

**ICANN Transcription  
Privacy and Proxy Services Accreditation Issues PDP WG  
Tuesday 19 August 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 19 August 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-20140819-en.mp3>

On page:

<http://gnso.icann.org/calendar/#july>

Attendees:

Steve Metalitz - IPC

Graeme Bunton – RrSG

Val Sherman – IPC

Griffin Barnett – IPC

Tatiana Khramtsova – RrSG

Frank Michlick – Individual

Volker Greimann-RrSG

Don Blumenthal – RySG

Holly Raiche – ALAC

David Heasley-IPC

Jim Bikoff-IPC

Carlton Samuels – ALAC

Keith Kupferschmid- IPC

James Bladel - RrSG

Michele Neylon – RrSG

Alex Deacon – IPC

Chris Pelling – RrSG

Luc Seufer- RrSG

Stephanie Perrin – NCSG

Daniel Burke – Individual

Tobias Sattler – RrSG

Roy Balleste – NCUC

Todd Williams – IPC

Kathy Kleiman – NCSG

Phil Corwin – BC

Justin Macy - BC  
Phil Marano - IPC

Apologies:

Lindsay Hamilton-Reid – RrSG  
Susan Prosser - RrSG  
Christian Dawson-ISPCP  
Sarah Wyld - RrSG  
Susan Kawaguchi – BC  
Kristina Rosette – IPC  
Darcy Southwell – RrSG  
John Horton – BC  
Osvaldo Novoa - ISPCP

ICANN staff:

Mary Wong  
Marika Konings  
Amy Bivins  
Danielle Andela  
Nathalie Peregrine

Nathalie Peregrine: Thank you ever so much Andrei. Good morning, good afternoon, good evening everybody and welcome to the PPSAI Call on the 19th of August 2014. On the call today we have Tobias Sattler, Tatiana Khramtsova, Steve Metalitz, Val Sherman, Holly Raiche, Dan Burke, Graham Bunton, Volker Greimann, Griffin Barnett, Don Blumenthal, David Heasley, Roy Balleste, Kathy Kleinman, Todd Williams, Michele Neylon, Keith Kupferschmid, (Alex Deacon, Phil Corwin, Frank Michlick and Justin Macy.

We have apologies from Darcy Southwell ,Lindsay Hamilton-Reid, Susan Prosser, Christian Dawson, Sarah Wyld and Susan Kawaguchi. From staff we have Marika Konings, Mary Wong, Amy Bivens, Daniella Andela and myself, Nathalie Peregrine.

I would like to remind you all to please state your names before speaking for transcription purposes. Thank you every so much and over to you Don

Don Blumenthal: I appreciate it Nathalie. I will add one reminder to the saying your name. Please make sure you are on mute if you are not speaking. Well first the general semi-regular reminder to please post any updates to your statements of interest. People do check those every once in a while.

And a couple of - just one thing in between kind of Item 1A. I just want to make sure that everybody's constituencies, stakeholder group, whichever has turned in your list of lodging requests for the face-to-face meeting in Los Angeles. It's only 10 o'clock. We are going to go over those and then try to figure a way to reallocate unused nights for groups that may need more or maybe even some individuals who aren't covered by one of the stakeholder groups or constituency or whatever. You know as an example, the registry groups will be using three of our six and we would like to put those resources to good use if we can.

Onto today's discussion. We've been asking people to be more involved in between phone calls and I think we may have run into be careful what you ask for. The conversations that Volker kicked off is just outstanding and unfortunately in some ways, it makes it hard to know where to begin. And once we have begun, where to go, so let me just tee things up with two - with one comment.

Keep in mind that what we are looking at here according to the GNSO charter questions is a baseline set of requirements. I mean there is nothing that says that service providers can't go beyond what we suggest. And I've seen a lot of discussions that haven't taken that into account and we need to provide a foundation. And I also want to reiterate something I said in an email during the week. That we are here to set the policies and certainly looking at implementation questions helps us decide on appropriate policies. We need to be careful to draw a line between what we intend to write up and what is more appropriately going to be on the implementation side.

With that out of the way, I think we are still looking at a threshold question here. You know which basically is going back to the fundamental question of what - where do we draw the line between a provider having full discretion to forward or the ability to limit what is passed along. And we have gone all the way from something as -- this may not be a good term -- restrictive in terms of what James suggested in terms of (unintelligible) to just everything goes through or everything goes through subject to some kind of spam filter.

Volker.

Volker Greimann: Yes thanks Don, Volker speaking. I would just like to say my proposal was not meant as a proposal for actual policy. It was more of a statement of position. What I think is indeed - what I think in detail a solution could look like in the end, because the last week we've been discussing back and forth about what the position is and so I went ahead and just wrote something up, which I thought could encapsulate what I think about this issue.

My basic terms which I tried to express in the proposed language in the discussion base if you will was mainly if it serves the purpose of having a contact address, anything should be possible. As in if I only allow mail, then so be it if that fulfills the possible objective of having the registrant contactable.

I am sure there are a lot of improvement and I think the discussions that we have been having following this proposal have been very fruitful because it has brought some very interesting arguments and made me think once or twice as well about what we have been discussing here. And I think with this as a basis, just to have an example policy out or an example wording out helped us focus a bit on what the basis of what (really should be).

I think we had a good discussion with Susan who has expressed some concern and I think made some good points and I think we have a good basis now to start from.

Don Blumenthal: Yeah, I absolutely agree. I really appreciate the effort you put in to toss it out. No, I can't speak for anybody else, but I never assumed that that was a proposal to be put in one of the templates. I always looked at it as a strong man type proposal to generate discussion, so you are off the hook there.

Steve.

Steve Metalitz: Yes, thank you, this is Steve. I just want to second what you said and to thank Volker for putting out this text because I really do think it has helped to focus a lot of our discussion.

I also want to just referencing back to the text that is on the screen now which the staff had generated a week or two ago. I thought it was interesting that one thread that we've had here kind of points in the direction of - you have down there about Option 1 and Option 2 for the minimum standard for relaying email. I think one thread here, which Volker contributed to might look toward making those two options two possible choices. In other words, you could - a provider could choose to automate this process and relay all of the requests received subject to (captia) and so forth or it could choose to have a more manual process as James called for two weeks ago and so forth.

But there are some things that would have to be sent forward and we've used the term - in the thread we've used the term legal claims for what is - we have down there as third party requests containing allegations of abuse or at least one example of that. So in a way, perhaps we could look at an either/or approach and also I just want to second one thing Don said which is that you know again we are trying to recommend policy here. There is certainly going to be implementation issues with anything that recommend, but we need to keep our focus at the policy level.

So I would just like to again thank Volker and also encourage people to look at the possibility of Option 1 or Option 2 and then - so that the service

provider could choose between one of those options in how it wished - the service which to offer. Or I think as Volker pointed out, it could offer both. It could offer Option 1 and then Option 2 as a value added service; so again, I want to thank him for putting those ideas on the table. Thanks.

Don Blumenthal: And back to Volker.

Volker Greimann: Yes, thanks Don and Steve thank you. I think that is right on the money. These are options as long as a certain form of contact ability is provided. That should fulfill whatever we are recommending in the end, because the purpose of having such contact ability is maintained. In fact, that's the way that we set up our system. We have the automated email that everybody can use and send directly to the registrant and we have the abuse contact, which is a manual - of which every communication is subject to manual review and deletion if it doesn't fulfill our requirements or forwarding if it does. So we have both kinds.

Don Blumenthal: Michele.

Michele Neylon: Thanks Don, Michele for the record. Sorry, I wasn't on the call last week since I was officially on holiday. Just in relation to options and various things, the idea of a service provider manually reviewing emails scares the hell out of me. I would be very, very opposed to that for the simple reason - I mean I'm not a lawyer, but from my understanding, if I am aware of something no matter what it is, then I lose any kind of mere conduit status that I might have in other circumstances.

So from my perspective, if as a provider I wish to offer a particular route for particular types of communication so that - I mean this has nothing to do with whether a contact that is provided in Whois or elsewhere is reachable or not, but the key thing being that I might provide you with a particular method for contacting us or our clients in particular types of abuse. But I would not want

the service provider to be stuck with reviewing anything manually. I just see that as being a massive legal can of worms. Thanks.

Don Blumenthal: Let me just follow up though. What about an option that - I am reading between the lines on these options. The ability to review if you want but not have (unintelligible) require it.

Michele Neylon: Was that addressed to me Don.

Don Blumenthal: Yes.

Michele Neylon: I don't want to review anything.

Don Blumenthal: Okay but are you all right with the policy standards coming up saying we may but not require you to.

Michele Neylon: I may drink 20 cups of coffee per day. I am under no obligation to do so. If I drink 20 cups of coffee today and I don't die as a result, that's fine. May means it is not a binding obligation on me, so you can put in all sorts of may's and might's and things like that in there. It is when it becomes an obligation that it is a problem.

Don Blumenthal: Okay, just making sure. Continuing the registrar corner, James.

James Bladel: Hi Don thanks. James speaking for the transcript and just a couple of comments or points. The proposal that I made on the list was probably more operational or implementation based than policy based, so I don't necessarily believe that it must be a manual process or an automated process. I believe you know that it can be - an innovative provider might find a way to automate the system that I was proposing.

And I also just want to point out that it is I believe compatible with Option 1, which is a commercially reasonable safeguard against abuse of

communication, so I am fine with that there and I am fine with the idea of having an either/or choice to establish a minimum set of practices with the allowance that service providers may build additional value added product on top of those. So just wanted to get those out there and thanks for listening.

Don Blumenthal: I appreciate it. Just to clarify the proposal you made, are you referring to the concept based on the RGS or...?

James Bladel: Yes the idea that the service providers would monitor the use of the relay reporting system as it - you know it could be restricted for those that were determined to be abusing that channel. That may not necessarily be a manual process.

Don Blumenthal: All right, I appreciate the clarification. A lot of things get put on the list in your proposals and sometimes it is hard to remember which is what. Finally, another corner hear from. Kathy.

Kathy Kleinman: Hi all. I missed the meeting last week. I think Option 1 and Option 2 makes sense. I particularly like Option 2 because it is narrower. It is much more towards the minimum standard. We are not relaying - we are not asking the proxy privacy provider to relay everything, but certain types of notices, and I know it doesn't have to mean - I don't think it has to mean that the proxy privacy provider reviews everything, because I agree with Michele. That's dangerous and I know we've talked over time about time consuming.

But if there were menus or pull downs, what type of you know email is this, it creates asking, - you know if someone is going through a Web site, asking them maybe not for full identification because I have some concerns with the EWG and the RGS overlay that I saw on the list. But just asking them what type of email this is, what type of - you know is it a law enforcement issue. What type of abuse, is there an allegation of abuse, and that could be kind of a pull down and that could also be used for auditing and checking for abuse,

which I am glad James is looking for and others are looking for, so I like Option 1 or 2. Thanks and good to be back, but it was fun to be gone.

Don Blumenthal: I agree although you lost me with the reference to (unintelligible).

Kathy Kleinman: (Unintelligible).

Don Blumenthal: Pardon.

Kathy Kleinman: Which reference (unintelligible).

Don Blumenthal: Yeah you lost me with the - and I agree that it is nice to be off, but you lost me with the reference to camping. Any other thoughts. Okay, let me - the other subject that got a lot of - took a lot of bandwidth was just the issue of legal communications, and so I wanted to circle back to that. Starting off with to what extent does where we seem to be going on this call resolve whether we need to address those issues at all. I've got some folks on the call who posted about the subject. Okay, I think we will take it under advisement as is we write up how the different threads fit together.

(Graham Bunton): Sorry Don, this is (Graham). I think a number of people missed that particular question. Could you repeat it? Thank you.

Don Blumenthal: Sorry about that. The other topic that got a lot of discussion on the mailing list was the question on legal communications under the heading of what must be forwarded as opposed to whether there might be some leeway. I guess my question and hoping to get some contributions from people who posted on the subject is have we resolved the issue of (leaving the forward) or requirements to forward by what we just talked about? Do we need to discuss the issue of legal communications and what (unintelligible)? All I can see S-T-E-P-H-A. Is that Stephane? Hello.

(Stephanie): It's (Stephanie).

Don Blumenthal: Hello Stephane, yes.

(Stephanie): Can you hear me?

Don Blumenthal: Yes.

(Stephanie): I'm having audio trouble.

Don Blumenthal: We can...

Man: We can all hear you (Stephanie).

Don Blumenthal: But she can't hear us. Let's move on to James and come back.

James Bladel: All right thanks and James speaking and we will see if we can get (Stephanie) back on the line. So I didn't participate in this discussion on the list. I think that you know if we start to coalesce behind the idea of the two options that were laid out earlier, then the idea of discriminating on the different types of you know legal communications, et cetera, we can probably roll up under one or both of those options. I think we may have covered that. I just want to weight in that you know legal communications to me is overly broad threats of lawsuits by you know non-legal individuals could essentially be considered a legal communication.

So I think it would be very difficult operationally to figure out what is and what is not a legal communication. But the good news is that I think if we start to take a closer look at these two options that we could probably just roll those up for all types of third party reports. Thanks.

Don Blumenthal: Excellent. Thanks. Kathy.

Kathy Kleinman: Is (Stephanie) back on?

Don Blumenthal: That's why I was hesitating because I don't see a sign she is.

(Stephanie): I think if you can hear me I'm back on.

Don Blumenthal: We can hear you way too well.

(Stephanie): Sorry, I cranked up the volume. Maybe I should crank it down again. But I think I was going to echo what James just said. It strikes me that a legal communication is extremely difficult to define and you - any way you turn it is going to be unfair to somebody, so my comment would be that I think that this group should not be in the business of constraining the services that are offered by privacy proxy services. If I choose to anoint my privacy proxy service provider as my legal filter, then they should be under no obligation to send on to me things that they can (routinely) turn away.

I would think that the one clear thing might be a subpoena or a warrant but that of course is also dependent on jurisdiction and (unintelligible) and all of those things. So I am not sure - I am not sure what the (regnant) of this group is with regard to making these determinations, but I just want to cast my vote in favor of leaving it to the service provider.

Don Blumenthal: Okay Kathy.

Kathy Kleinman: Sure. Can you hear me Don?

Don Blumenthal: Yes.

Kathy Kleinman: Great. I just wanted to note that whatever we do with legal communications here under relay may be different than what we want to do under reveal. I can see a broader definition for relay and a narrower definition for reveal, and so I just wanted to create that as kind of an asterisk in that we not automatically carry over whatever definition or lack of definition we create here to reveal because this is - because legal communication, jurisdiction, a lot of things

that we've decided not to look at here in relay I think will become very important in reveal. So just that note. Thanks.

Don Blumenthal: Okay, I appreciate that. Any other thoughts on the legal? Okay, let me put Volker on the spot and I warned you I might do this. Wait a minute, you did send back a chat message. It doesn't say no, so (unintelligible). Let me ask you because you know your proposal or your straw man better than any of us. Do you see anything critical in it that we should be addressing (unintelligible) before we (unintelligible).

Volker Greimann: Could you rephrase that? I don't think I got the question.

Don Blumenthal: You know your straw man better than we do and what you intended to generate discussion on. Are there issues in it that you think haven't been addressed to (unintelligible).

Volker Greimann: Probably.

Don Blumenthal: (Unintelligible).

Volker Greimann: Yes, Volker speaking not just for the record but for on general principle. I think there is a lot of holes in that straw man because it doesn't take care of everything. I looked at how our services provider and what were the considerations behind when we designed how to operate and what communications to take, how to forward those, and so on and so on. And building on that, I tried to put those into the straw man in a way that it also explains part of the thinking.

What I think is that we would have to look at different ways that these services are provided. If these suggestions meet those ways, but first and foremost should be that based on the discussion that we are now having, we should kind of try to distill the basic principles such as there must be some way of coming forward in communications, but how to enable that is up to the

provider within reasonable measures. So he may not for example require us sending (unintelligible) bills for forwarding, that would be unreasonable, but you know what I mean.

So basically, there has to be sort of a forwarding mechanism but it can be limited to certain communications. Certain communications may be filtered out and I think that's the gist of it, and if the basic principles work for all privacy service providers, then we can start elaborating on that again and building the policy out of that.

But first, I think we are having this discussion now and that's good to see where the holes are and everybody is invited to poke as many as they can, and then we should try to get a basic set of rules that work for everyone and also work for those parties that want to have communication sent to the registrant or at least are not onerous upon them.

Don Blumenthal: Yeah okay, thanks. I will ignore the fact that the thousand-dollar bill (unintelligible) forwarding but we should require forwarding paper. Todd.

Todd Williams: Thanks Todd Williams for the record. I am a little bit confused about the discussion on the definition of legal communications. My understanding was that what we were - it seemed like coalescing around was some sort of combination of Options 1 and 2. Option 2 as it is currently drafted says a provider must relay all email Web form notices, et cetera, and then the last clause is an third party requests containing allegations of abuse per in i.e. illegal activity. And then there is a footnote that goes into that in a little more detail.

And I guess my question is is everybody comfortable with that definition. Is the discussion that we were having about the definition of a legal communication distinct or different from that definition or are some of the points the same?

I guess my question is I'm not sure how closely connected the discussion we were having on legal communication is to the standard that it seemed that we were agreeing on. Thanks.

Don Blumenthal: Well I guess that was part of my question. Does the wording in there - do you - would you think that the wording in there and others of the discussion that happened in email?

Michele Neylon: Don, this is Michele.

Don Blumenthal: Let me give Todd a second to answer.

Todd Williams: Oh, I'm sorry. I mean my thought was this is a different standard and therefore the discussion we were having on legal communication might be as I think Kathy pointed out relevant when we get to Reveal that at least as it is right now, I think we can agree on a standard without having to answer that question but I'm not sure that everybody else agrees with that.

Don Blumenthal: Okay. Well, you're the one - you're the one who stepped up to the mic so we'll at least start - go with that to begin with. Michele.

Michele Neylon: Just actually speaking - the reason I raised my hand was to kind of speak to this entire point. What several of the registrars and others were talking about is that you get - we get sent -- how could I call them -- quasi legal notices from random third parties who don't identify themselves properly far too often.

Now it isn't an issue with normal proper lawyers who understand concepts such as headed paper, telephone numbers and other kind of contact details that could actually legitimize a request.

Unfortunately, you know, 90% of the stuff that we get sent doesn't contain any of that. I mean we get stuff saying, you know, Web Site X is offensive or

Web Site Y has, I don't know, some other random issue or is apparently breaking some law somewhere.

And the thing comes in and it's a quasi legal threat threatening to either sue us, sue our client, sue our client's client or sue the world but it's not coming through from a proper contact. It's not coming through on proper headed paper or if it's coming electronically you don't have proper contact details.

But I do have the rather amusing situation where somebody did provide proper contact details and reported the response we sent them to our own abuse desk. But that was a bit extreme.

Don Blumenthal: All right. (I knew that). (Stephanie).

(Stephanie): Hi. Can you hear me?

Woman: Yes.

(Stephanie): It's (Stephanie) for the record. Forgive me; I often get a sense of deja vu on this particular working group. I'm sure we must have dealt with this a while ago.

Back to the concept of having a standard form, couldn't we as a working group come up with a standard form and the persons who wish their communications to be forwarded could fill in the form at least for this particular area.

And then clearly if they're not going to identify who they are, if they're not going to identify the particulars of the case and cite, you know, enough evidence that you could act on it, then it goes in the sand bucket.

Or we can, as Steve just said in the chat, we could make this a recommendation. I think we need to make it pretty clear that we're going to

trash garbage such as Michele has been describing both on the line and on the chat. Thanks.

Don Blumenthal: Okay. I'll just point out this might be closer to mark to do something by the form of the second. I don't think we are receiving any (business) of that. I think designing anything it's going to be up to (unintelligible). James.

James Bladel: Hi. Thanks. So it probably won't be as eloquent or humorous as my Irish colleague there but just want to reiterate that, you know, in ICANN circles I think we're very familiar with the concept of service providers being tarred with the brush of the bad actors in their space. And we see this with registrars and privacy providers sort of being held to account for the lowest common denominator in their industry.

And I think that perhaps this is the first time that we have introduced the concept that this goes for reporters, legal, law enforcement or otherwise as well. But there are not always good actors in those areas as well who are participating in good faith. And that the signal (called) noise ratio for some of these reporting channels particularly like those that were established as a result of the 2013 RAA just as an example; not as an analog.

But immediately became overwhelmed with the garbage that flooded into those systems that drown out the legitimate and I would say urgent and time sensitive reports of actual harm. They were lost in a sea of junk.

And so I think that whatever we land on here is essential to ensure the effectiveness of these relay mechanisms that the service providers have the ability to put some basic and meaningful filters in place to discriminate between the folks who are operating legitimately, you know, in the interest of protecting their property versus those who are just harassing and making threats because the latter will outnumber the former, you know, by a factor of a couple of orders of magnitude.

I think that that's something that just has to be seen firsthand to really be appreciated. So thank you.

Don Blumenthal: Okay. Thanks. Anybody else want to jump in here before we move on to Reveal? There are some issues that we have not covered (unintelligible) we'll have time to come back to them whether it's just face-to-face meetings in - yes, in Los Angeles -- I've got a mental block there -- during our writing.

I do want to point out though that we discussed in the past the whole issue of forwarding paper. And (that might be something we're driving toward) a consensus - something else comes up. So I do want to suggest that the discussions here, you know, of legal, however you want to (apply) that in a sense (unintelligible) and the - I guess if there has to be some mechanism for either forwarding paper or scanning it, using email or something.

Again, I think that's something we can then turn to but I think I'm just hearing in a more focused way the concept of this really is an issue that we'll have to come to consensus on.

At this point I'm starting to think the consensus or I shouldn't put it that way. I'm starting to think that the people are demonstrating a need for some mechanism. Steve.

Steve Metalitz: Yes. This is Steve. And just I think is - thank you for the segue to this issue. As we've been looking at this document with Option 1 and 2, these are about relay via email and Web forms. And I think that's appropriate.

The one concern I have about Volker's straw man is the idea that a provider could say well the only type of communication we'll forward is hard copy or the only type of - in theory the only type of communication we'll forward is a fax.

I think, you know, the reality is we all know this email is how the providers are communicating with their customers. It's how people are used to sending notices of legal claims without getting into the definition of that. This is a - email is going to be the standard method.

So I don't think we can - we should be accepting that a service provider could say we won't forward any emails. We will only forward hard copy. I think the hard copy issue is a very small issue that we ultimately do need to resolve but not at the expense of getting the right standard in place on emails and Web forms.

So I would just emphasize that as we've been talking about Option 1 and 2 as a jumping off point and putting them together, we're talking about email/Web form, electronic communication and not about hard copy. Thanks.

Don Blumenthal: Thanks Steve. I agree. I was kind of - that's one of the reasons I kind of tossed it in as part of my mention and we'll be circling back to (this later). Just was suggesting that that's one I'm (guessing) we'll have to take up again. Volker.

Volker Greimann: Thanks Don. Volker speaking. I find myself agreeing with Steve at least on principle for what we've chosen for our service in fact. We only accept email. And people phoning to our telephone line are redirected to a message that says please send an email and we provide information in our - our Web site and our - and in the Whois as well that we will not forward any written communications or hard copy.

People are informed that hard copy is not accepted. So personally I'm seeing myself leaning very, very far towards email. I just can't imagine that there's other services that are set up in a different way. Maybe law firms that are providing some form of privacy service for certain customers that would require hard copy for good reasons that are different for - to the reason for me accepting email.

Email is easier to handle. I would love - I would love to have everything in email personally.

Don Blumenthal: Thanks. Well not seeing any other hands up, if I could ask everybody - everybody's in chat. You've got to follow your screen. Scroll down to Charter Question E2. Let's move into Relay. Excuse me.

(Mary): Don, this is (Mary). Did you mean...

Don Blumenthal: Yes.

(Mary): ...E2 for Relay or did you want to go to F1 for Reveal?

Don Blumenthal: I'm sorry. F1, which is not on there. And I don't know if this is going to be more or less interesting than the discussion of Relay. I certainly - well I'm not going to make values.

We had sent around the F1 template last week. I think we need to just address some - confusing word threshold. I (apologize). To begin with just explore how much how the standards will be different as a couple of people suggested.

Reveal by Relay is going to be somewhat more - the standards will be higher. I think -- one person's opinion -- I think by definition because Relay just passes information along. Reveal by definition kind of removes the purpose that privacy and proxy registrations exist. I was going to say a little bit more but I'm happy to let James jump in.

James Bladel: Hi Don. Just quickly. When we were talking about Reveal, I think at one point we were discussing two flavors or variations of Reveal. One is Reveal to an individual or a party or an organization is requesting. And then another one is,

you know, revealing in Whois in the public database for the whole world to see.

And I don't know if we're continuing to make those distinctions or if we've just lumped them under one heading and we're calling it Reveal.

Man: Hello.

Woman: Don, are you there? Don.

Don Blumenthal: Yes. (Hiding). (Looking). To me I think those two are variations on a theme. The way I was planning to address them was coming up with some core concepts and then seeing how they apply to the (two different) scenarios, you know, and base certain - if it's a law enforcement request, it may not be an issue. It may just be Reveal to the requester, not actually put in the database. But that's an extreme - that's an extreme example.

Again, my thought was variations on a theme and parse from that as we go forward. But I'm open to thoughts that there's a better way to do it. Steve.

Steve Metalitz: Yes. This is Steve. First I just want to say I agree with your approach Don. Let's talk about the standards and then see if they need to be varied for Reveal and published or what - we should have a standard terminology for that second option. But let's see if we can come to agreement on the standards.

Second, I would agree with you that standard has to be higher. Basically our approach and it's in the IPC provisional recommendations that you have on the screen there.

Relay we see as a process that could be pretty much totally automated. It wouldn't have to be but it could be. Whereas I think it's more - going to be a lot more difficult if not impossible to totally automate the Reveal process.

And so we've put forward our suggestions here about what the standard ought to be that would trigger Reveal again from the standpoint of intellectual property owners.

Second, that there should be some time standards as well for revealing. And then our - what our proposal is that the general rule although there would be some exceptions would be that before a reveal occurs the provider should give notice to the customer and give the customer some opportunity to object.

So that's - I think those are certainly differences from what we think is the appropriate model for Relay. So I mean, you know, we've put forward our suggestions and I would certainly encourage others to put forward their ideas of how a Reveal system ought to work.

But we certainly recognize that this is - again because the consequences are a lot more. You know, the consequences of a relay are to my mind extremely minimal from the standpoint of the customer. The consequences of a reveal obviously are more significant. Thank you.

Don Blumenthal: Appreciate it. Volker.

Volker Greimann: Yes. I just wanted to echo something the (gents) were saying and maybe make a suggestion to that. I think we're - when we're talking about a reveal, we mean two different things. And while they may be summarized on the term reveal, it may be helpful to differentiate them at least for the purpose of the discussion.

One would be the full reveal that is removal of the Whois privacy information from the Whois and replacement by the privacy information of the - the information of the original registrant. And the other one would be - I would term it disclosure, which is revealing the information just to the complainant for whatever reason.

Both would be I think acceptable forms of reveal. The question is if one should be mandated over the other and if two different recommendations are required for those or if they can be summarized.

Don Blumenthal: Thanks. Yes. We had discussed in the past and I think we need to (unintelligible). And I think I know we used the distinction of revealing (unintelligible). But you're right. This would be kind of mentioned and the step is to figure out how we treat them differently in our report and also how we treat them - how we discuss them - get to that point. How we shape the discussion as we talk about reveal/disclose to see what (unintelligible). (Stephanie).

(Stephanie): I just wanted to remind everybody that at least in my mind the issue of how data protection law applies to the Whois has not been resolved. And therefore the distinction between disclosure and revealing to the entire universe on Whois is a very important one.

Disclosing to the party that is asking about something is really only - it's fairly simple. It's permissible disclosure upon presentation of positioned evidence, which is where the form would be useful from a data protection law standpoint.

Dumping the identity of the customer out there on the Whois is an entirely other matter and has to be looked at very carefully. Thanks.

Don Blumenthal: Let me just interject with this before I get to Kathy. I think we got - one question is coming from the standpoint of an attorney who has done a lot of privacy work. I'd love to get into all of those issues (because it is close to me). Whether it's appropriate for us her or there - when we get to that point. It's just going to be this is what we recommend subject to, you know, data protection laws.

And I (don't want to discuss) laws because trying to identify any specific one that's going to cover the universe is going to be very difficult as more and more countries come up with data protection frameworks around the world.  
Kathy.

Kathy Kleinman: Good point. Actually could you skip to James? I have - I'm having a problem in the background. No. I (trusted) it. Can you hear me Don?

Don Blumenthal: I can tell something's going on here. Oh yes. Go ahead. It's gone.

Kathy Kleinman: Okay. Not surprisingly I got in line to say something similar to (Stephanie). First, whatever our terminology is and it's funny that my - the way I think of the terminology is of course to the opposite of what Volker was saying.

I think of reveal as revealing to the requester whatever information we decide. And we may decide on tiers of information that there may be times that we disclose all the information. There may be times you disclose some of the information. There may be some discretion there.

But revealing - whatever our definitions are, we just have to make them consistent so we all know. So for me revealing is disclosing information to the requested. Publication is putting it in the Whois.

And like (Stephanie), see I find both of them concerning because the human rights issues if you reveal to one party, that could be death or imprisonment and I've worked in situations like that for whoever gets that information. But certainly if you publish to the world you're really creating a problem for the customer.

So I would recommend we deal with them in two categories and that we start with the Reveal. We start with disclosure of the information to the requestor and then go on to publication as a different category. And we deal with them separately.

And I think someone threw out there and I'd like to keep it in the discussion, what type of response does the customer get? Is there an opportunity for the customer to respond as well? And I think that's an issue we have to look at in both categories. So thank you.

Don Blumenthal: Yes. I appreciate it Kathy. James.

James Bladel: Hi. Thanks. James speaking for the transcript. I think this is a good topic that we're on and I'm glad that we're spending some time on the terminology as well.

I think that just, you know, I posted something in the chat and I see I got a positive response from Steve was well. So I just wanted to reiterate it here on the call that whatever we build here in terms of reveal or publish or disclose functions, you know, we are building them as the obligations of the service provider in response to a request to do so by a third party law enforcement, whatever.

But I want to be sure that anything that we build in there like notification requirements to the underlying customer or timeframes, et cetera, are not applicable to the service provider's ability to deliver the service under the terms of their product such that someone is abusing the service or doesn't pay or otherwise violates the agreement that they have with their service provider.

The service provider is not constrained on their ability to terminate that service and they don't have sort of squatter's rights on their network that someone is hiding behind ICANN policy to prevent this or (unintelligible) for shutting them off.

So I just wanted to get that on the record that whatever we're building here is the service provider's obligations to the broader community and not

necessarily elemental component of its own delivery of the service to its customers. Thank you.

Don Blumenthal: Interesting concepts. (Turn to it). Okay. We still got a few minutes left. We - let me return to it now. Could you expand on the - James just (fixed in) a little bit on this concept of have the response (delivered) to the broader community and to the customer/clients might play out here (Jim).

James Bladel: Sure Don. And just briefly that if for example if we built in a requirement here that upon receipt of a court order or a warrant that a service provider will reveal, you know, a customer name to, you know, to that provider but will also notify the customer five days in advance before doing so.

Let's say hypothetically that some kind of rule or requirement came out like that. That wouldn't necessarily apply to the situation or scenario where someone had violated the terms of service and are being kicked out of the service that they don't also have the same notification and time constraints, you know, incumbent on the service provider in that scenario.

That what we're talking about here is limited just to responsiveness of the service to outside requests and not how they kind of keep their own house in order.

Don Blumenthal: Okay. Now I got it. Yes.

((Crosstalk))

James Bladel: If it's, you know, if it's irrelevant or whatever, it's really more of just a cautionary statement that we don't want to build in - we don't want to handcuff these folks in dealing with their own customers.

Don Blumenthal: Yes. I know it's irrelevant. But I think it's an issue that we'll have to keep in mind as we look at the more formalized reveal issues, which we don't step into the wrong territory. Volker, I saw your hand up briefly.

Volker Greimann: Yes. Volker speaking. Just wanted to add to James' comment but he summarized it pretty well. I just would like to say yes, there should be a right to be informed before and have a - the ability to counter but not if this reveal or disclosure would be based on a violation by the customer himself for abusing the service or using the service in a way that contradicts the terms of service.

In that case I would very strongly advise against having any form or recourse prior to the reveal.

Don Blumenthal: Okay. Thanks. And we - the clock on my computer that ended - well, we stop talking right at 11 o'clock. I like time limits. I appreciate everybody's involvement today. I think this is one of the best discussions we've had. Thanks again to Volker for providing the platform for getting into it. And I think we've jumped in - we've identified a lot of really critical process issues already for Reveal. So let's move on to continue with that next week.

I apologize for that E2 versus F. We've got two documents on the screen, which I think is over time becoming more and more of a mistake. Hey we'll all talk next week. So long.

Man: Have a good day.

Man: Thanks.

Man: Thanks.

Woman: Thank you Don. Thank you everyone.

Woman: Thank you very much (Andre). You may now stop the recording. Have a good day.

END