this implies, how it came to be, and how to actually move beyond being locked, having the domain name in lock status.

Marika Konings: Olof?

Olof Nordling: I would, from a logical perspective, see this very much as a tail of the dog. The dog itself is more the use of register lock, and then, we can sort of address this question whether that could be clarified, that particular context. So perhaps you could back one slide to D. I think that's a logical sequence to address them, D before E.

Marika Konings: Any other comments, questions?

Well, with that, I would like to thank you all very much for coming at this early hour and participating, and again, any of you that are interested in continuing discussions on these issues, please pass your details to me or Glen when she comes back, so we can add you to the mailing list for this working group.

And as mentioned, we expect the Council to discuss this issue in further detail on Wednesday when they will take a decision on whether to initiate a PDP on this issue.

Up here, you will find more information on where to find the (1:03:58 unintelligible) information and how you can participate. A Wiki has been created, so even if you're not interested in getting on the mailing list, you can monitor discussions there, and as with any PDP, there will be opportunities to contribute during public comment periods and follow our meetings we will be organizing.

So again, thank you very much and have a good day.