

**ICANN Transcription
Privacy and Proxy Services Accreditation Issues PDP WG
Tuesday 05 August 2014 at 1400 UTC**

Note: The following is the output of transcribing from an audio recording of Privacy and Proxy Services Accreditation Issues PDP WG call on the Tuesday 05 August 2014 at 14:00 UTC. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.

The audio is also available at:
<http://audio.icann.org/gnso/gnso-ppsai-20140805en.mp3>

On page:
<http://gnso.icann.org/calendar/#aug>

Terri Agnew: Good morning, good afternoon and good evening. This is the PPSAI Working Group call on the 5th of August, 2014.

On the call today we have Tatyana Khramtsova, Michele Neylon, Steve Metalitz, Holly Raiche, Val Sherman, Chris Pelling, Todd Williams, David Heasley, Graeme Bunton, Sarah Wyld, Dan Burke, Griffin Barnett, Libby Baney, Luc Seufer, Darcy Southwell, Justin Macy, Don Blumenthal, Christian Dawson, Kathy Kleiman, Susan Kawaguchi and Jim Bikoff.

We have apologies from Alex Deacon, Carlton Samuels, Stephanie Perrin, Roy Balleste and Paul McGrady. From staff we have Mary Wong, Marika Konings, Amy Bivins and myself, Terri Agnew.

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, Don.

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
Todd Williams – IPC
Michele Neylon – RrSG
Tatiana Khramtsova – RrSG
Frank Michlick – Individual
Luc Seufer- RrSG
Volker Greimann-RrSG
Don Blumenthal – RySG
Osvaldo Novoa – ISPCP
Libby Baney-BC
David Hughes-IPC
Holly Raiche – ALAC
Kristina Rosette – IPC
David Heasley-IPC
Dan Burke-Individual
Christian Dawson-ISPCP
Jim Bikoff-IPC
Sean McInerney-SOI

Apologies:

Stephanie Perrin – NCSG
Alex Deacon – IPC
Paul McGrady – IPC
Carlton Samuels – ALAC
Roy Balleste – NCUC

ICANN staff:

Mary Wong
Marika Konings
Amy Bivins
Terri Agnew

Don Blumenthal: Appreciate it, Terri. Fair warning, I'm going to be jumping off on mute quite often. Welcome to Michigan allergy - welcome to Michigan allergy season. And I just saw Chris's note here - are other people having problem with mic volume? Unfortunately I'm not sure how to turn it down, I think I'll have to reposition. Okay, Chris, let me know if this is better and other folks if you can't hear me. Oh okay.

At any rate, as suggested yesterday in email, I'd like to wrap up E1 today and move on to E2. We - I think - and the discussion has been good the last couple weeks, I'm not suggesting otherwise. But I think at times we've gotten wrapped up in details that might not - they're useful for education on what we should be doing or not but may distract from just moving forward with our policy recommendations as opposed to trying to come up with operational details.

So with that I'd kind of like to open up the discussion to - sorry about that, I told you I'd go on mute a lot - open up the discussion on these - kind of the overarching questions that I raised. First, the obligation to notify - the obligation of a provider to notify a requestor of a bounce message, of a clear delivery failure.

And then also try to come up with some parameters own that type of complaints or issues or requests, however we want to put it, should be forwarded and which ones shouldn't or which ones - maybe not shouldn't but does the provider have discretion on whether to forward or not.

So let me open the floor to just the affirmative notification question. Because, again, I think the E2 discussion may feed back into that second issue. Any thoughts on just in general should there be a requirement? Steve.

Steve Metalitz: Yes, this is Steve Metalitz. Just to answer that question our view is that there should be that requirement when the proxy privacy service provider knows that the relay is undeliverable. And I, you know, we've gotten into a lot of details about how they would know that and what form the notification would take but all that could be left to implementation and we would simply set up that principle that that's something that the provider would be required to do.

Don Blumenthal: Thanks. Any other thoughts? And maybe I should also toss out whether people have problems with the idea of pushing ahead of the core issue and not getting in the details. Kathy?

Kathy Kleiman: Coming off mute, can you hear me, Don? Hello everybody.

Don Blumenthal: Yeah.

Kathy Kleiman: I think the flip side is that there seems to be, in some cases, a very time consuming process involved in processing the bounce-backs. And there doesn't seem to be kind of any quick automatic way to do it. And there seems to be some issue about revealing information including IP addresses.

So the question is since we're creating baselines, not ceilings - floors, not ceilings, what's the baseline here? What would be the right amount to require given that everybody's systems seem to be set up a little differently on this? And I don't have the answer to that I'm afraid. Thanks.

Don Blumenthal: Okay. Sounds like you're reticent to just dump it on ICANN staff and walk away. Any other thoughts? Oh a bunch. Steve.

Steve Metalitz: Yeah, this is Steve. I would just contest the view that this is very complicated problem. This is a problem that providers have to deal with anyway because in that situation they're going to have to reverify the email address so they have to know - have some system for knowing when it's happening. And again, I'm not concerned with, you know, what the content of the notification so long as it lets the requestor know that is the relay attempt failed because it was undeliverable at the email address - the address that the customer provided to the provider. So I don't think it's all that complicated and I am prepared to leave the details on this to implementation. Thanks.

Don Blumenthal: Great. Todd.

Todd Williams: Yeah, Todd Williams for the transcript. I was just going to echo kind of the second half of what Steve just said which is if our concern is that the notification may reveal certain things and that we're leaking kind of into the reveal discussion I think the general principle that the submitter is notified of the bounce-back would adjust that, right?

I mean, whether the content of that notification reveals anything I think can be left to the provider. But just a simple, you know, notice of the bounce-back shouldn't necessarily get into that. Thanks.

Don Blumenthal: Okay. Appreciate that. Graeme.

Graeme Bunton: Thanks. This is Graeme Bunton for the transcript. It sounds to me like everybody is sort of on board that if we go down the route that the requestor is entitled to a notification that their message is not deliverable then what they are returned is a message that merely states that their message was undeliverable and probably nothing more. So it's not a return of a bounce, it's just simply that statement.

That said, I'm still not sure I'm convinced that the way this process works entitles a requestor to know if that bounce happened. In my mind, and I think this is what James was elaborating on previously and kind of where we're stuck at is that, you know, the requestor when they said that message is not communicating with the registrant, they're communicating with the privacy and proxy service.

If that piece of the message bounces then that's an issue for compliance. You know, it's then up to the privacy and proxy service provider to communicate with the registrant and that's our own communications with the registrant. If that communication does fail we need to kick off a, you know, a verification procedure.

But I guess I still remain somewhat unconvinced that that, you know, our communications with our registrant or, you know, name holder that a requestor has any right to that information. Thanks.

Don Blumenthal: I appreciate that. Never mind. Darcy. Darcy, you on mute? Yeah, Darcy can you - oh there I see you typing. Yes. Oh I was starting to think that we'll - okay, great. I'll look for your hand up. It sounds to me as if we've got - oh, Steve.

Steve Metalitz: Yeah, I just wanted to respond to Graeme. I mean, I don't know where you get the idea that we're trying to communicate with the provider. We're not; we're trying to communicate to your customer. You're running the business which - in which you have a responsibility to provide a channel for these matters to be relayed, that's the reason why we're trying to come up with what the standards are.

And if that doesn't work, if you're unable to do that, I think we're entitled to know that so that we can take other means to try to solve the problem. So, I'm just mystified by the idea that somehow we're trying to communicate with the provider. We're not.

Don Blumenthal: Susan.

Susan Kawaguchi: Hi. I just want to sort of add on to what Steve just said. You know, I do - we do enforcement all the time against domain name registrations that are infringing. And I think our first line, you know, our first step is to actually try to get a hold of that registrant and say do you understand that you've registered a domain name with Facebook and this could possibly be an infringing use?

And you, you know, should think about this now instead of a year down the road or even two months down the road once they've invested some time and money into the site. And, you know, there's a lot of people that unfortunately

do not get, you know, any sort of advice before they try to launch a business. If they chose a different domain name we'd have no problem with the content.

But so - and close to - somewhere between 25% to 1/3 of all those registrations are proxy registrations so it seems to me that the proxy company would prefer to have me go straight to their, you know, their client, customer, and iron all of that out without utilizing the services of the proxy company.

So I just do not understand why relaying the message and therefore getting some information about if that message went through or not wouldn't be important to the proxy company too? Do you want to deal with all of the - all of the communications that go back and forth and just, you know, sort of educating that new registrant and getting someone to comply, you know, with - or to not infringe upon a trademark.

I just don't understand why a proxy wouldn't be - is any different than a regular domain name registration in that you should be able to contact whomever is in control of that domain. And, you know, I'm not talking response; I'm not obligating a response. I'm just saying we should be able to know that that email address would relay whatever communication we send. It makes no sense.

Don Blumenthal: Okay. Michele.

Michele Neylon: Thanks, don. Michele for the transcript thingy. So we've been talking a lot about this for the last couple of weeks and my poor little head is beginning to hurt. At this juncture we're talking about what exactly? Are we talking about somebody using an email address that appears in public Whois and send something - sending something to that?

Or are we talking about somebody interacting with the provider via some kind of online form or whatever to submit something which they hope will get

through to a licensee or submitting a complaint? Because this is where I'm getting a little bit confused about the - it's all to do with handling of the bounces and everything else that seems to be causing me a certain degree of kind of headache and everything else. I'm not 100% sure exactly what we're talking about so if somebody could please clarify that for me it would help. Thanks.

Don Blumenthal: Well when I teed the question up my view is that since we're talking about privacy proxy we are talking about the obligation of a provider to notify a requestor that there's been a delivery failure.

Michele Neylon: Yeah but - but hold on. This is where the headache is coming from, Don. Because there's a difference - okay if for example - how do I phrase this? Because you're talking about the obligation of the privacy proxy provider to do something then it suggests that the privacy proxy provider is more involved in that process than might be the case.

Because to my mind if you're talking about what the proxy privacy provider is meant to be informing X and informing Y and informing Zed in relation to the others then that sounds like something which is very interactive between whoever wants to interact with the domain - the user of the domain name rather than somebody simply sending an email.

I see Steve's got his hand up, maybe he can clarify this for me. Thanks.

Don Blumenthal: Okay. I was but I'll defer to Steve. I hadn't seen his hand.

Steve Metalitz: No, no Don, go ahead.

Don Blumenthal: I guess now I'm confused by Michele's confusion. To me it's - what we're talking about is fairly - is much more straightforward. The provider gets a request. The provider forwards the relay - the request to relay. The provider

forwards the relay. The relay message bounces. What's the obligation of the provider to notify the requestor that there's been a bounce?

To me it's that straightforward. There's nothing involving - or whether there should be - there's nothing involving any direct communications between the requestor and the beneficial registrant.

Michele Neylon: Yeah, but, Don, why would - how would I, as a provider, know that there's been a bounce? You know, if the communication is directly - if the communication is directly between - I'll pick on Steve because he's big enough to take it.

So let's say Steve wants to contact you and you've got a domain name registered via - I'll pick on Tucows, they're big enough as well - via Tucows but using some kind of privacy service. So he's not going to Tucows, he's going to - he's doing a Whois lookup and he's getting an email address from Whois. He's sending an email to them. Now if there's a bounce who's getting the bounce message?

Why would I, as the provider, in this scenario, be even aware of the bounce? Because I'm not the one who sent the email so why would I get the bounce?

((Crosstalk))

Michele Neylon: That's not how email works? Sorry?

Don Blumenthal: Yes it is. You're the one - yes it is. You're the one who was forwarding a relay request...

Michele Neylon: No, I'm not forwarding the relay request.

Don Blumenthal: You were - wait, you're the provider...

((Crosstalk))

Michele Neylon: No but this is the thing. If you're sending an email to an email address then technically speaking...

((Crosstalk))

Michele Neylon: ...technically speaking all that is happening is that email is flowing through my system somewhere else.

Don Blumenthal: No.

Michele Neylon: Yes.

Don Blumenthal: No.

Michele Neylon: Yes.

Don Blumenthal: Okay, let me finish the statement before jumping in please and after this I'll defer to Steve.

Michele Neylon: Okay.

((Crosstalk))

Don Blumenthal: I'm the requestor. I send you an email saying please relay this to...

Michele Neylon: No, you don't. You send an email to the email in Whois.

((Crosstalk))

Michele Neylon: You're not coming near me.

Don Blumenthal: If you're a proxy provider it's your email that's in Whois.

Michele Neylon: It's an email which is in Whois. It might not be my email. But you're not going near me; you're sending an email to an email address.

Don Blumenthal: No, all I can say - all right, let me maybe - okay every proxy registration I've seen has an email affiliated with the proxy provider. Maybe my experience is too limited. Steve.

Steve Metalitz: Yeah, this is Steve. So, Michele, maybe this will help but if not just take two aspirin and hopefully that will relieve your headache. I'm looking at the E1 template and I see that different providers are doing this in different ways.

1&1 Internet says, "Messages received at the email address posted in the public Whois database for your private domain name will be forwarded to the email address associated with your account name or to another email address in accordance with the preferences you set."

So that's a situation in which it says, "Will be forwarded to the email address," that means will be forwarded by the provider to the email address. Now if that were to bounce back - if that were to be undeliverable, the provider would know but the requestor, the one who originally generated the message, would not know. That's the scenario that we are talking about.

Now the same thing is true with Domains By Proxy. "When you purchase a private domain name registration, DBP creates a private email address for that domain names at domainsbyproxy.com. Thereafter when messages are sent to that private email address DBP handles them according to the email preferences."

So, you know, again it goes on about forwarding. And we're going to talk in a few minutes about what the requirement is to forward. Now there are other services that generate a random email address that the requestor can use.

And in those cases the requestor would know if it had bounced back because they would send it to random at the domain name service. You know, this is something that changes every few days or whatever.

Then they would know. So what we're talking about here wouldn't come into play. But many of these services don't work the way. Whois privacy service, affiliated with above.com. "Messages received at the email address posted in the public Whois database will be forwarded to the domain contact email address provided in your account. This forwarding is not filtered in any way."

So again, that's a situation where the provider knows, the requestor doesn't know. All we're saying is that when that occurs the requestor should be advised. Thank you.

Don Blumenthal: Darcy, you're back on? Hopefully on?

Darcy Southwell: I think I am this time.

Don Blumenthal: Okay.

Darcy Southwell: Darcy Southwell. I guess kind of back to what Kathy said in the very beginning and also sort of a ground set I guess we're talking about minimum standards.

And there seems to be an assumption that the bounce - that's - it's a permanent bounce and it's like, okay, let's say that we do get a bounce-back, I would argue that the privacy proxy providers have an obligation to investigate and treat that sort of, you know, treat that failure as a reason to try to get correct information for their end user, for the registrant and get it corrected as opposed to simply notifying the requestor.

It seems like it's almost a TOS violation by the end user not to give the provider the right information so that things can be forwarded as they're supposed to be. Thanks.

Don Blumenthal: You're absolutely correct. And we - that has come up before. I think right now we're just focusing on the obligation to notify at all because there's been some disagreement on that. The obligation of the provider to try to remedy the issue is still going to be there.

And, you know, part of this is, okay, when - this may be too much into the operation of details - when should the notice of the bounce go? Should it go immediately if there is one? Should it wait until there are attempts to remedy? But to me that's kind of in - will fall in someplace different from the basic question here. That helpful?

Darcy Southwell: Yes, thanks.

Don Blumenthal: Okay. I'm looking at the chat and I think we really should move on to E2. We've got the basic (unintelligible) of agreement or disagreement. I will note that I don't think we can require anything any more than, you know, if there's no underlying issue I think here has been that bounces that the provider is aware of would have to be forwarded if anything; I don't see where it's practical to require notifications of bounce if the provider never knows about it. Mary?

Mary Wong: Hi, Don. And hi everybody. Thanks. Maybe your last sentence just clarified what I was going to ask, excuse me, which was the second question you wanted to discuss today, whether the - not talk about notification but just the initial forwarding, whether it's to forward all requests, some requests or at the discretion of the provider.

And the preliminary conclusion that we've compiled so far, you know, it's worded somewhat differently. So even if there's no time on this call to discuss

that it would be helpful for working group members to indicate, you know, where their support lies for the forward part of the relay request.

Don Blumenthal: Yeah. Yeah, that will be next. I do want to touch that. Obviously we're not going to make 1030 to cover those topics. Kathy.

Kathy Kleiman: Thanks, Don. I don't want to keep us from moving forward but I think I was going to highlight the same point Mary just mentioned that we don't yet have agreement, I don't think, I don't think we have convergence on what exactly should be relayed. I think there is agreement that certain types of abuse cases, and we have some good language on that, should be relayed but not necessarily agreement that every request should be relayed.

And I'm wondering what kind of implication that has for the question we were just asking which is bounce-backs and notification if something goes through. If we forward everything does it make it much harder to handle? And maybe this is something we deal with under Question 2?

Does it make it much harder to track the responses versus if we kind of narrowed down what must be relayed and then require a little more effort on those? So I just thought I'd throw the question out there because I'm thinking about it. Thanks.

Don Blumenthal: Steve.

Steve Metalitz: Yeah, this is Steve. I think Kathy's comment is a good segue to the next question.

Don Blumenthal: Yeah.

Steve Metalitz: I think there - which is, you know, what's the scope of the obligation to relay? So I think there are really two ways to approach this that we've heard over the past couple of weeks. One is what she's - what Kathy referred to as an

abuse case approach where you have a list of types of complaints or types of messages that have to be relayed. That's one approach so it's kind of additive is Case 1 and Case 2 and Case 3 and so forth.

The other is more - is more general and it says you should relay everything but you use commercially reasonable means to filter out spam and this type of thing - use of communications.

It's - I think they might arrive at about the same place but, in other words, saying there's a general rule you forward everything but you can have commercially reasonable measures to filter out...

((Crosstalk))

Steve Metalitz: ...as opposed to saying here's a list of things you have to forward. The difference it seems to me is that in the approach Kathy is advocating it's required that each provider look at each message and decide whether it falls in one of those categories or not. Is it a message about abuse Type 1 or abuse Type 2 or abuse Type 3 or is it not?

The other approach actually reflects a level of trust in the providers to say we know that some providers use filters. Not all do.

I just read one that didn't and I (unintelligible) under current practices, but as long as those filters are commercially reasonable and they are directed to meeting (unintelligible) not just weeding out complaints of abuse, then we are comfortable with them doing that. They don't have to look at every single one. They can use some type of automated method to decide what is not (forward). I think those are the two different approaches. They could end up at about the same place.

I think one of them puts a lot more burden on this provider, that's Kathy's approach, and the other gives a lot more flexibility to the provider and that's the one we are recommending.

Don Blumenthal: Thanks. I notice that James is not on the call. He was one of the - may have been one of the first to suggest that not everything should be - not every relay request should be forwarded. So specifically what - we will continue the discussion, but with that in mind to see if we can (tease) that argument out a bit as to why there should be a limit or conversely statements on why there really shouldn't be and this is getting us wrapped up in getting us or potentially a provider wrapped in too much detail. Holly.

Holly Raiche: You know I surmise where I think we are but I don't think I need aspirin for it. I think we are. If the privacy proxy that is between the requestor and the beneficial registrant, actually, the message goes through their systems and is forwarded and then it would be the privacy proxy provider that gets the bounce and that is what should be told to the requestor. If it doesn't go through, if the message does not go through a privacy proxy but goes through another address that is provided and the privacy proxy provider has - is not where the bounce back message goes, then we are saying well then they do not pass on that message.

So it boils down to what somebody said earlier I think and that is what is passed on is what the registrar or sorry this privacy proxy service actually provides and that's all that is passed on. And if they don't, if they are not in receipt of it, then they obviously can't pass it on. Now is that what we have agreement on?

Don Blumenthal: I think I said something similar to it in trying to wrap up. (Unintelligible).

((Crosstalk))

Holly Raiche: (unintelligible).

Don Blumenthal: Pardon. Yeah, I would agree with that statement.

Holly Raiche: Good, thank you.

(David Hughes): Steve, it is (David Hughes) and I have a question.

Don Blumenthal: Yeah go ahead. It is Don.

(David Hughes): Can you hear me?

Don Blumenthal: Yes.

(David Hughes): Okay, so the question I had was if there is a minimum going back to what kinds of messages need to be relayed. If there was a standard that said any abuse related messages have to be forwarded, then it would still be the privacy proxies - at their discretion. They could take the policy like the one that Steve) just read that said we forward everything or perhaps for an additional fee to the end beneficiary, they filter everything other than abuse messages. Wouldn't that be at their discretion then?

Don Blumenthal: Well, it would be at their discretion depending on what the guidelines the group comes up with.

(David Hughes): Right, so I am saying that the specifics of the guidelines aside, if the guidelines were something along the lines of if it is abuse related, you must forward it. If not, it is at your discretion. Then if filtering out everything that is not abuse related is too onerous, they can take the position that the other company took, which is we will forward everything.

Don Blumenthal: Right, I guess the issue before us now is whether we want to provide the latitude to limit what is forwarded or just say that things other than abuse also should go through. Steve?

(David Hughes): Well is anybody making that argument that anything other than abuse should be mandatory relayed? Anybody on this call taking that position?

Don Blumenthal: Yes.

Steve Metalitz: Yes, this is Steve. I think we've in fact agreed to that with regard to the transfer issues.

(David Hughes): Okay.

Steve Metalitz: There is notifications that have to go to...

(David Hughes): Okay, so my term of abuse - and I was trying to use shorthand, but abuse and (unintelligible) and registration. I mean there would be a list of things that would only make sense to forward and then we had the discussion previously about how many requests for transferring and so on. And I get that that's a detail to be dealt with later, I guess, but I suppose I mean non-spam messages if we can agree on what that is.

Don Blumenthal: Right and that's a part I think of discussion. How feasible is it going to be for any provider? Feasible, time consuming, or whatever to make the distinctions and you know that's obviously an internal question. But still, how much should we even want to provide to the discussion or should everything be forwarded to the proxy privacy provider (receives).

(David Hughes): Okay.

Don Blumenthal: Steve do you...?

Steve Metalitz: Yeah, this is Steve. I think (David)'s comment kind of illustrates what the divergence is. If we could generate a list of things, that they have - that the provider has to forward. If it would have abuse, it would have transfer, it

would have some of the other things we've talked about, we could go that way as long as all of those abuse cases are in there.

The question that I would like to hear the providers speak to is whether they would prefer to do that and therefore have to as I would understand it have to categorize everything that comes in or whether they would prefer to have a default that is forwarded but is subject to you know commercially reasonable anti-spam and anti-abuse measures. As long as those don't capture the abuse cases, then perhaps that is easier, but I guess I would defer to the - I would like to hear what the providers have to say about that.

Don Blumenthal: And again, (James) is not on the call. Graeme and Michele. I guess the question is is there any reason not to say that everything should be - if there is a request for relay then is there a reason to say that some should not be relayed. Kathy?

Kathy Kleiman: Yeah, I don't see how that meets the minimum baseline requirements. I guess I am confused because as I've been saying in the chat, we've spent such a long time talking about abuse and I thought it was -- and maybe I'm wrong -- a part of this category, Category E, Question 1. And so, I guess I thought we were coming up with that definition of abuse because those - we were creating categories of messages that must be forwarded.

Of course if its simpler and easier to create - you know to forward everything subject to you know certain filters, great, but what is the minimum baseline and I thought we spent a lot of time talking about categories of what must be forwarded and why they must be forwarded and why - you know what the relay means. And I guess I don't quite understand why we would be kind of jettisoning all of that right now rather than keeping it as an option. You can do A or B. You can forward more selectively or you and forward more broadly, but make your policies known, publish this, get it out there.

But if you have - and I don't want to speak for (James), but my sense is - and I could be wrong. Somebody correct me if I am wrong. If I've chosen the option in domains by proxy that says, I am not interested in domain name solicitations. I don't want sales. You know if somebody wants to buy my domain name, I am not interested in that email, can't I do that provided I get the abuse notices, provided I get the RAA required type notices. Aren't there things I can opt out of because I am not interested in them? Just a thought. Thanks.

Don Blumenthal: Well that's a good point. We wouldn't want to be infringing on opt out choices that proxy or privacy providers might be offered. Susan?

Susan Kawaguchi: So specifically to Kathy's question, you know currently I mean I have a domain site proxy account and currently you can select nothing is forwarded, filter for spam, or forward everything. So I - you know I am not sure. Is there a provider out there that would actually say I'm not going to send anything that looks like a solicitation to buy a domain name?

I am not going to send anything where people are complaining about the domain, the Web site's content. I am not going to send you know - if you go down the line, I don't even know how they would do that, but I am not that person that has to worry about that. But you know at least the domains by proxy is kind of not an option right now, so I am not sure why we would want to put that in as an option and a requirement for the proxies to have to consider providing.

Don Blumenthal: I'm sorry, I didn't quite follow. What isn't an option?

Susan Kawaguchi: An option to you know depending on the content or the subject of the message, to forward it or not. I mean it is either nothing is forwarded, it is filter for spam, or you receive everything including spam. Those are GoDaddy's options. I am looking at my account right now. So you know to Kathy's point that she doesn't want to receive any emails that are asking about selling the

domain name, I don't know if I have not done a survey all of the proxy services, but I would doubt that sort of granularity is available right now.

Don Blumenthal: Okay, I appreciate the clarification. Michele?

Michele Neylon: Just responding to Susan. Good afternoon Susan or good morning. I think the thing here is if somebody in the future wanted to offer that service and maybe somebody does offer it already, I don't actually know, we shouldn't end up with a policy that would preclude them from doing that. I mean ultimately, from your perspective, you want to make sure that your, you know, genuine abuse complaint type things get through. If a service provider blocks solicitations or other types of I don't know annoying emails. Well, you know, no harm no foul really. So I think it is just to allow the flexibility more than anything else if I've understood what we are talking about. Thanks.

Don Blumenthal: Okay, Chris.

Chris Chaplow: Yeah, Chris for the record or the transcript, sorry. Yes, going on what should or what should not be relayed, it is not for us to decide what should or shouldn't. It is up to the person who is receiving those emails or wants those emails because that's not (unintelligible). Now what we did and what I mentioned in the chat session there, is we don't block anything, we forward everything on, but for the person who is sending the mail to the person that needs to receive it, the registrant contact (billing) or technical or whatever it might be, you have to go through two more hoops. It is not just a simple case of fire off an email and I hope it gets there.

As an example, with our system - and not everyone does this, granted, but it is something to think about. Not all mail systems are the same, no email systems are (unintelligible). You can argue the (unintelligible) you know until you are blue in the face, but every email system out there should be the same, why not. You can't go until you get a reply.

Now other things preclude receiving emails. For instance, spam filters and everything else, and you can never guarantee getting through those spam filters because they are not controlled by the person sending or potentially sometimes the person who is receiving those emails. As for us in the privacy protection service, you would send an email to a blank contact at domain read and reply with a set of instructions, so it has to be read by a human being. If you wish to try and do it automatically, it can't be done, and that will stop a lot of the problems out there by people receiving spam because spam bots would just (unintelligible) a load of emails and hope for the best.

In some senses, it is not for us I the working group to decide who should receive and who should not receive the information we send. The working group decides how in our sense of doing this what should get through in a sense of abuse complaints for an example. I am not saying we should only allow abuse complaints. Because at the end of the day, that would be too tiresome on the privacy protection service.

At the very outset, the guys that want to send out for instance (unintelligible). (unintelligible) the MCA notices, et cetera, do want it to get through and that would normally be a person with a very long document than being an email to a particular party, and that obviously is the one document that needs to get through and that's just about it. Just a point really that mail servers are all different. You can't guarantee to get a bounce or response, but what we need to provide is the facility to get the mail through.

Don Blumenthal: Let me just jump in quickly. I thought somebody else had a hand up. I think we understand that and that's why we've talked about some kind of obligation only if the provider is (unintelligible) bounced, but I want to raise something that you focused on and kind of is implicit in what Susan just said.

It is sounding like there are providers out there who give the option of nothing, that nothing is forwarded. You know under our charter, and again what has been discussed and was going to be discussed very - in detail in E2

under our charter. Do we need language that says you don't have that option? We must relay abuse complaints.

Chris Chaplow: Again, I think that is down to the receiver of the email and the privacy protection service. An argument that was made before was with regards to should the sender be notified that the emails either got through or bounced. Well...

((Crosstalk))

Don Blumenthal: Chris, I'm not talking about bounced messages here. I am talking about the obligations to forward the relay and what conditions do we have to establish where there is no choice. The messages must be forwarded.

Chris Chaplow: Then surely that would be a modification to the RAA and nothing to do with the working group, because you are enforcing this. I mean it has to be done in Whols.

Don Blumenthal: I'm going to open this up. I don't agree with that statement that now that somebody else has a hand up. Susan.

Susan Kawaguchi: Yeah, I don't understand how a domain registration could not receive email. I think that you know maybe not specifically violates RAA, but violates the spirit of the RAA at the least. You know I'm not sure this was addressed in the RAA, but if you are a domain registrant, you have a responsibility to have a working admin email address. You know you can't - if you do not, you cannot renew it, you cannot you know transfer it, you can't do a lot of mechanics with the domain name registration and you have a responsibility to consumers out there to receive emails.

So I don't know why we would ever agree to do it and I've never understood why proxy services have gotten away with this. That the ultimate registrant, the licensee, or whatever you want to call them, the client of the proxy service

provider can receive no communications. And I would assume in that case that the proxy provider is not reading those either, so you know I mean to me that is just sort of the line in the sand. There has to be a certain amount of emails received by that licensee. I mean absolutely could not agree with allowing what is going on now and no emails being forwarded at all. Now how we get to the point of what is forwarded, you know, (unintelligible).

Don Blumenthal: And I agree and I think that is the question we have to focus on here. What bounces are a part of this. There haven't been requirements before and GNSO has now told us we need to come up with requirements.

Susan Kawaguchi: Right.

Don Blumenthal: And I think we have to operate on that basis. Michele?

Michele Neylon: Hi, thanks Don. See now, Susan, this is where you and I will disagree to a certain point. If I am not trading or doing any commerce or doing anything that generates any real revenue from some service or Web site, or whatever hanging off a domain name, then I am not really under any obligation to publicly publish in Whols an email address for me as a registrant. And if you look up Michele.cat, do a Whols look up; you won't find my email address. It is not there because the .cat Whols is compliant with Spanish and European data privacy.

Now does that mean that if I was doing something untoward with the domain name that nobody would be able to reach me, no of course not because there are other methods of doing that? Also as well of course, the registrar is contactable. Now in the case of proxy privacy, the thing is the proxy privacy provider is going to be reachable and the registrar is going to be reachable in cases of serious abuse.

So I think this is kind of a - there is a difference here, but I think Susan and I have discussed this for many months, so I think she is well aware of my difference of opinion in all of this. Thanks.

Susan Kawaguchi: If I could just jump in there and respond. But if we limit this discussion to gTLDs, what ICANN does control, then I do think there is a responsibility for the RAA.

Michele Neylon: I would have to look up the Whols for (unintelligible), Susan. Have a look at the Whols for (unintelligible).

Don Blumenthal: I would really like to stay on focus. We are not talking about - you know and I know what I am doing wrong. I think we have a very focused discussion here. It doesn't have to do with direct communications or anything else. The issue before us is, does this working group set up mandatory requirements for forwarding, and if so, what are they?

Steve Metalitz: Don, I think you have some hands up in - the screen there.

Woman: Yeah, you've got three people.

Steve Metalitz: Don are you with us?

Woman: Is Don there?

Steve Metalitz: Well maybe can we just go ahead. (Volker) do you want to...

Woman: Yeah, (Volker) go ahead.

Steve Metalitz: (Volker) are you there? I think something has happened to the audio.

Woman: Yeah.

Man: I can hear you fine.

Man: I can hear you fine.

Woman: Me, too.

Man: Okay, if (Volker) can't talk, whoever is next in the line just go ahead then?

Kathy Kleiman: Okay, that's me. It's Kathy. And (Volker) - whenever you come back in let me know and we will jump to you.

So I agree with what Steve said in the commentary that at one point in this discussion we did agree that kind of the option of opting out completely from email is probably not something we are going to support. We will support some type of mandatory minimum requirements.

As you know, I always thought that that followed pretty closely from where the questions are, so mandatory legal requirements about allegations of illegal activity, and I thought that by consensus we had expanded that to include RAA type notices like renewals and other kinds of concerns. Obviously updating email addresses, verification and validation type emails.

So I thought that's where we were and I thought what we are talking about here is going above and beyond that, so just adding my two cents. Thanks.

Woman: Steve, you are next and (Volker) says he can wait.

Man: (Volker) can wait.

Steve Metalitz: All right, I will go ahead. I am here just answering Don's question which is what should be a policy. We put forward a proposal about ten days ago. I am glad to recirculate it. It is basically the relay everything but subject to commercially reasonable filtering. I am happy to consider an additive

approach. If someone can provide a list of the types of complaints that they feel should be forwarded again as a mandatory matter, we are glad to take a look at that.

And obviously, some providers on this call have said they would prefer that approach. Others we haven't heard from, so maybe they wouldn't, but let's get the two options out on the table and try to figure out which is the best way to go. As I said, they may end up practically speaking in approximately the same place, but let's get them both out there and then let's try to decide. Thank you.

Woman: Well given that we don't have Don and we've got less than a minute, maybe we can do it all by email.

Steve Metalitz: Yeah, well we may have to. (Volker) did you want to have the last word?

Woman: (Unintelligible).

Steve Metalitz: I guess he can't. All right, well, we are approaching the top of the hour here.

Woman: Yeah, we are at the top of the hour so it is...

Steve Metalitz: Okay, well.

Mary Wong: Steve.

Steve Metalitz: Yeah Mary did you...?

Mary Wong: I was going to follow up on your suggestion and what you and Holly are saying, but since we are one minute off and it seems like we are not getting agreement on this, that maybe we could take it to the list. And what staff can do is try and summarize the gist of where things seem to be today and see if we can get some discussion and possibly agreement with the hope that for

next week we can fully focus on anything else to do with E2. Would that work?

Woman: That's fine.

Steve Metalitz: Let's try and do that.

Mary Wong: Okay.

Steve Metalitz: Thanks everyone.

Woman: Thanks everyone.

Woman: Thank you everybody.

Man: Thank you very much. Have a good afternoon.

Man: Thank you.

Woman: Thanks all. Bye-bye.

Man: Thanks all.

Coordinator: Thank you. Once again, that does conclude the conference for today. Please disconnect all remaining lines at this time and thank you very much for joining. (Andres) if you can stop the recordings.

END