ICANN Transcription
Privacy and Proxy Services Accreditation Issues PDP WG
Tuesday 28 October 2014 at 1400 UTC

Note: The following is the output of transcribing from an audio recording of Privacy and Proxy Services Accreditation Issues PDP WG call on the Tuesday 28 October 2014 at 14:00 UTC. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.

The audio is also available at:
http://audio.icann.org/gnso/gnso-ppsa-20141028en.mp3

On page:
http://gnso.icann.org/calendar/#oct

Attendees:
Steve Metalitz - IPC
Graeme Bunton – RrSG
Griffin Barnett – IPC
Frank Michlick – Individual
Don Blumenthal – RySG
David Heasley-IPC
Jim Bikoff-IPC
Chris Pelling – RrSG
Kathy Kleiman – NCSG
Justin Macy - BC
Susan Kawaguchi – BC
Kristina Rosette – IPC
Darcy Southwell – RrSG
Paul McGrady – IPC
Sarah Wyld – RrSG
Victoria Scheckler - IPC
Michele Neylon – RrSG
Val Sherman – IPC
Alex Deacon – IPC
Todd Williams – IPC

Phil Corwin – BC
Volker Greimann - RrSG
Holly Raiche – ALAC
Theo Geurts - RrSG
Osvaldo Novoa - ISPCP
Tatiana Khramtsova - RrSG
Stephanie Perrin - NCSG
David Cake - NCSG
Susan Prosser - RrSG
Christian Dawson - ISPC

Apologies :
Amr Elsadr - NCSG
Carlton Samuels – At-Large
James Bladel – RrSG

ICANN staff:
Mary Wong
Amy Bivins
Glen de Saint Géry

Glen de Saint Géry: This is the PPSI call on the 28th of October. And on the call we have Graeme Bunton, Holly Raiche, Steve Metalitz, Tatiana Khramtsova, Don Blumenthal, Theo Geurts, Sarah Wyld, Alex Deacon, Chris Pelling, Phil Corwin, Frank Michlick, David Heasley, Jim Bikoff, Todd Williams, Susan Kawaguchi, Darcy Southwell and are there any other people that have joined the Adobe Connect room that I haven't mentioned? Volker Greimann, Val Sherman, Todd Williams.

And for staff we have Mary Wong, and Amy Bivins and myself, Glen de Saint Géry. Have I left off anyone that has joined in the meantime? And we have apologies today from Carlton Samuels, and James Bladel. Has anyone else perhaps noted any apologies?

Thank you very much. Don, it's over to you.

Don Blumenthal: Thanks, Glen. Just for what it's worth, James, as he put it is talking with diplomats. He's at the Plenipod over in Bussan so have no clue what the time

difference is but that what he's doing and he decided not to call in. I can understand that.

The usual reminder, please update your SOIs. Yeah, Volker, you might have to try to download another mic or call in or get a call out. Back up to chat. In any event please update your SOIs. I don't think we have any new members since the last time although somebody promised me repeatedly in Los Angeles that he would be sending us one so we'll see.

First thing I want to do is take a look at the updated work plan that we sent out. It's on the screen now or you should have received it in an email. We're actually still in very good shape with respect to our initial work plan. That was an extremely ambitious outline.

We've spent more time on E and F than I think we expected. But we're still lined up to at least have a draft out I think by - well two weeks ago we were saying by Marrakesh - at this point I'll say by whatever and whenever. Keep my flexibility going here.

You know, for the most part it follows along with what we've been talking about in terms of discussing issues, reviewing them, writing. But we have two weeks there from now that weren't there before. We talked about having a SME presentations and I'll continue to use my subject matter expert terminology from law enforcement - one week in data protection, another - just a second. My voice is getting better than it's been but still isn't quite there so I'll be jumping off real quick - mute pushes.

To be honest I wanted to - well, number one I want to toss this version out - well we did toss it out; I want to toss it out for discussion in general but also I think with a focus on what we're talking about for November 11 and 18.

To be honest I thought we were drifting toward a consensus on doing something like those but in LA - but more so afterwards on the list. And I want

to make sure of that because I've seen some concerns that we hadn't - that I hadn't heard before. I think this is a reasonable schedule. It's still an aggressive one but reasonable. It'd be really nice to get that prelim report out and then have a final ready by wherever we are for the second meeting in 2015. Any thoughts? Is it perfect?

Just going down the list and see who's here to see if I can put somebody on the spot. No. Okay we - given all the work that law enforcement has done within the ICANN community it would be very easy to identify people who talked to us.

I have two names so far that have been suggested for people from the data protection world. They both seem appropriate to me but they are both - have a European background which is fine because that's where protection frameworks were pioneered.

But if anybody has any thoughts of people we might be able to reach out, for example, with APAC, Asia Pacific economic community because they have a privacy framework. A number of countries have their own, for example, in South America. If you have any leads there it would be great in terms of having a balance - or not balance, a broader set of viewpoints. There are some differences in approaches.

Okay, no comments on the work plan. Why don't we move on to - sorry about that - why don't we move on to the face to face meeting. I'm looking at Holly's comment there. Just to make sure we're on the same page I was referring specifically to APEC framework.

Oh, but I'm a firm believer in getting the specific country representatives because, you're right, they do vary. In Europe there's a variety under the EU framework. So APAC or APEC is fine, however we want to approach it. So again if you've got thoughts from that territory you and David were in mind when I mentioned that region, please.

Okay, based on comments that I received, whether directly or just chatting in the corridors, I think the face to face went very well. It was a worthwhile exercise, say, as a pilot for ICANN going forward. But that's largely because - I say that because I think it was very successful for us being able to sit together face to face, see who was talking, see reactions, really zero in on specific subjects for an hour and a half apiece without a lot of distractions that sometimes happen when you're on the phone. I think it was real productive.

Mary sent out I think preliminary conclusions based on what we talked about there. And first off I'd like to see if - I appreciate it, David - I'd like to see what reactions are to what we all came up with, first staff but then Graeme and Steve and I took a look in terms of what our conclusions were from the three sessions.

Steve.

Steve Metalitz: Yeah, thanks. This is Steve Metalitz. First, I agree that the session went pretty well. I think we made some progress. I think, in terms of what's on the screen, I think there's a big difference between Roman 1 and Roman 2. I think Roman 1 does reflect kind of the discussion quite - pretty well.

I know Val had put in some comments on it on the list - Val Sherman - so we might want to discuss those. I think 2 is a little bit different category because it's basically Thomas's notes as amended by some - by some of the members. And I don't think it's - or some of the participants - I don't think it's quite - there wasn't really any discussion of this, let's put it that way, very little.

But, you know, it's certainly grist for the mill when we turn to disclosure. But I think the relay stuff that's up there is a good starting point. I mean, in terms of adding this to what we've already done as far as a preliminary conclusion

with some points that Val has raised I think it's worth spending a little time on that. Thanks.

Don Blumenthal: Great. Thanks. Holly.

Holly Raiche: Could I ask why we're using the term "disclosure"? We were talking about - as I understood the language - relay was simply forwarding on a message; reveal, as I understood it, simply meant you revealed to the requestor only details and disclosure was - or more publication was simply details are published which is not what we're talking about.

So I'm just asking why are we using the term "disclosure?" Is that there instead of the term reveal? Just a question.

Don Blumenthal: Well I think what we had come up with was that we would, except for shorthand, replace the term "reveal" with "disclose" which is provide the information to the requestor or publish, which is to post it out on - within the Whois system.

Holly Raiche: But they're different things.

Don Blumenthal: I know that. Well what are...

((Crosstalk))

Holly Raiche: No, I mean, my question is for disclosure do we mean reveal? Is the Heading 2 actually the discussion we had on reveal?

Don Blumenthal: Steve, is that a new hand?

Steve Metalitz: Yeah, it is. This is Steve again.

Don Blumenthal: Okay.

Steve Metalitz: Holly, if you look at our preliminary conclusions on Section F, Charter Category F, the first one is recommended definitions.

Holly Raiche: Yeah.

Steve Metalitz: And there's a definition of publication, which is publishing in Whois...

Holly Raiche: Yeah.

Steve Metalitz: ...there's a definition of disclosure. So I think it's being used in that sense.

Holly Raiche: Okay it's just I'm - I was just a bit surprised to see because I guess I was used - because we actually talked so much in - on October 10 just about relay and reveal so I was a bit surprised by this but, you know, go ahead.

Don Blumenthal: Okay, I'm just checking chat here. Thanks, Steve. Kathy.

Kathy Kleiman: Hi, all. Coming off mute. It was nice to see everybody in Los Angeles. In light of Holly's critique maybe we should - and because there are other people who may not have done the shift with us - maybe we could say reveal-disclosure because it is a category of reveal that we've discussed, that might be clearer.

And the suggestion that was made there that we're dealing with intellectual property complaints in particular, I think should be adopted. It's there kind of tentatively but I think that's really the context that we were talking about. Everything under the reveal-disclosure discussion was intellectual property and particularly trademarks and copyrights certainly not patents. Thanks.

Don Blumenthal: Not everything perhaps. I think I did talk a little bit about the law enforcement anti abuse perspective will work differently particularly in terms of how reveal

and relay might or might not work together and whether we should require relay requests before we require reveal requests. Kathy, new hand?

Kathy Kleiman: Absolutely. Absolutely. But I thought that we were going to handle disclosure for abuse reasons in a different - it was my sense we were going to handle them kind of at a different time because, if I remember correctly, Don, what you said, and accurately so, is that there may not be any turnaround time to the registrant in an abuse situation.

What we're talking about here - so I thought we had kind of almost saved that as a category for another time but that what were talking about here was the allegations of intellectual property which the proxy privacy provider is really under no obligation to investigate but that they're stating with great specificity and then giving the registrant an opportunity to respond.

Again, I thought that was kind of the unique mix that we were creating for certain types of intellectual property requests.

Don Blumenthal: Okay that's fair. I was just more reacting to we only talked about intellectual property. But you're right, the other category - well I think it will take some more focused discussion which we hopefully will get when law enforcement is on the line and use that to come up with some kind of - well, see if we want to use that to come up with some kind of unified model - unified baseline.

Are there any other comments here? Steve.

Steve Metalitz: Yeah, I guess - this is Steve Metalitz. I guess I'd be interested if anyone has any objection to the relay points with the changes that Val talked about which were basically to change the "shoulds" to must. I mean, should - if we're talking about minimum standards here it would be best to express them as such rather than should which is a bit squishy.

And then I think she's - Val has teed up the issue in the last brackets on the second point there about cost and who should bear the cost of this alternate delivery mechanism. So I guess I'd be interested if people have comments on that.

Don Blumenthal: You anticipated where I was going to go next although I was going to - I'm not trying to pull Val into the discussion directly. David.

Steve Metalitz: I think her points on the right there.

Don Blumenthal: They are. I like to vary participation. David, I saw your hand up for a second, is it - oh okay well we'll look for you. Well let me ask for reactions to what Steve said. Should we pull - should we just make the edits that Val suggested? Any objections to making the edits that Val suggested? I think they're fairly straightforward. Kathy.

Kathy Kleiman: Yeah, I'd like to ask the providers what the implication is of...

Don Blumenthal: Yeah.

Kathy Kleiman: ...changing "should" to "must." I think that that's a big change. And one that removes any of the discretion that we've heard throughout the discussion that proxy privacy service providers want to keep.

And in terms of mandating costs be put on the customer, again, let's think about some of those really, really crazy examples that Graeme posted. And I don't remember who, you know, this was to the meeting - the face to face meeting. But Graeme posted all sorts of strange things: diapers, sadistic pictures, you know, there's a lot of stuff that occasionally is requested to be passed on.

Is it appropriate? Are ultra-harassing letters appropriate? You know, really vile cease and desist letters that are kind of beyond the pale and would be

very scary for receipt. I've seen some of those. You know, we had left some room for the discretion of the proxy privacy service provider on purpose and so I'm reluctant to move it. Thanks.

Don Blumenthal: Okay Darcy.

Darcy Southwell: Yeah, so I guess I would say as a provider, if we're going to change "should" to "must" I'd also want to see a qualifier in there that as a provider we have been able to correct the situation. It seems to me that if we have - the way I read this is if we have a failure we have to - if we change it to "must" we just have to turn around and immediately notify the requestor.

And I think the better bet for everyone involved is to get the provider to make sure that they have a workable contact with their customer for a variety of reasons. And so if we're going to change it to "must" I'd rather see a qualifier added that that is only when we can't correct the delivery failure somehow. Thanks.

Don Blumenthal: Okay. Steve.

Steve Metalitz: Yeah, this is Steve. First, I'd be open to Darcy's suggestion there as far as the first bullet. But I think let's - again let's put this in context, I mean, if we're talking about minimum standards what are the circumstances in which the service provider should have the discretion when it knows that it's relay has failed and that it's been undeliverable. When should they have the discretion to not tell the third party requestor that?

I'm not sure that - this is not the same discretion we're talking about or we were talking about in the disclosure context, this is a narrow circumstance in which an electronic communication has been sent for relay and the relay has failed. So I don't see the need for discretion as much in that circumstance.

And then, you know, as far as the - Graeme's diaper and those other very amusing examples, they actually are totally irrelevant here because this is only when we're talking about an electronic communication that has failed. So - and there's a lot of flexibility here that says some alternate for further form of notice. And we talked in LA that there might be a couple different ways to do that. So this provides as much flexibility as possible in the context of trying to get the message to the - to the third party.

And remember, this comes in with our already-adopted preliminary conclusions that allow, you know, that provide for the use of a spam filter or other types of commercially reasonable mechanisms. So I think let's put this in context; this would be coming at the end of the other conclusions that we've previously adopted and would really just deal with this narrow circumstance in which electronic communication has been attempted but has clearly failed. Thanks.

Don Blumenthal: I can't let Graeme's diaper go without saying something. For what it's worth somebody at (MOG) thought the solution to that would be 3D printing - to make a copy.

Michele.

Michele Neylon: Hi. Michele for the record. I'm not comfortable with changing from "should" to "must" at all. I think "should" is fine for now and we should - and it should be left as-is. I mean, the thing about all this is we're currently working our way through a lot of very complex contentious issues. While there may have been preliminary agreement on various points it's not definitive.

And as the entire patchwork comes together to make the wonderful quilt that will be the proxy privacy accreditation - whatever the hell we're calling it at the far end I think a lot of our opinions and views on various aspects of that - of the patchwork will change over time. Thanks.

Don Blumenthal: I like that patchwork description. David.

David Cake: Right. There was the issues that were raised in that email about when electronic communication has been attempted and failed then that should mean that the cost - then the costs should not be paid by the person who's attempting to contact but revert to the customer. I don't - I had issues with that sort of suggestion basically.

The issues of whether - if - for a start there's an issue about there's only really an actual, you know, something is being done wrong by the PPSAI customer if they are - you know, if they're providing an email address that just doesn't' work it may be the case that they are choosing not to reply or it is getting caught up in spam filters or something.

But there are legitimate reasons why they might choose not to reply, where they feel that they, you know, they've received a legal communication and they don't feel that it is appropriate to reply to. I mean, of course there are - there are, you know, bad actors in, you know, in those who have tried, you know, there are bad actors in - on that side of the equation as well in - you know, copyright trolls and so forth.

So we don't - just the fact that someone has - communication has been attempted and failed does not necessarily presume some wrongdoing on the customer's part. Though obviously if they're not actually providing a working email address, like we're getting hard bounces or something that does mean they are failing to pursue their responsibilities as a registrant.

But the main thing is that also that idea of reversing the onus of cost needs to be borne in mind of what is a reasonable cost. I think just, you know, just because the - we have to consider the case where it may be that the registrant has failed to provide a proper email communication and that other means need to be attempted but that doesn't mean that you can - all the examples we saw in the face to face that you, you know, that doesn't mean

that they - you can send them on - that suddenly the customer should be paying to receive 19 pounds worth of documentation or the other weird and wonderful things.

So just basically we need to consider that onus of cost in that there may be some - maybe if a customer does not provide an email address there should need to be some reasonable costs of other means of contacting them, but we can't just do that as a total straightforward principle. So that was basically my concern about the ways Val had suggested that we change that onus of cost issue. So that was all I really had to say.

Don Blumenthal: I appreciate it. Well why don't we just move on? Michele.

Michele Neylon: Thanks. Michele for the record. David seems to be kind of mixing in two things here that I think we've already discussed at length. I mean, the issue that Steve and others is concerned about is non-delivery of a communication not lack of response. I think we all agreed that lack of response was perfectly okay.

I'm also a little bit concerned about this burden of cost concept. And I'm not too sure exactly where he's going with that. I mean, I would have concerns about loading costs onto my customers just because some third party has got nothing better to do with their time than send lots of spurious requests.

I mean, we're currently dealing with a rather entertaining, though quite frustrating, abuse, in large quotes, where one company is saying that another company has been taking abusive actions against each other whereas really what it's all down to is a competition matter where they hate each other. So, you know, there's things there I think we have to be very, very careful about. Thanks.

Don Blumenthal: That brought back some memories of some antitrust cases that I worked on years ago, more vendetta than law. David, is that a new hand?

David Cake: Yes.

Don Blumenthal: Go ahead.

David Cake: Yes, no I'm just - to qualify I'm replying to Val's comment where she says - I mean, I agree that, yes, we've discussed the non response versus non - versus not working issue at length. And if everyone is on the same page with that we can - I'll quite right, we can move on.

I was just referring to Val's comment where so costs - the customer - to quote from Val, you know, the customer is also responsible for ensuring the (unintelligible) content or the cost to attempt to reach the customer via further form or mode due to repeated delivery failure should not be attributed to a requestor but to the customer.

And I was just saying, well, that line of reasoning sort of seems reasonable to some extent but only to some extent. That is if the - you know, suddenly that means they need to, you know, that the proxy privacy provider needs to, you know, do something like call or fax or something the customer to pass on - to ensure that they're contactable and that attracts a fee, well fine, but just because there has been repeated delivery failure then that should not mean all costs are moved to the customer, which was what would be the sort of straightforward reading of Val's comment. That's all.

Don Blumenthal: Okay. Before handing it over to Steve I just want to toss something out that I saw an email. We spoke about hard bounces in - we've spoken about hard bounces on calls and again in Los Angeles. And I think we may have to come back to that issue at some point. And I'm just looking at Val's comment there. And, you know, I think we will need to focus in on what a hard bounce is whether it's a repeated failure, whether it's a specific type of message or some combination of different factors.

You know, is a can't be delivered now but we'll keep trying a hard bounce? Those can go on for a long time depending on how the mail server is configured. Steve.

Steve Metalitz: Yeah, this is Steve. I'm basically agreeing with Val's comments. And, David, look at what Val has proposed. She said the provision should specify that any reasonable feel accrued by the provider as a result of having to use an alternative method to contact the customer in the event of a persistent delivery failure is to be borne by the customer. So it has to be reasonable.

It's only in this case that we're talking about a failure of electronic communication. And it's only, you know, to contact them. And as you said, it might be just a phone call.

But so I think it is already pretty limited. And if you're agreeing to the concept to a certain extent then, you know, let us know if you think that this goes beyond that extent.

As far as the hard bounce question is concerned we have discussed this at least a dozen times in this group. I don't think we need to discuss it further. It's an implementation issue. I think the formulation that's in there, that came out of the LA meeting, a certain minimum number of delivery failures within a certain specified timeframe is probably sufficient for - I would suggest it's sufficient for our purposes now.

And finally on the "must" versus "should" yeah, we're going to have to go back through this entire document and see which things we think are minimum standards. But, again, that's the goal. And so "should" is fine but "must" is something that provides a rule that people can use to figure out whether or not they're meeting the standards for accreditation. So I think we should be looking at must in the cases where we have a conclusion. Thanks.

Don Blumenthal: Thanks, Steve. You're right about hard bounces. I want to raise the issue just in terms of what terminology we're going to be focusing on. I think the persistent failure is a better - is a better concept to work with. I want to revisit it in case there's a thought that we should be going back to the old phrase.

Michele and then I'd like to see about moving on to the next topic.

Michele Neylon: Yeah, thanks Don. Michele. Just I think some of this, you know, should really be kept narrow in its remit. I mean, if you look at the error codes for SMTP, I mean, there's a bunch of them there which refer to different types of message failure. I mean, you know, that's probably what we should be looking at as a baseline as opposed to trying to reinvent the wheel.

I mean, if an email - if I try to send an email to somebody and I get 500 reply or a 550 or a 5-whatever then that's it. I mean, it's failed. I mean, sure there might be some level of extra complexity that people might want to add to it. But at the same time I think we should try and keep this as simple as possible. Thanks.

Don Blumenthal: Appreciate it. Before we move on let me just ask is that for us or is that for the implementation team? I mean, should we be looking at persistent failure and then letting the, you know, ICANN staff and whoever joins the implementation team later come up with a more specific definitions?

Okay I'm just looking at Kathy's notes here. Mary, could you bring up the next document on our hit parade here? We had talked about getting a proposal that I really appreciated Volker but - Volker and Steve working on; one submission, one edit. I thought - we thought it was worth coming back to it and having a focused consideration on the list because it - I think is a core piece for how we're going to consider some issues.

I don't want to go through this line by line. We don't have time to do that I don't think - not in 18 minutes, not and allow any discussion anyway. Was

wondering if - well not wondering, I'm going to call on Volker and Steve to at least talk about the document at a high level so that we can focus our discussion. Volker, I apologize, I mean to send you a note last night saying I was going to put you on the spot and just flat out forgot. I think Steve knew it was coming.

Okay. Been so long that we forgot what we wrote? Oh, sorry, Volker, that presents a problem.

Chris Pelling: Don, it's Chris. Volker's not dialed in.

Don Blumenthal: Yeah, no I just saw the - I just saw his post in the chat. That does create a problem. Steve, can you at least go over and maybe we'll have to revisit this when...

Steve Metalitz: Yeah, I mean, I...

((Crosstalk))

Steve Metalitz: Yeah, I briefly walked through our proposal in LA and then Volker was not there at the time but I guess it's in the transcript. But I think it would benefit from having both of us discuss this. I mean, I think, I mean, obviously Volker has made a lot of proposed changes here as shown by the amount of blue in - on my screen - type.
But I think there's a lot of common ground as well and I appreciate him giving, you know, kind of a concrete response on these. We're going through this and to see where we might be able to come out with common ground.

And I also would call people's attention to some very detailed comments that James presented in LA that are also in the transcript about this in which I think he ended up saying he thinks we're in the same postal code at least if not in exactly the same place on this so I think that was a hopeful sign as well.

I guess what I might suggest, I mean, I'd be happy to have Volker's comments and maybe, you know, we could just defer that to the beginning of the next call. But in the mean time we'll go through this and try to identify some areas of agreement or areas where we might be able to suggest another approach on this.

We - at the outset we do have a little bit of a clash of legal constructs here between the prima facie level that we suggested be the trigger for disclosure and the German legal concepts about blatantly obvious legal duty to investigate. And we're going to see if we can get some other insights on what is the distance between those.

Obviously there is some but I'm not sure that it's an unbridgeable gap. So let's - it might be useful over the next week to see if we can get a little more detail on that. And then of course I'd be glad to start next week's call with Volker's presentation on that or maybe we'll have some other, you know, middle ground let's say to suggest before then. Thanks.

Don Blumenthal: Excellent. That'd be really helpful. Yeah, sorry about the very - or possibly obtuse reference to validated postal code in the chat there. I was steeped - well, the issues of Whois verification and validation were all over the place in Boston last week.

Volker, welcome.

Volker Greimann: Hi, Don. I dialed in now. So, yeah, just listened to Steve and I also think that we're not that far apart. There is probably a bridge that can be crossed here. I just felt that by amending his original proposal I made some suggestions of - that would fit more than just the standard providers and that enabled them to have multiple routes or ways of proceeding with informing a customer.

So, for example, by removing the direct communications method in the first part, the preliminary statement then indirect communication might be sufficient as well as some privacy services do only offer that indirect means of communication.

And that's the kind of theme that all these changes that I made go under, i.e. what would be the minimum standards that would be required for certain action or a certain behavior of the privacy provider. And I obviously based them on a certain German legal tenures because that's the system that I'm most comfortable with and feel at home with.

So there might be some explanation that might be necessary and I'm of course willing to answer any questions to that. I do believe that there needs to be prima facie blatantly obvious violation of the law that the provider can see with the blink of an eye that does not require any legal investigation on behalf of the provider because anything beyond that would require such an investigation would already not fall under the liabilities that a privacy provider normally has.

Just scrolling down a bit. Been a while since I wrote this. And I didn't know I would be called to the spot. I also think that the - there should not be an automated disclosure of full - of all data that when a partial disclosure would be sufficient or another method would be sufficient in reaching the same goals.

So that was the main intent behind most of these changes. And I think, as Steve indicated in the - in LA, we're not that far apart as it seems, it's just finding the right graduation of response that is required as actual fact for accreditation and that must be fulfilled and what the leeway is that a privacy provider has in interpreting that.

Don Blumenthal: Great. Appreciate that. Phil, welcome. Phil?

Phil Corwin: Oh sorry, I thought I had turned off my mute. Can you hear me now?

Don Blumenthal: Yeah...

((Crosstalk))

Phil Corwin: Okay. Yeah, I have a concern about this draft document insofar as it refers to allegations of trademark infringement based upon the domain name. It says that on Page 1 it says, "Disclosure may not be denied based on the lack of a court order, subpoena or pending action, UDRP, URS proceeding," which would mean that the complainant would not have to file a UDRP or URS or bring a court action under a law like the anti-cyber squatting act.

And then it says that the information will be provided based on Number 3, domain name, you know, disclosure of domain name that infringes the trademark. If we're talking about a disclosure policy when a trademark owner says this Website is selling counterfeit versions of my goods or is impersonating me in regard to trademark services, that's one thing.

But I think where we have an existing ICANN-approved procedure for allegations regarding infringement caused by the domain name itself we should steer clear of that and leave this issue for the upcoming UDRP and URS review and potential reform which is going to start in spring of 2015.

This creates a situation where someone can believe, you know, allege that a domain name is infringing - is identical or confusingly similar to their trademark. In some cases that might go to UDRP or URS and be denied and yet we seem to be creating a situation here where the registrar would have to disclose information and not leave it to the registrant the decision of whether they want to participate in the UDRP or URS or have a default action.

So I think we should steer clear on that one and carve out things covered by the UDRP and URS.

Don Blumenthal: Do we expect a proxy privacy provider to know what's appropriately covered by those?

Phil Corwin: Well I think, you know, we could just - if we create a policy that carves out allegations of trademark infringement based upon the domain name itself rather than an activity at the Website I think it should be clear to the registrar or the proxy - independent proxy provider that they're not required to disclose the information.

And I'm not talking about relays. If a complainant believes that a domain name is infringing their trademark and wants to, through the provider wants to have a letter relayed - a cease and desist letter - I don't think that's a problem. It's where we might require a disclosure of things where that basically creates an alternative process separate from the UDRP and URS focused on the same type of complaint.

Don Blumenthal: Okay. Appreciate the clarification. As you might guess my question was from experience on looking at a complaint and trying to figure out exactly what it said. Darcy.

Darcy Southwell: Yeah, this is Darcy for the record. In the general policy - I really have a question because in the general policy section we talk about, you know, why disclosure may or may not be denied. And one of the reasons that we could deny as kind of edited by Volker is that it has - the complaint has to do with content yet we're talking, I mean, two of the three key issues below really talk about Website content, the copyright infringement and the trademark content as opposed to trademark and a domain name.

And I'm just - I'm just trying to understand where we're headed with this because I find it - I don't know, challenging a little bit because we seem to be talking about both issues in the same document.

Don Blumenthal: Thanks. Go to Steve.

Steve Metalitz: Yeah, this is Steve just responding to the last two comments. First on Phil's comments, we've had some discussion about this previously and the idea is that disclosure may obviate the need for a URS or UDRP which obviously saves everybody time and money and stress if the disclosure, you know, shows that it's somebody that may have some basis for using this or for some claim of rights in the trademark.

Also, I mean, it's not an alternative procedure in the sense that the remedies are quite different. Remedy here, if you want to look at it that way, is to basically find out who the registrant is and how to contact them. Obviously the remedies in URS or UDRP are much more drastic; suspension or forfeiture of the domain name. So I don't think the two are related. One is not a substitute for the other clearly.

With regard to Darcy's comment, well, you know, this change that Volker made is obviously one we very strongly object to. And I think it's actually inconsistent with what we've found out during the discussions of current practices that most of the - of the providers do not automatically rule out taking some action simply because the claim is not about the domain name itself but actually has to do with something - something having to do with the resource to which the domain name resolves.

Because by that standard you wouldn't take any action on malware, you wouldn't take any action on - which is content - you wouldn't take any action on a lot of other things. So that's not - I don't think that's a bright line rule, nor should it be so that's why we proposed disclosure may not be denied based on the fact that the complaint refers to material other than the domain name itself.

Volker's crossed out the "not" there and obviously we don't agree with that. This is not an area where we're in the same zip code, the same postal code

but that's why those sections, B and C, have to do with the counterfeiting and piracy situations. And, again, these are examples that we've provided because we know the intellectual property area but there are obviously a lot of other types of abuses that would need to be addressed by this.

And I'm hoping we could come up with similar templates for those. But if not this would at least be an example of the kind of test that we would propose. I hope that's helpful response to Darcy. Thanks.

Don Blumenthal: Okay, we've got two minutes, very quickly I think we're going to - as we go along and discuss content we may have to be careful or come up with definitions, whatever you want to say, however you want to phrase it because at least in my case well PIR would not consider malware a content issue and we can explain - you know, we let's floor that later but let's stick to this topic.

Paul.

Paul McGrady: Hi, this is Paul McGrady for the record. I just wanted to reiterate what Steve said with regard to how the UDRP and URS are not a substitute for this process that the UDRP and the URS both require certifications that the party filing with them are essentially acting in good faith.

And I think that includes, to the extent that a respondent makes it possible to know who that respondent is and whether or not they might have any rights that would make a UDRP or a URS an inappropriate thing to file against them whether or not they hide entirely is up to them sometimes. But simply filing one of these blind as a method to obtain the disclosure I don't think would be looked upon very favorably by either the UDRP panelists or frankly the providers that are involved in that.

So if we - we actually discussed this topic at some length in Los Angeles. I'm hoping that we can, as a group, decide to put the topic to rest since I don't

think that anybody who files UDRPs and URSs would view these two things as equivalents. Thank you.

Don Blumenthal: Great. Thanks, Paul, for - and we'll give Volker the final word.

Volker Greimann: Thanks, Don. Just two questions for Don and you may want to answer off list if at all. The first one is the thing that Paul just mentioned with the UDRP where you find out after the complaint that, oops, the complainant - the respondent actually had a right in this domain name. Well, that's what we call an invalid complaint and that should not lead to any disclosures on the matter of principle.

If you are kind of fishing for the respondent and to find out if a UDRP is warranted or not then you're abusing the system right there. So I object to this interpretation and this use of the reveal provisions.

The second part is I have a very strong opinion and from what I hear from Don, PIR handles it similarly, is that content is not a matter of domain registration question. Content issues should be handled with content hosting providers and the domain name or registrant as the owner of the domain name, not with privacy proxy services or registrars.

The privacy - the proxy registration is just about the registration of a domain name. They have nothing to do with the hosted content; content is not part of the scope of this. And that's my final word.

Don Blumenthal: Okay. And that's, except for what I'm saying here, the final word for the call. Too bad because the chat is coming up with some excellent points. If chat dies before you finish please continue in email. Thanks and we will gather again next week. Same time, same place.

Mary Wong: Thank you, Don. Thank you, everybody.

Man: Thanks very much. Have a nice weekend.

Graeme Bunton: Thanks, everyone.

END