ICANN Transcription
Privacy and Proxy Services Accreditation Issues PDP WG
Tuesday 29 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 29 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-20140729-en.mp3

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

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
Alex Deacon - IPC
Kristina Rosette – IPC
Paul McGrady – IPC
Carlton Samuels – ALAC
Todd Williams – IPC
Michele Neylon – RrSG
Tatiana Khramtsova – RrSG
Roy Balleste – NCUC
Frank Michlick – Individual
Phil Marano-IPC
Luc Seufer- RrSG
Volker Greimann-RrSG
Don Blumenthal – RySG
James Bladel – RrSG
Osvaldo Novoa – ISPCP
Libby Baney-BC
Susan Prosser-RrSG
David Cake-NCSG
David Hughes-IPC

Apologies:
Holly Raiche – ALAC
Stephanie Perrin – NCSG
Tobias Sattler-RrSG
Lindsay Hamilton-Reid-RrSG
Tim Ruiz - RrSG

ICANN staff:
Mary Wong
Amy Bivins
Terri Agnew

Terri Agnew: Good morning, good afternoon and good evening. This is the PPSAI working group call on the 29th of July, 2014. On the call today we have Tatyana Khramstova, Graeme Bunton, James Bladel, Steve Metalitz, Alex Deacon, Michele Neylon, Roy Balleste, Susan Kawaguchi, Sarah Wyld, Chris Pelling, Griffin Barnett, Justin Macy, Darcy Southwell, Todd Williams, Val Sherman, Osvaldo Novoa, Libby Baney, Don Blumenthal, Frank Michlick, Paul McGrady, Volker Greimann, Kathy Kleinman and Phil Marano.

We have apologies from Tobias Sattler, Holly Raiche, Lindsay Hamilton-Reid) and Stephanie Perrin. From staff we have Mary Wong, Amy Bivins and myself, Terri Agnew. I also see that Susan Prosser has joined us as well.

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

Don Blumenthal: Hey, I appreciate it. Going to make a request before I get going, I seem to be an eternally headset challenged person and I can't - so I'm experimenting with ways of muting my system.

Please let me know if what I do is creating background noise. Send me a text or whatever but - we get this figured out. In any event, it's - just as I was about to comment on how last week's email list had been so active and this week's had not been, I opened email this morning and suddenly that wasn't the case anymore.

So I really appreciate the - everybody's involvement. It's great and really important for moving us along to keep the conversation going in between discussions.

And if nobody heard mute come on that time, then I think I got it figured out. Heard mute come on - that's a little bit of an oxymoron but I'll move on. Normally I would start off with returning to last week's subjects but I think we kind of began that in the discussion that's gone on yesterday and earlier this morning.

So I think generally let's move on with you. I'm not sure if we'll have time to get into how things have picked up. And I'll be honest with you, I'm frantically looking for a draft of something I had yesterday that's disappeared. Who does - I'll just flat out ask. Steve, did you get my message about forwarding…

Steve Metalitz: Yes, I did, and I resent but I'll do it again.

Don Blumenthal: Please. Sorry about this. Okay, I seem to be having some problems with my email program here. Let's see, okay, Steve or (Graham), could you remind me, what was number one and then I'll - everything will come back in place?

Steve Metalitz: Yes, this is Steve Metalitz. I think the first question that we left from last time was this issue about an email message is sent for relay and it's relayed and it bounces back as undeliverable. So the first question was - that I think we had not fully resolved, was just the providers are supposed to notify the submitter of that bounce back.

Don Blumenthal: Yes, and as you were talking, most of your follow up showed up, so. I appreciate it. The gremlins are here. Yes, I looked at - listened to the transcript, read the - listened to the recording, read the transcript and looked at the follow up on the email list.

And, yes, wanted to see where we are on one of the questions. If email bounces back, does the submitter have to know? I saw comparisons to the RAA requirements but I guess the questions is, are they (topical)?

Because, I think as has been pointed out, the requester, the submitter for lack of - however you want to call it, knows if there's been failure in the case of a registration that's in the open. The submitter doesn't know if there's a failure if it goes through a proxy privacy.

And should that be different? And I want to clarify. I think there might have been some confusion last week on what we were talking about. It looked to me as if some people responded to the question whether there should be - what happens if there's a failure of email to the proxy privacy service?

And I don't think that's what we were addressing, a failure of message from the privacy proxy through the registrant or the beneficial registrant of a (unintelligible). Any thoughts on where are there or where we should be? Steve?

Steve Metalitz: Well this is Steve Metalitz. Our view is that the requester or submitter should be notified in that situation. Again, as you said, that puts them on the same footing as in a non-proxy situation. They know that the beneficial registrant or customer or whatever you want to call it has not received the message, so then they figure out what else they try to do to contact them.

But that's, you know, without that, they don't know. They just send something out and they haven't received any response which may, as several people have pointed out, simply means that the registrant chose not to respond.

Don Blumenthal: Okay, thanks. James is early on this (issue). (I'll) hand it over.

James Bladel: Thanks, Don. James speaking for the transcript. And understanding the scenario here where a third party has sent a message to the privacy service for relay, privacy services attempted to relay to the email address that is a non-public email address that it maintains for its customer and that email address - that email bounces or is somehow undeliverable.

You know, just a couple of quick thoughts here. First off, if we're going to align this with the equivalent procedure in the RAA, then the trigger on this - the triggered event would be that the privacy proxy service would then have to contact their customer and reverify the information that they have on file.

That is currently the obligation that we have if a verified email address bounces either with an ICANN message or a required communication. So I think that is definitely something that we should require. However, to my understanding, I don't know of any requirement or obligation under the RAA that would require us to report that happening to a third party aside from ICANN compliance, not the sender or any other third party.

And I just wanted to point out that bouncing of email messages or undeliverable email failures could result from a number of situations that are not related to the email address being invalid. For example, there could be - an email server on the receiving end might be down or the mailbox may be full or the, you know, the privacy proxy service may have been tripped up.

Something in the message itself may have been tripped up by a spam filter. You know, if you used a keyword, for example, that you know, is triggering a spam filter, that thinks that it's a solicitation or, you know, or some adult material or something like that. So there're a number of reasons why something could fail and be unrelated to the validity of the email address. Thank you.

Don Blumenthal: Volker?

Volker Greimann: Yes, I basically agree with everything that James said. I'm trying to keep the workload as light as possible but still be reasonable with the information that the complainant deserves.

And I think it's not as easy as I immediately thought and I wrote my responses last week because if the complainant is not informed that the message has bounced, then he would be under the assumption that the recipient has at least received in some form the communication and that would not be the case if it bounced.

However, the message bouncing would trigger all kinds of different things and I would suggest that any proxy email that bounced would trigger the reverification process as is the case with registrars at the moment.

So - and then once the data has been fixed, then the message would be relayed again. That would be the course I see. I don't feel a necessity of immediately having to inform the complainant that the message has bounced but it might be something that is worthwhile looking at again down the road when the informa- when the data has been fixed or not fixed and the domain name -well, the actions have been taken by the privacy provider with regard to the invalid address.

Don Blumenthal: Appreciate it. You know, (unintelligible) answer to the question I was thinking about tossing into the mix will wait now. Alex?

Alex Deacon: Yes, hi, so I just wanted to understand I guess James' point a little better. This is Alex Deacon for the record. The reverification step that registrars and privacy proxies, perhaps, need to do, is a mechanism between the privacy proxy or the registrar and the end user.

But I think that's different than the use case that I have in mind at least, if I understand things correctly. And this is an email from someone on the outside being sent through the privacy proxy service to the registrant. If that bounces, it seems to make sense to me that this bounce notification - and I understand there're lots of reasons why things will fail.

I'd suggest that they all make it back to the original requester. It seems to me that these are different mechanisms so I'm not too sure that the RA- 2-2013 RAA is kind of in effect in this use case. So any clarification you may have would be appreciated. Thanks.

Don Blumenthal: Okay. You know, let's move on then. Michele?

Michele Neylon: Yes, Michele for the record. Not with addressing the previous question because I can't really because I wasn't the one who was dealing with it. Just another thought that kind of struck my mind around bounced messages is there are privacy implications with that because it would give quite a bit of information potentially about somebody's mail server on the far side. But that might not be a major issue, but at the same time, could see that being a potential issue. Thanks.

Don Blumenthal: Yes.

Michele Neylon: I'm sorry, by bounce in this context, I'm talking about, say, soft bounces as part - as opposed to hard bounces.

Don Blumenthal: Okay, do you want to clarify, distinct…

Michele Neylon: Yes, sorry, for the - a soft bounce could be when the mail server on the far side cannot process the mail for a number of reasons such as the mailbox is full, the mailbox is unavailable or the mail server is having some kind of technical issue, but the soft - a soft bounce message could include a whole lot of information about the server on the far side.

This would not - eventually the mail may be relayed but you'd still get the error in the interim because it's a four star code error as opposed to a five star, if you speak fluent SMTP. Thanks.

Don Blumenthal: I didn't know it was its own language. Did - James, did you have your hand up?

James Bladel: No, Michele, I think covered it, and others as well. Just - no, I think I'm good.

Don Blumenthal: Okay, just want to make sure you (teemed in) on purpose, that's all. Steve?

Man: I think the more relevant question was whether it went up on purpose. That's when it came down on purpose. Thanks.

Don Blumenthal: Oh, okay. I'll leave the other one. (Unintelligible). Steve.

Steve Metalitz: Yes, this is Steve Metalitz. Let me get back to James' point about this trigger reverification. If there's such a confusion about what's a soft bounce, what's a hard bounce, what's four digits, what's five digits, when does this reverification obligation kick in?

And let me just take it in the non-proxy situation. If you - if the registrars sends a, you know, Whois reminder notice or something else, to the address that's given, the email address that's given in Whois and it bounces back, that presumably triggers the obligation to reverify under the 2013 RAA.

So is there difficulty in determining when that applies or isn't there - or is there a way to determine when that happens and why couldn't that same test be applied here, in other words, when you're forwarding to the address given by the registry? So I just pose that to James or others in the registrar community who somehow seem to find it very difficult to determine when there's been a bounce back.

Don Blumenthal: Okay, yes, I saw James hand shoot up right there. Let me ask is - Volker or James, do you want to respond? A hand came up quickly. Do you want to respond to that point?

James Bladel: This is James speaking. I think if I understood the question - and I'm sorry if I didn't. The question I heard at the end was, do registrars have difficulty determining when a bounce has occurred?

I think that that answer is usually no. If we are watching for it, we can determine that a bounce has occurred. If, you know, if it's something that is being tracked.

I would state, however, that it is the capturing of that and then making the determination of whether or not a third party would have rights to the information that's contained in the bounce message or, you know, as Michele said, we probably - may have privacy implications on sending the raw bounced message because it may give away some aspects, some valuable, in fact, vulnerabilities about the mail server.

And then the additional point being that, you know, just the fact that the bounce occurred at all, does that - is there a right of visibility by third parties, you know, to that event? And I guess my question is, I'm trying to understand why there would be. You know, I'm trying to get my mind around…

Steve Metalitz: I don't think you understand my questions, James. So…

James Bladel: Then I probably don't. Steve, can you help me?

Steve Metalitz: Let me ask if I can clarify it. Leave the third party out of this. This has nothing to do with third parties. The question I'm asking is, under the Whois accuracy program specifications, if the registrar has any information suggesting that the contact information is incorrect, such as registrar receiving a bounced email notification or a non-delivery notification message in connection with compliance with ICANN's Whois data reminder policy or otherwise.

I mean, that's not the only circumstance, but that describes a circumstance in which you received a bounced email notification or non-delivery notification message.

Now, why couldn't you apply the - in that case, you have to go then validate and reverify. I mean, there're other things you have to do then. This is the trigger that you were talking about. Why wouldn't that same test - why couldn't that same test be applied in this case?

And I just want to make sure that I'm understanding that the problem is not that you don't know when this happened. The problem is that you don't want to let the requester be put in the same position he would be in the non-proxy setting of knowing that it's happened.

James Bladel: So thanks for clarifying, Steve. The - I think we're in agreement that it should trigger that reverificaiton. But I think I do agree with your latter piece here, the last piece of your comment, is that I don't understand why we - why it should be that a - when the proxy service is the listed contact in the public Whois database, that if the contact to that public Whois contact is successful, that any subsequent contacts - and there could be more than one, not just to that customer but that customer could be a law firm or a Web host or something else that's operating on behalf of yet another fourth party or something like that.

And I'm saying that the chain of visibility to that contact's success or failure, to my mind, ends once the contact is established successfully with the public Whois contact. And that any subsequent contact after that are private communications.

Steve Metalitz: Well, James, this explains to me why your policy states that you can - that the customer can opt out of receiving any relay whatsoever. And I thought we decided last week that that was not an appropriate standard and should not be allowed under our accreditation process.

But you're basically saying there's no obligations really. Once I've sent it to the address that's given by the proxy service, that's it. That's all I'm entitled to. Isn't that what you're saying?

James Bladel: Well, I'm saying that we're open to the idea that some parties are privileged such as ICANN and the registrar and perhaps law enforcement. And that's what we're discussing as part of this accreditation program.

Steve Metalitz: But nobody else is entitled to have anything relayed, correct?

James Bladel: Well, I think we're going to shake that out, Steve, but we're - my position is no. But there may be others. We may uncover other types of contacts or communications, you know, as we go forward, but off the cuff, it seems that - to me, those three and perhaps the registry, would also be included.

Steve Metalitz: And so no one else is in…

((Crosstalk))

Don Blumenthal: I think James made the point. I jumped (Kathy) and I'd really like to get back to her. (Kathy).

(Kathy): Hi, can you hear me, Don? Hello everybody.

Don Blumenthal: Yes.

(Kathy): Okay, so my question is not related - is not directly related to what James and Steve were just talking about, so if you wanted to continue that, please do.

Don Blumenthal: No, I just wanted to isolate that one question but we went into (some other) areas. Thanks.

(Kathy): Sure. Okay, well, I wanted to take actually one kind of giant step back per some of the stuff I was putting in the chat room. I can definitely see why a requester would want to know if the email went through or if the message to the customer went through - to the proxy and privacy customer.

But I wanted to go back to the feasibility. How feasible is it to transmit all bounced back messages back when we're dealing with automated systems? And I know we talked about it a little bit last time and I apologize for the background noise her, as the saw's go on - my next door neighbor.

But how feasible is it if we're dealing - we can envision that once this relay system is in place, it's going to be used a lot. And so a lot of messages going through, how easy is it to sort the bounced back messages in automated systems and get back to every requester when something bounces for all the different reasons that we've been talking about?

Just on a feasibility side, how easy is that? And then we can go into the details. Similarly, if a courier package is forwarded on and bounces, you know, it doesn't go through. What about that? Or a fax message and they're out of paper on the other side? It seems like an awful lot of stuff to track and I'm not even sure it's possible. So, again, key question - what's the initial feasibility? Thanks.

Don Blumenthal: Well, I think Volker had wanted to jump in on the last conversation, so I can go to Volker and also ask if you, as a registrar, if you've got a thought on (Kathy)'s question.

Volker Greimann: I would have to think about that. It's a bit complicated and I was thinking about the previous discussion so I didn't catch it all. Sorry for that. With regard to - I would like to just go to two points. One is the entitlement questions and I can see James' position. I can - I support that insofar that privacy provider at this point can choose what to forward to its customers and what not to.

I think the question of what needs to be relayed is something that we are supposed to be discussing as part of this group. I'm not sure that we should be talking about an entitlement here, rather, the question of what is appropriate?

For our service, it's always been appropriate to forward email and nothing but email automatically if directed to the address in the Whois and some of those that are sent to our emails as well.

But that's the way we choose to operate our service. That's not because we think that one party or the other has an entitlement. The second point I wanted to go into was the question of bounces and currently the way the RAA is structured is we do not have to do anything if a bounce happens.

We have do to something if we become aware that some information in the Whois is incorrect. For example, if there's a bounce there we can directly associate with an email address, so if we get a bounced message that tells us this email that we sent to this email address was wrong, was undeliverable, then we have to do something.

If we receive a bounce that says there was a bounce. Not sure which email that was. Nothing else there. Then we don't have to do anything. And that's the distinction I wanted to point out.

Don Blumenthal: Okay, thanks. Interesting (scoop) there. James?

James Bladel: Hi, thanks. James speaking. Just (Kathy)'s statement reminded me of something I think I read - actually I think I read it from (Kathy) on the list, either yesterday or perhaps a couple of days ago.

The question about feasibility reminded me that she had asked a question about could a service, a proxy service, for example, offer to block, let's say, solicitations for the purchase of a domain name but relay, you know, other types of communication?

And it got me thinking a little bit that the real challenge here might be to relay or not relay and make that decision based on content rather than on the sender. And I was thinking about how difficult it would be just from an operational perspective to build a system that could make the determination what the content or intent of a communication was on an automated high volume basis.

And thinking a little bit about how that would - could prompt, you know, like an arms race or a spammer and other unwanted communication, trying to get around those filters that were making that determination.

So it seems like the approach, at least from an implementation side, might be to, you know, identify senders or, you know, or other types of key words because I'm not sure that that can be built to be abuse-proof.

Anyway, it was just something - I don't know if that directly answers your questions, (Kathy). It probably answers a different related question, so sorry about that.

Don Blumenthal: Thanks James. I think to some extent we'll probably get into that type of discussion. We'll move on to - I need to. Alex?

Alex Deacon: Yes, hi, it's Alex Deacon. Yes, so I just wanted to comment on the question that (Kathy) posed regarding how difficult it is to do. I mean, you know, SMTP is a protocol that's been around for a long time. I think it's - people understand how it works, you know, just to mention a thread that's on the chat.

It's not perfect but, you know, emails that are sent, you know, through orders and proxies and on, you know, perhaps two or three layers deep, as long as these headers are properly maintained and mapped, then I think the response on the way back should be quite easy to track. And there're ways to do that.

There's, you know, there's the to/from headers. There's reply to headers, you know, proxies in the middle or mail forward is in the middle – can put, you know, X dash headers, you know, their personal if you will headers to – with global user IDs or global IDs to track requests and response.

So I, you know, this – I don't think that's difficult to do. You know, I've done that in a past life and it happens every day today and has for many years with SMTP.

So I just wanted to, you know, to raise the point that this isn't difficult. Sure there's so much cases that you have to deal with but I don't think it's too challenging.

It's definitely possible to do and, you know, the fact that it's hard or perhaps a pain in the neck shouldn't be a reason to not do this.

Don Blumenthal: Okay Michele and then I think we could go on because there are nuances particularly to this kind of auto floating type concept that could take us for a long time.

We can take it back to the list. We'll do Michele and then I want to move on to the next subquestions if you want.

Michele Neylon: Michele for the record. I'm not sure if I want to be done but okay, thank you. Now just in relation to communication methods, as somebody else – and fax was mentioned a couple of times, and I think somebody else pointed out that the fax contact isn't an obligatory field so I think it's best to ignore it.

With respect to this entire email thing it's – we could end up in quite a circular conversation around this. My main concern is around whatever language ends up in a policy or a contract because I'd be – I'm very wary of how it ends up being phrased because if you make it a binding obligation on Registrars or privacy/proxy providers to do certain things, that's very different to – than making best efforts, et cetera because if we fail to relay a single message for some technical reason, then we're in breach of the contract and that would not be very pleasant.

The other thing is in relation to feasibility of doing things. I mean, at the moment we are currently exploring a service that we want to offer some of our clients, which would involve forwarding mail from one country to another.

And the problem we've run into is working out how you can actually price those in the same fashion because none of the companies that operate in that space will give you kind of blanket pricing.

They won't even give us X number of items relayed per – sent per month in the pricing. So actually scoping out the cost becomes a major challenge - just something to bear in mind. Thanks.

Don Blumenthal: I appreciate it. I'm going to – back to actually something I said a minute ago. I hadn't realized so I relooked at Number 3 on the subquestions how much we really have been covering all three.

So I'd like to continue the thread but I want to remind folks of the discussion concerning relaying of snail mail. I'm not sure there was agreement on whether it should be done or what kind of costs to be passed along to the submitter.

And getting back a little bit to something James mentioned that I said was going to come in E2, I think it might be appropriate to get also in the context of snail mail and what obligations are there to forward snail mail?

How much in the way of costs can be passed along and not passed along? Another issue is the extent to which snail mail is going to present a separate set of issues with – for that and being able to do screening/backup of message if they needed to see in an email what the subject is, and whether it's really something which should be forwarded if we take that approach as opposed to the sending approach.

But I'm not sure that's possible at least under U.S. law anyway in the case of regular mail. So then let's keep this going but I'd also like to spend a little bit of time focusing on paper mail, because again I don't think there was agreement last week when I actually prepared this. Alex?

Alex Deacon): Sorry. That's an old hand.

Don Blumenthal: Okay.

Volker Greimann: Yes regarding paper mail/paper communications I might be very controversial by saying that anything that is communicated by paper can also be communicated as an attachment to an email and paper would require the provider to get up from his desk, go to the scanning machine, insert the USB, scan the damn thing in, hundreds of pages, whatever, go back to his desk, enter the, you know, enter this into his - USB into his computer and then send out an email to the Registrants.

I don't think that's practical. Anything - especially if you can just request somewhere in your terms and conditions that any communications be sent by email.

I think postal communications in most cases as most providers do go directly to the trashcan and rightly so.

David Hughes: Right. This is David Hughes. I'd like to speak next if I could.

Don Blumenthal: Sure. Yes go ahead David.

David Hughes: Okay. This…

Don Blumenthal: David you're breaking up pretty severely.

David Hughes: Okay. Can you guys hear me now?

Don Blumenthal: I'm sorry. The only – okay now yes and when you asked if you could speak - nothing in between.

David Hughes: Okay. If you can't hear me I'm sorry but it's about the establishment of this physical location. It's not about sending hundreds of pages. A one-page letter with a link, "Please go to this Web site and click," or something would be enough.

But in law enforcement and IT enforcement our last line of, you know, our last recourse is usually try to establish the physical location. And if the emails and electronic communication did not work and if you can't establish a physical, then I have to question the purpose of WHOIS at least for certain purposes including law enforcement.

Don Blumenthal: Okay.

David Hughes: Can you guys hear me?

Don Blumenthal: Yes.

David Hughes: Yes. Okay.

Don Blumenthal: Well let me just clarify. Are you suggesting that paper mail, I mean, what we're talking about here is say forwarding a paper mail that came in to the – actually privacy service.

Are you suggesting that the service would send something else in via paper that could generate as opposed to just forwarding the message itself?

David Hughes: Well if there's no response to any electronic communication from the end client, then there's no chain to the, you know, I don't understand the purpose WHOIS if you can't get to the end of the chain, if you can't get to the user.

I'm not sure you guys would call it a user in the case of a client/customer in the case of the privacy/proxy. Alex maybe you can articulate my concern better if you share it.

Alex Deacon: Yes this is Alex. I'm having a hard time following myself David. I apologize.

David Hughes: Okay. Okay maybe I'll write something up and share it with the – that I'm thinking of because really that's a better use of our time than talking about it on the phone.

Don Blumenthal: Okay thanks. Steve?

Steve Metalitz: Yes, Steve Metalitz here. I just want to say I think the issue on – that we've been talking about on snail mail or hard copy if you will is really just the situation that David is talking about.

We're not talking about a situation where there's been an attempt to relay an email and for example it's bounced or it's been undeliverable. In that case Volker's argument that anything you could send by hard copy you could also send attached to the email is not relevant because we've tried to send it by email and that email doesn't work.

In that circumstance the question is whether there would then be an obligation to forward it to the mailing address that the provider has been given.

So it's – I think it's a much narrower circumstance than saying anything that comes in via snail mail has to be forwarded, although I noted last month, or excuse me, last week on the call that a number of providers already say they do that.

But leaving that aside I – I'd like to focus on the narrow case where there's been an attempt to send via email. The email has been undeliverable and should in that case there be a requirement to forward snail mail or hard copy of the requester asks for that. Thank you.

David Hughes: Thank you Steve. It's David.

Don Blumenthal: David?

David Hughes: I just wanted to thank Steve for clarifying my position. Yes I think this is a – this is when every other, you know, when all electronic communication has failed and we have no recourse but to resort to physical hard copy mail.

Don Blumenthal: Okay I appreciate it. That is much clearer. Chris?

Chris Pelling: Afternoon all. Chris Pelling for the transcript. As I mentioned last week and unfortunately kind of bluntly probably last week - and Don wasn't on the call so I'll come at it again probably the same way unfortunately because I have no longer any standing.

In some senses I don't think we have any argument with LEA as in law enforcement, you know, the – in our jurisdiction sends us as an example a letter that needs to be forwarded on and it's from law enforcement.

I think a lot of points are made that as Volker was saying if it's general snail mail it would probably go in the bin unless it's something that's really important, i.e., law enforcement.

Now as an example and I mentioned this last week if we receive a request to send something to a Registrant be it from, I don't know, whoever, we will ask and put forward that there is a charge of $30 to forward that on and that is paid for by the requester, i.e., the person sending the document and it has to come via FedEx or it has to come via UPS.

It won't be accepted via snail mail. The reasoning, you know, for that is is because this takes time guys. You know, we're going to spend as Volker was mentioning not five or ten minutes doing this.

By the time you receive the mail, open it, take it to a scanner, play with the scanner, get it onto a stick or send it directly to their stop, whatever you want to do with it, and then relay that document you are talking a man-hour.

Now in the UK we charge our man-hours as 100 pounds an hour. You've got to consider that if we are taking time to do this and there is a time involvement, there is obviously a charge.

LEA, you know, in some sense is the – want to forward information. Or I think it was David -- I could be wrong. I do apologize -- who was saying that if he wanted a letter – a one-pager to go out that's slightly different I think because obviously we're acting on LEA stuff and now again it's from my jurisdiction. That's all I wanted to point out. Thank you.

David Hughes: I might add just an idea -- this is David -- that a corresponding electronic proxy may be required.

Don Blumenthal: David you're not – you're breaking up pretty badly again.

David Hughes: I will try one more time. I'm so sorry. I'm just in a bad place and I – I'm – what I'm saying is that there could be – we could discuss a requirement that a parallel electronic communication has to go to the privacy/proxy.

So if they get a FedEx they would have an electronic copy in their inbox as well that they could then forward and would not require them, you know, but in the end if something is going to have to go to a physical location I don't know a way around it.

I mean, we could send the scan by email and with a request that says, "Please send this physically," if that – if, you know, and we would be willing to discuss paying a fee for this.

This is not something that happens frequently. I mean, we're really talking about, you know, we've got to the point now in many cases where we're thinking about litigating and that's going to cost us tens or hundreds of thousands of dollars.

I don't think in these serious IP infringement scenarios that paying a fee of, you know, whatever it is is out of the question. I think that this is very infrequent but it is, you know, without this recourse we sort of hit a dead end.

Don Blumenthal: Okay, appreciate it.

David Hughes: Okay?

Don Blumenthal: Volker?

Volker Greimann: Yes, two points. First of all I would just like to reiterate that failure to – of the Registrant to respond to an email or a communication does not equal undeliverable message or – and a inability to communicate with the Registrant.

If he chooses not to respond that's his prerogative. To Steve's point I agree that if the message bounces then there's a problem. This is why most privacy/proxy services - and I would propose this also as a standard for best actor or behavior before the project is accredited is to have a separate abuse contact somewhere on their Web site in a prominent place that says, "If you cannot communicate with the Registrant because of email address bounces, or you think that we should be involved directly because we don't see what you sent to the Registrant directly, then contact us at this abuse at whatever email address and that way you can communicate with us and ask us any kinds of questions."

I think that's – that would solve that problem. And the last point, the address of the privacy/proxy service, is rather irrelevant so checking that I – I'm not sure if I understood David's point correctly.

Checking the email address of the privacy/proxy service by sending an – sending something – sending the physical address of the privacy source or just sending physical mail is irrelevant once those proxy – privacy/proxy providers are accredited because then that would already be checked by ICANN upon their accreditation.

So asking – sending them postal mail and asking to forward is – does not fulfill any purpose other than making work for us and that's why we refuse to do it.

Don Blumenthal: Thanks. James? I'm sorry. Appreciate it. James?

James Bladel: Thanks. Sorry. I couldn't get the mute button to go off. I'm thinking – and going back I think to a couple of comments ago - and I think that the conversation may have passed up my question here a little bit.

But there was a comment I believe from David regarding establishing – using WHOIS and maybe I misunderstood but using WHOIS to establish the physical location of the Registrant.

And I think that the thing that popped into my head there was that that is precisely why some of these services are engaged is so that law enforcement - and I'm thinking particularly here of areas where, you know, the content of the Web site may be politically or religiously, you know, persecuted or something like that.

I mean, establishing the location would, you know, essentially undermine the value of the service. You know, we certainly wouldn't want to hand over the physical location of a, you know, of one of our customers only to, you know, have them get their door kicked in by some group because of something they said on their Web site.

So, you know, I think that – but I think that Volker or perhaps it was Chris – yes it was Chris that it should be for the appropriate jurisdiction that's applicable to the proxy service.

Now to me that makes a lot more sense and I think that if we're going to establish that then I think I'm okay with that particular concern. The operational, you know, one of the things that happens a lot on these calls is that I think we take too narrow of a view and we really sometimes in ICANN circles don't appreciate the scale and the speed of the industry that we're talking about when we're dealing with perhaps, you know, hundreds of thousands of domain names being looked up or created or altered every hour.

And then we translate this into communication attempts. So when we deal with anything that's going to involve physical mail that's going to significantly slow down the process.

It's going to step out of an automated channel from many respects and as I think Volker pointed out step into a – one that is very labor intensive. So I think that there should, you know, if we're going to go down the path of requirement then we should definitely – that must be accompanied by the ability for the Registrar – or I'm sorry, the privacy/proxy service or perhaps the Registrar to recoup those costs from the sender, because that is going to be a significant issue particularly if it's on the service's dime and it's something that could be abused by spammers or even, you know, competing services.

So just a couple of potpourri of thoughts there and - collected during the long conversation and I apologize if some of those topics have already passed me by and moved down the road. Thank you.

Don Blumenthal: Okay and wish we had more than five minutes left. I've got a few follow up questions. There's no time. I'll send an email. Michele?

Michele Neylon: Yes thanks Don. Michele again for the record. Agreeing with both James and Volker on this. I mean, the key thing here, I mean, this thing about physically sending something to somebody, I mean, ultimately you're – if you want to send a complaint about a – the user of a proxy or privacy service you will have the proxy and privacy service's full contact details.

So if you want to send a registered letter or whatever to the proxy/privacy service you'll be able to do so. But you're not going to be able to do that to the user of the service – well not directly because as others have said, I mean, the entire point of having a proxy/privacy service is not to divulge the end user licensee, whatever you want to call them to divulge their contact details.

Now for us as an Irish company, you know, you get me a court order from an Irish court or if you're Irish law enforcement and you send me in a properly formatted request then we can have a conversation about that.

But if you don't fall into either one – if you don't have a court order from an Irish court or you're not Irish law enforcement then, you know, you're going to have to communicate with us. Thanks.

Don Blumenthal: Thanks Michele.

David Hughes: This is David. I have a very quick comment. Maybe this will help.

Don Blumenthal: David I…

David Hughes: I don't know.

Don Blumenthal: We've got – David we've got two more people on the queue so why don't we get to them?

David Hughes: Okay. Go ahead. Go ahead.

Don Blumenthal: Steve?

Steve Metalitz: Yes I want to actually take James up on his invitation to step back a little bit here. And I would just encourage – remember we're talking about relay here and we're going to talk about - later about reveal.

Relay is one method of making reveal unnecessary. Not in every case but in some cases if you're able to contact the party that's engaging in abuse you may not need to then go through the reveal process.

You may be able to solve the problem. If – the more that I hear the Registrars on this call weakening the whole issue of reveal and making it more difficult to have an effective, excuse me, of relay and have – making it more difficult to have an effective relay.

And, you know, and then again these are the cases where we try to relay but the relay – the address you the provider have doesn't work. That's mostly what we're talking about here.

But the more that you restrict relay or, you know, say there's no obligation to relay, which again I'm really kind of surprised to hear on this call, then you're going to increase pressure for reveal.

I mean, I think it's just pretty obvious that relay is a less invasive if you will approach to this problem. So I would just encourage people as you think about these issues over the week to come and hopefully we'll have further discussion on the list, please think about this in that context that if you – if we don't have an effective relay procedure then it increases pressure to have an effective reveal procedure and to make it more available in more circumstances. Thank you.

Don Blumenthal: Appreciate it. Volker?

Volker Greimann: Thank you Steve. Like I said I'm not opposed to relay. I think relay is important. For my – for our privacy service we have always relayed certain communication while there's what goes to the bin as I have explained before.

It's just to – I think we need to agree on what level of relay is appropriate and at what – how that should be structured. That's I think the discussion that we should having – should be having, not relay in general.

Second point, for the law enforcement I think it makes sense to differentiate between law enforcement and – that are applicable. For example we see law enforcement requests from all different kinds of jurisdictions.

And while we are only bound by certain ones, for example the ones that – where our privacy/proxy service is located or the ones that – where we are located or where we are doing business with an – physical office, those we treat as our own.

And there's others that we receive and then we treat as a general abuse complaint because they are not our jurisdiction, but we still look at what they are saying because it might still be relevant to our laws.

And I would suggest that that be borne in mind when discussing this topic as well.

Don Blumenthal: Thanks. We're technically past – we're one minute past 11:00. David can you make your suggestion or throw in your comment here or would it be better on the list? I don't know what you think.

David Hughes: Sorry. I think Steve clarified what I wanted to say which is the differentiation between relay/reveal. And I think we got a note back that said, "We have relayed your physical hard copy," and they confirmed receipt.

That's the end of the chain of relay and reveal. Let's have it discarded. We're not asking you, "Please tell us the address of an – person." We're saying, "Please confirm that you got our correspondence," and I think that's a big difference.

Don Blumenthal: Okay appreciate that. I think people are kind of circling back towards each other as the call wraps up. Thanks very much for all of your involvement on the phone and in chat.

It's really productive hour and two minutes and I look forward to seeing everybody next week.

Man: Thanks Don.

Man: Thanks Don.

David Hughes: Thank you.

Chris Pelling: Thank you Don.

Volker Greimann: Thank you Don.

Don Blumenthal: And everybody else as well Chris.

Sheri Falco: (Jill) if you can please stop the recording.

END