ICANN Transcription

Privacy and Proxy Services Accreditation Issues PDP WG

Tuesday 22 July 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 22 July 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-20140722-en.mp3

Attendees:
Steve Metalitz - IPC
Justin Macy – BC
Sarah Wyld - RrSG
Chris Pelling – RrSG
Darcy Southwell - RrSG
Graeme Bunton – RrSG
Val Sherman – IPC
Griffin Barnett – IPC
Susan Kawaguchi – BC
Kathy Kleiman – NCUC
Stephanie Perrin – NCSG
David Heasley – IPC
Alex Deacon - IPC
Jim Bikoff – IPC
Kristina Rosette – IPC
Paul McGrady – IPC
Carlton Samuels – ALAC
Todd Williams – IPC
Tim Ruiz - RrSG
Michele Neylon – RrSG
Tatiana Khramtsova – RrSG
Roy Balleste – NCUC
Frank Michlick – Individual
Phil Marano-IPC
Luc Seufer- RrSG
Volker Greimann-RrSG
Maria Farrell-NCUC
Tobias Sattler-RrSG
Sean McInerney - SOI

Apologies:
Holly Raiche – ALAC
Don Blumenthal – RySG
James Bladel – RrSG
Osvaldo Novoa – ISPCP
Christian Dawson – ISPCP

Don Moody - IPC

ICANN staff:
Marika Konings
Mary Wong
Terri Agnew

Terri Agnew: Good morning, good afternoon and good evening. This is the PPSAI working group call on the 22nd of July, 2014.

On the call today we have Val Sherman, Tatiana Khramtsova, Graeme Bunton, Carlton Samuels, Steve Metalitz Chris Pelling, Sarah Wyld, Roy Balleste, Frank Michlick, Paul McGrady, Justin Macy, Darcy Southwell, Phil Marano, Susan Kawaguchi, Todd Williams, Tim Ruiz, Griffin Barnett and Alex Deacon. We have apologies from James Bladel, Osvaldo Novoa, Christian Dawson, Holly Raiche, Don Moody and Don Blumenthal.

From staff we have Mary Wong, Marika Konings and myself, Terri Agnew. And just joining us right now is Kathy Kleinman.

I would also like to remind all participants to please state your name before speaking for transcription purposes. Thank you very much and back over to you, Graeme.

Graeme Bunton: Thank you kindly. So before we get going a usual bit of business. Does anyone have any updates to their SOI? Anybody? Nope.

Okay. Moving on, any issues with today's agenda which is, as I see it, going to be continuing our discussions on E1 and possibly getting to E2 if we have the time? Nope?

Looking good. So let's maybe do a little brief summary.

So we're still on Category E, Question 1 which is what, if any, are the baseline minimum standardized relay processes that should be adopted.

We've had a bit of discussion on the list about this this week which has been excellent. Thank you, everybody, for participating.

The way I see it we're going to do a little bit of intro here, talk about the minimum. And I think we might have some input there from Kathy and Steve.

Hopefully a little bit later we're going to get to what happens if there's a failure in the relay communications. That was discussed by I think it was Alex and James on the list.

And then maybe we'll get to hard copy that was raised by David too. So we've got some sort of meaty topics ahead of us.

So Steve was suggesting on the list that we -- and I want to make sure everybody's comfortable with this -- that we - the option to relay nothing is off the table, that there, you know, privacy and proxy services must relay something. And I think Kathy's addition to that that she sent out early this morning -- and maybe I'll get both of them to clarify here -- is that sort of the minimum. And I think there's agreement on this is that privacy and proxy services must relay all communications that are sort of required by the RAA or consensus policy within ICANN.

Steve or Kathy, perhaps you could elaborate on those points.

Steve Metalitz: Well this is Steve. My point was just that a policy that says we won't forward anything would not be acceptable.

I agree basically with Kathy that those things that are required to be sent to registrants should be forwarded. But I also think that bona fide complaints about abuse should be forwarded. So I agree with Kathy as long as it's understood this is not a - this is a minimum but there are - there's some additional things that should be required under the standard relay processes.

Graeme Bunton: Okay. Thanks, Steve. Kathy?

Kathy Kleinman: And Graeme, I think you got it exactly right that the baseline minimum should include the forwarding of emails required under the ICANN rules to registrants.

I just remember that there was a tweak that was discussed that meant that some of the proxy privacy service providers had already taken care of responding to some of this communication in their contracts and in their procedures. I'm not really sure how to reflect that. But just establishing the baseline minimum of the communication itself, the - this kind of routine communication was what I was seeking. So thanks very much.

I also think David Hughes had an addition as well. I don't know if he's on the call.

Graeme Bunton: David, I - I'm not sure if David is either. I believe he was -- thank you, Kathy -- I believe he was talking about hard copy. So we may get there. Hopefully we'll get there.

So from that we've got that there - there's a (unintelligible) that all the (unintelligible) RAA required notifications seem to be sent out. Steve is suggesting that on top of that any bona fide complaint should be relayed as well. And I'm not seeing any hands or any disagreement on that. So that sounds like there's, I think, reasonable agreement on that.

Tim's raising in the chat what does bona fide mean which is a good question. Do we have anyone who wants to speak to what bona fide might mean in this context?

Steve does. And then we've got (McKaley). Please, Steve.

Steve Metalitz: Yeah. I mean I'm just - I'm using this in a very general sense that we've - I think we've already agreed or we've had some discussion about steps that would be legitimate for providers to take to screen out harassing, you know, auto-generated submissions such as a CAPTCHA use of a web form.

And I think we've also agreed that it's appropriate if -- although not required -- to have some type of spam filter. We might need to talk more about what that it. But I'm kind of going beyond that, that I think there should be an obligation to forward, you know, the presumption should be that relays - that the relay would happen.

I'm not saying that necessarily providers would be required to manually look at these and decide whether they are bona fide or not. But I'm just talking about screening out the - through CAPTCHA and through spam filtering, but everything else should be forwarded. That's kind of my perch on this.

Graeme Bunton: Thanks, Steve. If I can interject before I get to you, (McKaley), you did raise that on the list. And I think there seemed to be agreement from the last call that that sort of implementation of spam and CAPTCHA was an acceptable limitations on relaying everything. (McKaley)?

(McKaley): Yeah. Thanks. I mean I suppose from my perspective what I'd be looking at is rather than defining what I would consider to be a genuine or legitimate or bona fide or whatever term you're comfortable with, complaint more what I consider to be the - an abusive complaint.

But I've - we have one particular entity who sends us I think on average 500 complaints per day, all in relation to one or two domain names even though we've told them repeatedly that what they're sending us is of absolutely no use to us. They keep on doing it.

So from our perspective rather than bothering our client with 500 spurious complaints every day we just reject all the notices from that particular

complainant because I mean in many respects it's harassment. It's also incredibly stupid.

So I think, you know, this - there is a line there somewhere. I mean I'm not sure what - how one can clearly define the line. I don't know how we can do that.

I mean I think, you know, Steve mentioned on - a few things there. Again for the record I find it odd that Steve and I actually agree on some of this. It's like oh my god, hell's freezing over.

But, you know, it, you know, the thing is that obviously, you know, I would assume that certain people know what the hell they're doing and aren't going to send a registrar in Ireland or a privacy service in Ireland something that they can't do anything with and vice versa.

I mean I don't think that two (unintelligible) would be particularly impressed if a local - the local guard, the sergeant, from (Carlo Town) appeared on your doorsteps. You wouldn't have a clue who the hell he was. It's the same with anything else like that. So I think that's probably my way of looking at it. Thanks.

Graeme Bunton: Thanks, (McKaley). I'm not sure where the sort of upper bounds fits that you're discussing there, that, you know, if we...

(McKaley): I don't...

Graeme Bunton: Need to say...

(McKaley): I don't know. That's the problem, Graeme. I just think it's one of those things. It's like, you know, when you know it you'll recognize it. When you see it you'll recognize it.

I think we need to be careful about being overly proscriptive in how you define this because otherwise you'll see people just working around ways to circumvent it on both sides.

Graeme Bunton: Thank you, (McKaley). This is Graeme for the transcript again in case someone missed me saying that.

If I can put my registrar hat on for a moment, as (unintelligible) liked to say, if there is an opportunity to abuse that relay service it will be abused has been our experience anyway. So it is worth discussing and maybe thinking about maybe as a discussion for the list on what sort of constitutes that sort of upper bounds. And I'd be very curious to hear other people's thoughts on that as well.

That's enough from me. Kathy?

Kathy Kleinman: Hi. Am I off mute then? Okay.

I wanted to agree with (McKaley). And I'd actually got in the queue to say something similar which is that we should be setting a floor, not a ceiling because I'm concerned, you know, harassment by divorce attorneys happens all the time in lots of arenas including domain names but just one of many.

So this idea of letting the proxy privacy service provider decide when something's become harassment I think is something we should leave for them. That call is being made in lots of other arenas. It should be made here too. Thanks.

Graeme Bunton: Thanks, Kathy. Registrar hat again for the moment is that I think you're probably right in that respect that we see that sort of behavior and we're able as a registrar to identify. And for the most part that works in the context where we see it.

Anybody else on this particular topic before I think we're going to try and move on to relay failure as Alex raised it? I see another hand from Kathy and Steve. So let's go to Kathy unless that's an old hand.

Kathy Kleinman: Sorry, old hand.

Graeme Bunton: Steve?

Steve Metalitz: Yeah. This is Steve Metalitz just to say I feel reasonably relaxed about this as well. But I think we do have to recognize that there is also a capability to abuse this the other way and to decide that, you know, allegations of abuse are per se harassment or in some other way act in bad faith that - and not relay.

I, you know, I think we could probably come up with a pretty good formulation that recognizes that there's no way to completely anticipate this but that reasonable - commercially reasonable types of spam filtration and so forth are acceptable. I think if a registrar - we - I think we just need to leave open the possibility that if a privacy or a proxy provider is kind of abusing that capability that there would be a way to get a remedy for it. Thank you.

Graeme Bunton: Thanks, Steve. This is Graeme. I suspect that if they were abusing that it would be an issue for compliance. But I think we can clarify that a little bit more as we go forward.

Anyone else? Yeah. Carlton's agreeing there. All right.

So is Alex on the call? He is. So he was raising how does the requester know of a failure to communicate with the registrant. And he was suggesting that there should be parity between the private - the non-privacy in a proxy world where if they email someone from the Whois information and they get a bounce they know about it whereas if that occurs through a privacy and proxy service provider that they don't know.

And James responded. And he's not here which is too bad cause I think he's quite well dialed-in. And I'll see if I can characterize his response. And then we can discuss it a bit more. But anyone feel free to correct me if I have - if they think I've done so in - that's not - in a way that's not true to what James is saying.

So what I think James was saying is that that first bit where you're contacting - where you use that information, the Whois, that is for the privacy and proxy provider you are communicating with the proxy service and not the registrant. And so if that fails then that's a compliance issue.

The communications between the proxy service provider and the customer, a third party has no, you know, right to access - to know whether that failed or now. However if that communication is be - around a verified field under the RAA and it fails then that would kick off a verification process again. And by looking at the domain 15 days later you could know if it had failed or not.

So I think that's the gist of what James was saying. Perhaps, Alex, you could elaborate if you wouldn't mind on your position if I can put you on the spot.

No. Sorry, Alex, can't hear you.

So Alex will dial in. We'll give him a minute. Does anybody else have thoughts on this particular topic around what happened if there's a failure to communicate with the registrant?

Man: There's a question from (Christine) in the chat, Graeme.

Graeme Bunton: I see that. (Christina), you would know because the domain was suspended. So either it doesn't resolve anymore or the DNS has been changed to a notification page about that.

It's not super precise however cause unless it is a this domain has been suspended due to failure to verify contact information or if it just doesn't resolve then it could have gone down for other reasons. So it's perhaps indicative but not definitively indicative. Steve?

Steve Metalitz: Yeah. This is Steve Metalitz. I think you - I believe you've correctly characterized James's position.

And I don't agree with it. I think that in the situation in which the registration is not a proxy registration you know immediately if the email that you've sent to bounces back, for example, just to give that - use that example.

And so the idea that in 15 days you might find out, you would encounter a scenario, if you happened to check, that showed, you know, that would at least be consistent with the email address not working but might also be explained by a lot of other things, I just don't think that's a satisfactory substitute.

We really want to, you know, we're not - the goal here is - or what the third party's trying to do is contact the registrant. And I think it makes sense to put that third party in the same position, at least to know whether - that the route he's tried has failed and then he must - has - needs to try to find some other way. I don't see the justification for holding that information back.

Now I think in the dialogue that Alex and (Luke) had online it may be that they were coming to convergence on that. But I don't agree with James's position.

And I think in response to (Chris)'s question, yeah, in that situation where the email works but there's no response, that's a different situation. But until - basically the third party doesn't know if they sent something to be relayed and then they get nothing back they don't know which of the two scenarios applies. Is it something where the email is invalid and has bounced or is it something where it's been received but there simply has been no reply? And

I think it's - we want to be able to allow the requester to distinguish between those two situations.

Graeme Bunton: Okay. Thanks, Steve. Alex, you want to give it a shot?

Alex Deacon: Yeah. Can you guys hear me now?

Graeme Bunton: We can hear you. Thank you.

Alex Deacon: Okay, good. Sorry about that.

Yeah. I think it's been summarized well while I was struggling to get my headset working.

You know, I think the ability to know when something has bounced or a failure has occurred is important. And I just want to make sure that there is parity.

I also don't agree or don't quite understand James' comment that, you know, that there - we - that a requester has no right to know when something bounces. I don't quite understand that. Maybe I just don't appreciate it.

But in the end I think whether it's email and whatever form of email is implemented by the privacy proxy service and if there is a known failure then it should be returned to the original requester (unintelligible). And similarly I think that should follow through for trying to contact via phone although I understand that doesn't happen too often. But also with snail mail and postal mail if there is a failure in that relay then that should also be made known. So that's basically what I was trying (unintelligible).

Graeme Bunton: Thank you, Alex. Chris, did you have a registrar response there?

Chris Pelling: Hi guys. Chris Pelling for the transcripts.

A couple of points, Steve and Alex, listening to that. I made a point last week in connection with how we will be handling our way of doing things. But reading obviously the left-hand side text boxes that face up and down, there are going to be issues whereby you would email as in law enforcement or whatever service will email the privacy protection service. That may well be relayed.

And (Michelle) mentioned this earlier. However, Gmail or Hotmail would or may well mark that as spam in which case it will go straight to somebody's spam folder.

Now we (unintelligible) although we've done our part of handing that over we confirm back to you that oh the mail has been successfully delivered, as an example, to, oh gosh, give out one of Gmail's long, funky server names and at that point you still don't get a response. What will that prove to you? At the end of the day it proves nothing on the basis of you still don't receive a response back.

I mean if it's a straight bounce, as I think (Michelle) was saying this earlier, it comes straight back under the RAA 2013 where the contact is a failure and it bounces. And at that point after 15 days the domain is put on a suspension page.

And my concern is - here is we're not here to police this. The biggest problem is automated delivery systems. As an example, (MTA), it's (Metro Transfer) service. They will look at an email. And spam assessing does a very good job at this unfortunately. They will look at an email and go is it spam or is it not.

Now with servers doing that and therefore blocking content, at no point can any privacy protection provider or any registrar guarantee that the email has been put in front of a physical person to read. Just a quick point.

Graeme Bunton: Thank you, Chris. Alex, is that a new hand?

Alex Deacon: Yeah. Hi. I just wanted to -- it's a - it is a new hand -- I just wanted to respond to the point that Chris just made.

I don't disagree. I think in the case where there is no privacy proxy in between the - and there is no filter in between, you know, sending emails off to a black hole and the response is returned, the original, you know, sender of the message would receive the error back, again all I'm asking for is that if a bounce does - is returned or an indication of failure is returned to the privacy proxy service that that makes its way back to the original respondent.

You know how email works and how filters complicate things. And I just want to make sure again that we have parity between the case where there's a privacy proxy service in between the requester and the registrant.

Graeme Bunton: You broke up a bit there near the end, Alex, I think. Could you repeat that last part?

Alex Deacon: I just want to make sure that there's parity. I don't know where I broke up. I apologize.

I want to make sure that if there is a - if the privacy proxy service does receive a - an error response of any kind that that is relayed and made known to the original requester. I understand that...

Graeme Bunton: Okay.

Alex Deacon: There are services in between that may block that. That's the case whether there's a privacy proxy service in play or not.

Graeme Bunton: Okay. Thanks, Alex. Tim raises an interesting point that -- and this is worth thinking about -- that - how would this would verified or enforced. And I'm -

can't think of anything off the top of my hand. Volker, did you have something to add?

Volker Greimann: Yes. I mean I look at such tickets from time to time from - that we get in the abuse queue and some of those that we get in the Whois queue. And certain times depending on how the mail server of the recipient is set up we just get a mail back: your message could not be delivered. But we don't actually see which message this bounce message is referring to. So we might get a bounce message but we have absolutely no clue which one of the hundreds of tickets that we just sent out over the day this actually is.

So this may just - depending on how the mail servers of recipients is set up we might not even know which one has bounced and never be able to find out without putting an extraordinary amount of work. So before we make this a recommendation we should check for the realism of actually being able to give that information back.

Graeme Bunton: Thanks, Volker. Was it - if I could get you to clarify briefly, it was Key Systems, I think, that does the - that has the scenario where you rotate the sort of random character string at your privacy service as part of the email (unintelligible). That only lasts two weeks. So you would need to be able to store a history of that sort of thing. So you've got this mechanism to prevent spam that might make it extremely difficult to track bounces back to the initial address it was sent to?

Volker Greimann: It really depends on how the message is sent up - set up. In some cases the - where the encoded string is used for an email to the registrant, in most cases the bounce would be sent back immediately to the sender because we only relay. But in some cases there - the bounced message doesn't specify which message it's referring to. And it just says your message could not be delivered. And it never says ID or subject or whatever might be helpful to relay that. And then though - in such cases we simply cannot relay.

But yes we do have a history. And the encoded string actually includes information on how and when the information was sent and who is the recipient. So yeah, we have a history function for that.

Graeme Bunton: Okay. Thank you. (Chris)?

(Chris Vanetta): Hi guys. (Chris) for the record, (Vanetta). The guys actually - one way to use it making the argument but all intents and purposes it's the discussion we're having, making the argument about relaying and getting back responses, etcetera, etcetera.

I'd like to put the cat amongst the pigeons, typical British term of asking a question. How exactly do you handle sending them a letter to appear box in America that you get no response from and continue to get no response from? You don't get any receipt that the letter's been received? You may get a signature if you send it as a - in the UK it's called a recorded delivery.

But I'm just trying to work out the different avenues you're going to use to contact as somebody that may be on - not using a privacy protection service. But you've sent your email. You've gotten a response or a bounce-back. And you're now doing a letter. I'm just trying to work out in - from a privacy proxy service. Would you then go on from there cause obviously at that point it's much the same as not getting any confirmation via email? That was the question. I'll stick it out there and (unintelligible).

Graeme Bunton: Thank you, (Chris). Anyone care to respond to that? (Christine) is pointing out that U.S. postal service does provide delivery confirmation. Steve?

Steve Metalitz: Yeah. This is Steve Metalitz. I'm not sure if I understand the question. But I think there is a distinction in the PO box situation between sending something and never getting a response or sending something and getting a stamp back from the post office says this post office box does not exist. That's really the distinction that we're talking about here.

And I mean I accept that there may be ambiguous situations where it's not clear that the message has bounced but I think what we're suggesting here is that where it is clear that the message has bounced the - and the requestor ought to know that.

I think (Luke) pointed out online that in many cases that would be he case but where it's not I think that we're suggesting that it should be, thanks.

Graeme Bunton: Thanks Steve, (McKaley).

(McKaley): Yes (McKaley) for the record. I'm kind of - my heads beginning to hurt. What exactly are we trying to do here. I'm like are we trying to rewrite communications protocols or are we simply trying to set some kind of requirement that people can actually follow without their heads exploding?

I mean the thing is, you know, you're taking email - email is one of these things that as a hosting provider you realize very quickly that if I switched off our email servers our phone system would probably melt, explode or whatever for the number of phone calls we get.

Whereas if I turned off our Web servers for half an hour quite a few of our customers wouldn't even notice and there is kind of wonderful assumption that email works beautifully and wonderfully and smoothly all the time.

But as others have noted it's impossible at times to know what the hell is going on once an email has left your route box. I mean I regularly get bounced messages from some ISP's even though the mail has actually been delivered, which I find terribly confusing.

Volker mentioned getting bounce backs that aren't at all clear and we could spend hours talking about all the technical issues around this. But the

question I have is, you know, on a much simpler level without getting bogged down and giving us all massive headaches.

What exactly do people want to achieve with this? Do you want to achieve - do you want something - kind of thing that okay if the registrar or the proxy provider is knowingly - has been made aware of or has knowledge of a problem with something that they're meant to do with or are you asking them to go off and to go to all the crazy lands with little or no actual return, thanks?

Graeme Bunton: Thanks (McKaley) I think you are close to what the ask is I'll see if I can characterize it like this that - and then I think Mary was there also is that, you know, if a privacy and proxy service has knowledge that a communication has failed then they are required to notify the requestor.

And it's sort of the - is that the sort of thing that we can include in our recommendations here? Alex.

Alex Deacon: Yes, thanks Graeme this is Alex. So I think we're getting closer to what we're requesting clearly is to go back to the question around postal mail if in the case where no privacy proxy is in between and it goes to a PO Box or whatever the equivalent is elsewhere and there's no response then we would get no response.

In the case where that happens between the privacy proxy service and the registrant then again I assume that the original requestor would get no response.

But I think if there is a failure that the privacy proxy service is aware of whether it's email or postal mail or otherwise then that should be returned in the case of Steve's example where he says there's a specific error that says this postal or this person is not known at this PO Box.

Then we should - that information should be relayed that's all we're saying. We're not - I'm not asking to, you know, create new communication protocols that's clearly not within scope I'm just - I want to make sure that we get the, you know, information back in a case where there's no privacy proxy involved.

Graeme Bunton: Thank you Alex, so there's a lot going on in the chat that I'm also having a bit of a tough time following that as well as the conversation so if there's something I need to highlight in there please bring that to my - we've got Kathy, Kathy care to respond.

Kathy Kleinman: Hi Graeme, hi all. Yes what I wrote into the chat and thanks for the invitation to bring it into the oral discussion is that I really like Steve's idea of using the term commercially reasonable.

So as I understand it a phrasing of that would be that the proxy privacy provider uses commercially reasonable means to deliver the email, you know, any of these emails that fit the categories that we've been talking about.

That makes sense to me that attempt to deliver but any kind of response I think sounds like it's going to be technically burdensome in terms of staff and personnel and perhaps impossible to pass on a response.

And I think we're beginning to talk about huge numbers of emails that are going to be relayed through these systems. So let me throw the idea out there and I don't even want to go down this path because I think we should really stop at commercially reasonable means to deliver.

But when you get a return receipt in the U.S. you paid for it and so I saw that floating around in the chat as well. Should those who are trying to send messages to be relayed pay for some kind of receipt if it's even possible? So thanks Graeme.

Graeme Bunton: Thanks Kathy I saw that in the chat too and it's an interesting idea I'm curious to hear other peoples responses. I'd like to spend maybe a few more minutes on this topic but we're - we've also been dancing around the, you know, the physical mail, snail mail aspect of this a bit and so maybe we should cover that a bit more directly.

So let's try and wrap this discussion up a little bit and then we'll move on, (McKaley).

(McKaley): Yes, thanks Graeme, (McKaley) for the record. You know, just on the commercially reasonable just to make sure that we're clear, you know, what would be commercially reasonable for (Tucos) or for GoDaddy wouldn't be commercially reasonable or may not be commercially reasonable for (Black Knight) or other registrars.

I mean there's a significant difference I mean how many staff does (Tucos) have as a group? You have a call Graeme you can answer. You know, we have like 30 on staff (Tucos) has I don't know hundreds of staff?

You know, there's a lot of differences in what's commercially reasonable for a small registrar or proxy provider and what's commercially reasonable for a very, very large provider, thanks.

Graeme Bunton: Thanks (McKaley) I'm going to let Mary jump in.

Mary Wong: Thanks Graeme and just before we move on I think - I'm just trying to go through some of these suggestions and capture them in notes. So going to first the commercially reasonable point and clearly that's no problem with adding that.

It seems to staff though that that deals with the act of trying to deliver and that would be what happens when the provider first gets the request and then tries to deliver it.

It seems to us that maybe Steve and Alex and others were talking about something slightly different as in what happens after that is something is not delivered or undeliverable.

Should there be some kind of a partial obligation to report that at least in a case where the provider knows that there was a failure. So it seems to us that the two points are slightly different and the now conclusion or preliminary conclusion we might want to capture both labors.

So I just wanted to clarify that with you and the rest of the group, thanks.

Graeme Bunton: Thanks Mary I agree those are two distinct points. Todd.

Todd Williams: Thanks, Todd Williams for the record. I, you know, I have been listening and I just kind of wanted to try and simplify. I think I understand that the argument is that, you know, it may be difficult to determine when there has in fact been a delivery failure.

But I think Mary's point, which is well if you add something like knowingly that in large part addresses that what I'm not understanding is in okay say we have knowledge of delivery failure what is the argument as to simply notifying the original requestor of that knowledge?

And I don't know that I've necessarily got my arms around what the counter argument on that point is especially given that, you know, as I mentioned in my email that little bit of information can be quite valuable to the requestor.

I know we've got to move on I just wanted to put that out there, thanks.

Graeme Bunton: Thanks Todd, Steve.

Steve Metalitz: Yes I know we need to move on, Steve Metalitz here but just to say my suggestion about commercially reasonable really applied to the use of

filtering or preventing harassment not necessarily to delivery as a whole I don't have a problem with commercially reasonable efforts to deliver but I did use it in a different context.

And I would agree that what we're really talking about on the bounce back situation is whether it's known to the provider that delivery has failed, thank you.

Graeme Bunton: Thanks Steve. I think we'll probably need to discuss this a little bit more on list and there was also that idea floated that I haven't heard directly addressed around if the service provider is able to charge a fee for delivery receipts by mail.

So let's continue to think about those things and all right (McKaley) I'll let you jump in there quickly.

(McKaley): No sorry, just very quickly on the cost thing I mean just for those people who are actually on the call I mean, you know, Steve and others I mean would you have a massive issue with us charging you a nominal fee for a notification if we were able to guarantee that we were to give you I don't know something back that you could use for whatever.

I mean do you find that completely offensive or would you consider that would be reasonable. I mean I honestly don't know, which is why I'm asking thanks.

Graeme Bunton: Thanks (McKaley), let's try and do this quickly Steve and then Todd and then Kathy and then maybe we'll...

Steve Metalitz: This is Steve I'll just give my quick response, which is I mean I'm really concerned about Tim's point in the chat if it has value to the requestor and the cost recovery fee seems reasonable that - under that logic you should start charging for Whois and you start charging for anything that's of value to the public if you could find someone to pay for it.

I just don't think that we should be going there and my initial reaction would be if you know it's bounced back let the requestor know because you want to put them in the same position as if they were - have them disadvantaged because...

((Crosstalk))

(McKaley): Steve with all due respect that's not what I'm asking. I'm asking if for example I was to give you something more than simply informing you of a bounce back that's what I'm asking you.

I mean it's - it's like in technical terms I can self-sign an SSL search but I don't have any guarantees with it because it's not signed by VeriSign or (commode) or whoever.

So if I was to charge you let's just say a nominal fee I'm not talking about cost recovery but a nominal fee and give you something more than that is that offensive to you or is that something that you could consider, thanks.

Steve Metalitz: Okay well thank you for that clarification we'll consider that. I'm still not sure exactly what you're offering here but let's pursue that.

Graeme Bunton: Thanks Steve, Todd and then Kathy real quick.

Todd Williams: No that's fine I mean I know we got to move on and I would basically agree with what Steve said, you know, my point was more on just the notification. It sounds like what's on the table is actually something more than the notification so I'll kind of reserve comment thanks.

Graeme Bunton: Thanks Todd, maybe we can have (McKaley) flush that out a little bit on the list for us, Kathy.

Kathy Kleinman: Thanks Graeme just a quick point as wrap this up that somebody is going to have to pay for this service, which sounds like it's time consuming. This type of response from what we're gathering sounds like it requires human intervention, it requires sorting through a lot of material, interpreting messages that aren't clear.

Somebody is going to have pay for it so it's either the requestor or the customers. So as between the two we really have to think about it, I think it should be the requestor thanks a lot.

Graeme Bunton: Thank you Kathy, so let's continue to have that discussion on the list I'll see if I can push James to clarify his position as well and we'll see if we can move that discussion forward there.

Snail mail hard copy, forwarding (David) from the RAA brought this up on the list and we do need to cover if there are minimum requirements for relaying physical mail.

If you read through the responses from some of the privacy and proxy providers on the information that we've collected then there are - there's a number of approaches people are taking.

Quite a few people won't take any of it or sorry some people won't take any of it, quite a few people are doing where they'll scan and relay. We need to decide I think if three is a minimum requirement on physical mail, Volker.

Volker Greimann: Okay personally we do not on our service relay messages we are not a mail forwarding service and any communications can just as well be sent out through emails so we don't need a physical copy.

And when we get a physical copy and when we get a physical copy I personally lit my furnace with it seeing that there was no way that I could with reasonable effort forward it to the complainant to the registrar.

And we sent the complainant an email saying please send it again. If you want us to forward it to the recipient please send us an email or even better use the coded email that's in the Whois.

That way you will be certain that it reaches us but we will not forward. In certain cases we were not able to do that because the complainant did not include an email address. In such cases we just throw them away.

Graeme Bunton: Thanks Volker, someone should correct me if I'm wrong and sorry this is Graeme as I speak for a moment. I don't believe that the physical address fields are verified under the RAA, which means physical mail may be less likely to get anywhere than email. So (McKaley).

(McKaley): The 2013 RAA the only things that can or could be verified under the contract would be either a phone contact or an email address. However that doesn't mean that the physical address is necessarily going to be incorrect.

I mean that's like saying well I don't know 20 Christians on the call how many of you have seen God, I mean just because you haven't seen your God doesn't mean that your God doesn't exist, you know, it's not a logical step to say that just because it hasn't been verified it's going to automatically be wrong, thanks.

Graeme Bunton: No I'm - sorry I wasn't trying to suggest that it was by default incorrect just that it is potentially less reliable. Steve you're saying there that (David's) suggestion was forwarding mail and electronic communications was failed in particular could you elaborate?

Steve Metalitz: Yes this is Steve, going back and looking at (David Hugh's) email he said when we've tried and we've failed to communicate electronically we're making another attempt through physical letter.

So Volker's point was, you know, when he says he gets back to the requestor and says send an email to this, you know, to the address we've provided this I think (David) was talking about a situation where that's already been tried.

And maybe there's been a bounce back or maybe there just simply hasn't been a response I guess it could be either and I guess if we're not told if there's been a bounce back then the requestor wouldn't know which it was.

But he's saying at that point when it's been - when the email address that the provider has given to the requestor hasn't worked should there then be an obligation to forward it on so it's just in that case.

Graeme Bunton: Okay thanks Steve. The reality mail is interesting in that it is expensive to do, you know, it requires someone to open that mail and scan it as we do and so there is a cost to that service, which I think was part of (David's) question. Do any registrars on the call have a sense of that cost and or do we collectively think that we - do we or sorry privacy and proxy service providers I guess in this case are they obligated to do some sort of forwarding with mail and is there a cost recovery mechanism that's amenable to the community?

(Chris) do you want to speak?

(Chris): We looked at it from the point of view of the majority of complainee's is the wrong word to use but you understand by I mean the ones that connect to a registrant normally are law firms.

And a lot of time you go through the fact you've told them you don't or you are not the hosting company. You receive essentially a ream of paper. By the time you've signed for the document, open the packet, read the first 10, 15 lines to find out what it's about.

Then 10, 15, 20 minutes in trapping the scanner getting it in the IDF, pressing the button, getting the registered record, getting the email address, basically

scanning it to a PDF, sending the email you're looking at around about one-half hour per document depending if you IDF is quick enough of course.

At the end of the day that comes to man hours, you know, if you're doing 10 of those idea ideally that's five hours. On a cost basis that's 500 pounds, 100 pounds an hour.

So, you know, you've got to consider that largely what we do as an example we charge the sender. If they wish to send us a FedEx package up to 30 pages they are charged $30.

That pays for us to sign for the document, scan it, send it, provide back to the sender by email a letter signed by us to confirm it has been delivered. And then oversee - you don't find out who it was delivered to but you do get from us a letter confirming it has been delivered.

The cost basis is time and in this day and age like lawyers you charge for it so we must as well that's it, I'll sign off.

Graeme Bunton: Thank you (Chris). Any other responses to that? There we go Steve, thank you please go ahead.

Steve Metalitz: Yes this is Steve I agree there's a cost involved here but I think let's kind of look at what we know now as we look through the template at the summaries of the terms and conditions of the existing services I see that one and one Internet will forward - will forward and scan all first class mail, mail received either certified mail or courier.

I see that the names by proxy will forward certified or traceable courier mail or first class U.S. Postal Mail at least if they're legal notices. I see that Whois privacy service will forward registered mail or traceable courier so in other words some hard copy material they will forward.

In other words a number of privacy proxy services seem to be doing this now so this is, you know, obviously not everyone is doing it and there are cost considerations to be taken into account.

But I just want to point out that a number of them say that they do this now as part of their regular business, thanks.

Graeme Bunton: Thanks Steve as a registrar we do scan and forward on registered mail and traceable courier packages as well. I will endeavor to go back to our compliance team and figure out what kind of volume that we see to get a sense of how impactful that is for us. I'll see if I can share that with the group, (McKaley).

(McKaley): Yes this is kind of not directly on this but kind of related. I think one of the things we need to be very, very clear about and make sure there is (unintelligible) there because I just see it as causing headaches for everybody is, you know, there is no obligation on a registrant to respond.

Be that to an email or to a snail mail notification I mean it doesn't matter what the notification is it's a better communication. I mean I'm right beside my desk at the moment I have three letters that were sent to me in the last week or so by various companies that are trying to get us to buy products and services from them and they somehow managed to get my name and everything else.

I mean I'm not going to reply to it I'm under no obligation to reply to it. Sure you send me a court order, you send me something, which is legally obliging or legally binding on me fine of course I'm going to take action of course I'm going to respond to it.

But I want to make it very, very clear that, you know, you don't want a situation where let's just say I'll pick on Microsoft or Google that, you know, Google has to respond to every single serious request that they get about I don't know domains or things that they host or that they have on a domain.

I mean it's just the concept of that kind of obligation scares the hell out of me. You know, that a privacy proxy service would need to relay something, make best effort commercially reasonable et cetera, et cetera and everything else fine but this, you know, the thing that worries me is any obligation for a response, thanks.

Graeme Bunton: Thank you (McKaley), really quick Darcy.

Darcy Southwell: I just - this is Darcy Southwell I just wanted to say we have a couple different platforms so we do it two ways one of which though we do funnel everyone into no mail and they have to email us.

And I guess I'm concerned that we're talking about requiring privacy proxy providers to allow for all methods of forwarding. If we have proper contact information that works as a provider then we should be able to funnel everything into email.

And it seems like we're focusing on having and we haven't talked about phone calls today but we talked about them last week about how we need to handle all of these different methods.

And I'm concerned that we're not focusing on having good contact information and funneling it into a way to easily get it to the registrant, which is the focus, thanks.

Graeme Bunton: Thank you Darcy and I think that's a good point to end on. So I think we'll probably be doing a little bit more of E1 next week. Hopefully we can continue to have some really good discussion over the list, which was great to see some of that this week.

I strongly encourage everyone to participate there again this week and then hopefully we'll be able to dig into E2 as well next week. So thank you

everyone for coming and we'll see you again in a week and (Don) should be back for then.

Man: Thank you.

Man: Thanks Graeme.

Woman: Thanks Graeme thanks everyone, (Terry) we can stop the recording.

Man: Thank you.

Coordinator: Thank you very much, again that does conclude the meeting for today thank you everyone for joining. Please remember to disconnect all remaining lines. (Andre) if you can please stop the recording.

END