ICANN Transcription
Privacy and Proxy Services Accreditation Issues PDP WG
Tuesday 12 August 2014 at 1500 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 12 August 2014 at 15:00 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-20140812-en.mp3

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

Attendees:
Steve Metalitz - IPC
Sarah Wyld - RrSG
Chris Pelling – RrSG
Darcy Southwell - RrSG
Graeme Bunton – RrSG
Val Sherman – IPC
Griffin Barnett – IPC
Susan Kawaguchi – BC
Tatiana Khramtsova – RrSG
Frank Michlick – Individual
Luc Seufer- RrSG
Volker Greimann-RrSG
Don Blumenthal – RySG
Libby Baney-BC
Holly Raiche – ALAC
David Heasley-IPC
Jim Bikoff-IPC
Stephanie Perrin – NCSG
Paul McGrady – IPC
Carlton Samuels – ALAC
Osvaldo Novoa – ISPCP
Keith Kupferschmid- IPC
Phil Marano - IPC
James Bladel - RrSG
Amr Elsadr - NCUC
Susan Prosser - RrSG
Christian Dawson-ISPCP

Apologies:
Alex Deacon – IPC
Kristina Rosette – IPC
Lindsay Hamilton-Reid – RrSG
Michele Neylon – RrSG

ICANN staff:
Mary Wong
Marika Konings
Amy Bivins
Danielle Andela
Terri Agnew

Terri Agnew: Good morning, good afternoon, good evening. This is the PPSAI Working Group call on the 12th of August, 2014. On the call today we have Holly Raiche, Griffin Barnett, Val Sherman, Keith Kupferschmid, Chris Pelling, Tatiana Khramtsova, Steve Metalitz, Don Blumenthal, Graeme Bunton, Volker Greimann, Carlton Samuels, Sarah Wyld, Darcy Southwell, Libby Baney, Phil Marano, Phil McGrady - pardon me, Paul McGrady, James Bladel, David Heasley...

James Bladel: Thank you.

Terri Agnew: ...and Osvaldo Novoa. We have apologies from Alex Deacon and Kristina Rosette. From staff we have Mary Wong, Amy Bivins and myself, Terri Agnew. I would also - oh and I apologize, also joining Danielle Andela.

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.

Don Blumenthal: Appreciate it, Terri. Did somebody go on mute? Okay, I think that's better. Here we go. Well welcome - is anybody else getting this echo that I'm getting?

Terri Agnew: Yes, this is Terri...

((Crosstalk))

Terri Agnew: ...from staff, we're going to try to isolate that.

Don Blumenthal: Okay. Appreciate it. Anyway, welcome to this morning's call. I'll do what I frequently forget to do which is remind people to please update your SOIs if there's been any changes.

Before we really get into the substance of our discussions today just kind of a brief apology, I guess, is the right word, I was a little on edge last week. A lot of things going on on the personal side and I think I just let it get to me a little too much. If nothing else, you may be disappointed, as Michele shows up, I promise we won't get into any yes, no mature back and forths like happened last week. I look back on that one and really couldn't believe it had happened.

In any event, I want to just insert one brief thing on our agenda here. We're coming up on deadline for submitting names for the funding for the face to face meeting so if you haven't done that please let Mary and Marika (unintelligible) should be on the list - know who is going to be coming from your group and how many nights they'll need. As a reminder - as a reminder there's I think six nights will be handled per group.

So, yeah, I think that deadline is Friday, Mary?

Mary Wong: Yes, Don. If we could get the names from each stakeholder group or constituency, whichever is applicable, by this Friday that would be great because then it will allow you and constituency travel to be on the same page earlier rather than later. Thanks.

Don Blumenthal: Okay. We have discussed the possibility of if one group doesn't take all its nights reallocating to others that have been, say, more active than might be able to use the extras but that's still in discussion stage, just depending on what kind of logistics, problem it might create for us, ICANN travel and whoever else is involved. That finishes the preliminary.

We, we meaning a group that meets every Monday morning, Mary, Marika, Steve, Graeme and I, kind of talked by email and then yesterday and thought it might be - thought it'd be worthwhile to move on to E2. We still do have some issues pending from E1 particularly since they focus - some of them focus on just definitions of what might trigger actions and those definitions are part of E2 we thought going ahead would be beneficial because then we can look back.

If you haven't seen your email this morning or in the last 10 minutes, by strange coincidence, I got a copy of a terms and review policy that's used by a current proxy privacy registrar. That was very interesting and I really wish I'd had it to send out well before the call but it treed a lot of thoughts in terms of how we might approach our definitions; how things are laid out in E2.

Got to switch screens here because I can't read - can't read what's in front of me.

So as usual I'd like to just throw things open to see if people have thoughts just to get us started in terms of the issues that are raised in the two templates that Mary sent around - that Mary sent around yesterday. I'm sorry, I'm reading email that came in on this subject.

Steve.

Steve Metalitz: Yeah, this is Steve Metalitz. Just to get things started here the question asks, "Should the providers be required to forward to the customer all allegations of illegal activities they receive relating to specific domain names to the customer?" And the answer - proposed answer is yes.

I mean, the real issue here is defining this phrase, "all allegations of illegal activities," and I think that's where the indicative lists that we talked about in an earlier phase come in handy as well as the material that Don circulated by email earlier today and that, you know, appears in most of the other - in

different forms in most of the other terms of service that we've compiled or staff has compiled.

So, I mean, I think that we have a - I don't know that we need to define with excruciating detail what exactly is encompassed within all allegations of illegal activities. We certainly have many examples of it in these lists. And I guess if - the question is how exact and precise does that need to be?

And this kind of goes back to E1, if you're building an additive list of what needs to be forwarded upon request or relay then this category needs to be in there. If you're - that's the second option that's been put forward.

If you're - if you're taking the approach that everything should be forwarded subject to commercially reasonable filtering then we just need to make it clear the commercially reasonable filtering doesn't capture this stuff. So I think it really could kind of go either way. But I think we have these lists and that may be sufficiently clear to move forward.

Don Blumenthal: Thanks for getting it started. James.

James Bladel: Hi, Don. James speaking for the transcript. And I've been absent for the last two weeks so hopefully I'm not too far behind on this discussion. But I wanted to say that although my immediate reaction to the question is no, I actually agree with Don. And I think that it just needs a couple of tweaks and then it will be fixed.

The language of the question would be something along the lines of, should ICANN-accredited privacy proxy service providers be required to forward allegations of - either all allegations - we would say - well founded allegations because that is the language of the RAA and that helps us, as service providers, to ensure that, you know, let's say spurious or just abusive allegations are not necessarily forwarded.

And then the second bit would be unless otherwise directed as part of an investigation. There have been certainly a number of occasions where law enforcement or other organizations do not want to alert the registrant or the customer that they are the subject of an investigation. And, you know, and that may actually part of a court order or other legal action on a registrar or service provider in case to not reveal that that is ongoing.

So I would say in this case we certainly don't want to put a registrar or a service provider in a position where the court is telling them don't, you know, don't alert this registrant that they're the subject of an investigation but then the (unintelligible) policy requires them to do so. So I think with those two fixes, you know, we're probably good to go on this requirement.

Don Blumenthal: Appreciate it. How - just a question though. How does an organization determine well-founded?

James Bladel: Well, that is an excellent question and it certainly doesn't lend itself to an immediate answer. I think that the key is to ensure, first and foremost, that the jurisdiction matches to some extent.

But secondly I think to ensure that what the - what is being alleged as illegal activity is in fact illegal according to the legal counsel of the service provider and where they exist or where they believe their customer exists or the jurisdiction that governs their registration agreement or whatever. You know, I really don't have a quick answer. But certainly we cannot forward every allegation simply on face value. That is, I think, can lead itself to abuse fairly quickly.

Don Blumenthal: Okay. Steve.

Steve Metalitz: Yeah, this is Steve. James, could you specify what the abuse is that you're concerned about? I mean, certainly...

((Crosstalk))

James Bladel: For example, Steve, you know, recently we received something from another country where they did not like a Website that was using their language and was advertising or blogging about firearms. They said firearms are not legal in our country and we want you to take the site down and give us, you know, give us some information on who's operating this site and...

Steve Metalitz: Well that's obviously - James, that's not what we're talking about here because that's not a relay request. That's a reveal request and a takedown request. Service providers can't take down because they're not registrars.

((Crosstalk))

James Bladel: Okay well that...

Steve Metalitz: This is relay. So could you tell me what you think would be the abuse if you forward all allegations of illegal activities as a matter of relay?

James Bladel: Take that same request, Steve, and convert it to a relay request or - then if that suits you. I'm giving you an example of a not well founded or a poorly founded allegation of illegal activity.

Steve Metalitz: So what's the harm?

James Bladel: The harm in forwarding?

Steve Metalitz: Yeah.

James Bladel: Well I think, you know...

Steve Metalitz: Customer receives a poorly founded allegation, is that - how harmful is that?

James Bladel: Well the harm is that you're being contacted, you're receiving unsolicited communication which is the whole point of enlisting this service.

Steve Metalitz: Okay that - I'll be interested in people's reactions as to how serious that...

((Crosstalk))

Don Blumenthal: Yeah, Volker's got his hand up here.

Volker Greimann: Well I can see quite a lot of situations, for example, if the messages that we're being asked to forward is phrased in a very intimidating way there may be legal activity that's not - or activity that might be illegal but it's not obviously illegal so we wouldn't be able to determine that. And by forwarding such messages we would then put a domain owner in a situation where he might feel threatened or intimidated by the receipt of that message.

And he explicitly uses this service to, for example, have his free speech right uninterrupted and don't - and he doesn't have the - in Germany you say the scissors in your hand so to speak. So you are influenced. But in what you're writing you don't have censorship but you're self-censoring yourself.

So that may be a factor that could be considered abusive wording on messages that are abusive in themselves.

Don Blumenthal: Steve, is that an old hand?

Steve Metalitz: That was an old.

Don Blumenthal: Apparently it was. Okay. Thanks.

Steve Metalitz: But I'll be glad to raise a new hand if...

((Crosstalk))

Don Blumenthal: Well, okay, I was about to jump in but go for it.

Steve Metalitz: Yeah, so, Volker, are you also willing, as James is, to take on the obligation of determining whether an allegation is well founded? And if so what recourse is there or should there be if you - on your decision?

Volker Greimann: Well...

((Crosstalk))

Steve Metalitz: ...activity by one of your customers how should I be able to challenge your determination that my complaint of illegal activities is not well founded?

Volker Greimann: Well, I (unintelligible) these under German law so I look at the complaint and see if - what the complaint is about is obviously illegal. If I feel that the complaint is not abusive, is not threatening, for example, in an undue manner, of course there may be threatening words in a due manner, so I am able to analyze the message itself and decide under its merits whether I forward or not.

Don Blumenthal: Thanks. I'm wracking up my own questions here but I'll defer. Susan.

Susan Kawaguchi: I'm just really curious to know that every time I send out an email to a proxy service there's going to be a live person reviewing that email for the content, the subject matter and making a legal decision on whether or not I'm overstepping my trademark rights or overstepping and providing a chilling effect to the registrant.

So if you do not want to relay things so are the proxy service providers going to actually review every email that comes into the email address on record for that domain name registration?

Don Blumenthal: Well, James is next up or Volker can respond to the question.

James Bladel: This is James. I'll go ahead and respond. Yes, Susan, if it is a request to reveal or a request to relay that's coming from let's say someone with whom we have an established, you know, history of, you know, processing those reports I think that, you know, human intervention is almost always called for in those cases. I don't think you can automate that. Certainly you can't automate the checks and the tests and the analysis that Volker was discussing.

I think I wanted to just kind of touch back on something Steve said which is how do we challenge the, you know, if a registrar or an affiliated service providers says, you know, we don't believe this is a well-founded request, how does the requestor then escalate that and essentially say, you know, you're wrong in this case and we do want you to reveal or relay the information.

And I think that that case - in that case we would specifically point out that we always respond to court orders to subpoenas or any other sort of formal due process that would require us to reveal communications or to reveal - relay communications or reveal the customer information.

I think what we're talking about here is what would our obligations be short of a legal process, which would be in an ICANN policy, or even just a cooperative best practice. And I think that's where service providers will say that we need to have discretion in those - in those situations.

But I was just trying to come back and make sure that Steve is aware that, you know, I don't think we're saying that they should have no obligation to relay those communications, it's just what are the thresholds or the tests that need to be passed first before we can require that to happen.

Don Blumenthal: Thanks. Volker and then I'm going to jump in with a couple of issues. Susan's question at least, took one off the table.

Volker Greimann: Thanks, Don. Volker Greimann speaking. Just to respond to Susan's question, it kind of depends on how the service is set up and what the service is designed to do.

In our service there's two options, your rights to the abuse contact and then someone will look at it and someone will make a determination on the complaint or you write it to the automatic forwarding and then it will be scanned if it's spam and filtered and so there's some filtering happening there as well.

But you also have service providers that are mass market. You have service providers that are only catering for a very small customer base, for example, lawyers that are engaged to provide privacy services for their customers for whatever reason they're doing that.

So you have to look at the big picture here that there's different kinds of privacy services engaged for different purposes. And each of these may be set up differently. Some of them will only have manual forwarding; some of them will only have automated forwarding. Some of them - the big market ones will probably have a version of both. But it really depends on how the system is set up and how are the services set up.

Susan Kawaguchi: Can I respond to that, Don?

Don Blumenthal: Sure.

Susan Kawaguchi: So - but since we're designing what the requirements will be going forward, then I think what I hear you and James advocating for is no relay and only relay if you've decided that it is - if the proxy service provider has

reviewed each and every email and decided that it fits the criteria, you know, for relay. Is that what you're advocating for?

Volker Greimann: Not necessarily. I think we need to find the minimum standard of notifying someone of a problem with a domain name that's on privacy services. How that is dealt with, how that minimum standard looks like that's something that we should determine here. But I would be very cautious in advocating any business model that would exclude a competitor from continuing to provide their business.

Susan Kawaguchi: Thank you.

Don Blumenthal: Okay, and again, as each piece discussed here and my questions are kind of disappearing. I'll reformulate - and go to Steve again.

Steve Metalitz: Yeah, this is Steve. Don, I'm happy to have you go first if you want but otherwise I can...

Don Blumenthal: Oh no...

((Crosstalk))

Don Blumenthal: No, I've got to kind of, like you said, things are getting answered that I had planned to ask so I'm going to...

Steve Metalitz: Okay. Okay.

((Crosstalk))

Steve Metalitz: ...because I don't think I'm getting any answers and I hear from James and from Volker that there should be a standard but I'm not clear what it is. And James, I still don't understand what my recourse is other than getting - going to court and getting a subpoena.

If you refuse to forward an email, again we're not talking about a take down here, if you refuse to forward an email in which I claim that one of your customers using your service is violating my intellectual property rights or committing - impeached in operating botnets, phishing, piracy, fraudulent or deceptive practices, anything on this list what's my recourse?

And of course you know, James, I'm sure that in the US the court is going to say if I seek a subpoena, have you asked the service provider first? I'm just not clear what my recourse is in your view.

James Bladel: Don, you want me to...

Don Blumenthal: I was going to say since you are next on the list go for it.

James Bladel: Well this is kind of a response to Steve and Susan. You know, I think - I don't know that we're talking about the same thing. You know, I'm not saying that we should have no obligations to relay those communications are reveal.

I'm saying that's when we are establishing the obligations, you know, we can have reasonable discussions on this group and certainly I think, you know, those of us who have worked with - those of you who worked with privacy services that unaffiliated with know that we have some very, you know, we are very responsive in this regard.

But we are kind of taking a hard line here, unfortunately because we have to because we know how compliant - we can anticipate how compliant (unintelligible) on us. And essentially what they're going to do is they're going to hold our contract against us or pit us any gap between our contact and our contract with ICANN and our legal obligation.

And so what we're trying to say here is that if we're going to put anything in place, at least - and I don't want to speak for Volker - but what we're trying to

say is - what I'm trying to say is we're going to put some obligations in place - contractual obligations, they have to mirrored within the RAA to some extent and also mirror what - they can't necessarily be over and above what our obligations are legally because then, I mean, I believe that puts registrars and other service providers in the difficult position of, you know, of either respecting the rights of their customers or following their ICANN contract.

And I think it's too - unfortunately, you know, our experience with the 2013 RAA is that we don't have a lot of wiggle room here and when we are faced with these issues with compliance.

So my thinking here is a let's find ways that we can develop, you know, very clear escalation paths that we have terms that mirror the RAA like well-founded. So far to my understanding, that has not created those, you know, the types of issues that Steve was raising where people are just stonewalling requesters - legitimate requests, at least I'm not aware of that happening. And that's in, you know, a similar situation where is abusive to let someone know that they are the subject of an investigation?

I don't know. But I know that it does. And, you know, this is a - this is something that we certainly don't want to put ourselves in position where we're between a rock and a hard place between the cops and between ICANN. And I'm concerned that the path we're going down with some of this.

Don Blumenthal: Appreciate it. Paul and then I will use my prerogative.

Paul McGrady: Thank you. My question relates to the end-user and what their recourse is if the privacy proxy service gets it wrong on relay. Maybe these privacy proxy services all have an (unintelligible) legal staff that can make multijurisdictional analysis and decide that, you know, this or that claim is baseless under all the possible applicable jurisdictions.

But my concern is that what we're talking about is a decision not to forward a legal notice of a - regarding potential criminal activity or potential rights violations, things of that nature. And the customer might the better their position legally if it turns out to be a real problem that the privacy law proxy service didn't spot if that end-user is able to act sooner rather than later.

So how do we - but other protections for the customer when their privacy proxy service gets it wrong if they refuse to relay the message. Thanks.

Don Blumenthal: Appreciate it. And by legal notice you are suggesting something short of court order, right?

Paul McGrady: Correct. There's all kinds of notice letters and other communications that are short of, you know, complaints in court.

Don Blumenthal: Okay. Just clarifying. I just want to raise two things. First, to what extent should we be - and other hand there - to what extent should we be really drawing comparisons between what a registrar is required to do and what a proxy service provider is required to do? How analogous are they in terms of what the outcomes of their communications going to be?

To be honest I'm concerned, a little bit of what I'm hearing is suggesting what compliance may or may not be doing, I mean, the context it might really not apply with privacy proxy.

The second thing I want to point out is, is we are talking here about baseline requirements. So I just want to remind that a proxy privacy provider could be very expansive should we require them to be expansive or is, say, the minimalist approach - (unintelligible) suggested acceptable as the baseline with freedom for providers to go way beyond that.

And I hope my question on the first part was clear enough. Let me know if it wasn't because I'm not quite sure. Stephanie.

Stephanie Perrin: Yes, thanks. Stephanie Perrin. I was just going to insert another rock in this rock and a hard place scenario. I'm wondering if folks that are subject to spam legislation have a view on whether a requirement to relay track that is not well founded, let's just use that word, would be a violation of the spam legislation?

We have brand new spam legislation in Canada and it seems to me that this could become a way of subverting that legislation because the privacy proxy service provider has a prior relationship with the client the folks that are sending the mail do not. So just a question.

Don Blumenthal: Yes - hassle. Canadian law. I see your point. I think, you know, just toss this out because I don't think we want to get into deep discussions of the can't stand and (unintelligible) laws there are. I think there would be an easy workaround in terms of contracts, you know, requiring provisions whereby a proxy privacy user would agree to accept relay messages. So we can do the quick and dirty lawyering (unintelligible).

Steve.

Steve Metalitz: Yeah, this is Steve Metalitz. I want to respond to - Don, what I think your question was, if I understood it, and that is how this relates to the RAA standards. And I think that it's quite different because, again, let's remember all we're talking about here is a relay. The RAA is a basis, you know, that's the registrar who can take away the registration. Here we're talking about relay.

The provider - it's true, I mean, if you look at the (unintelligible) by proxy terms of service it goes on for a couple pages about the basis on which it can take away the proxy service in its sole discretion without any liability to you whatsoever because it has absolute right and power.

Again, I don't see much of a rock or hard place from the service provider's perspective with that language. And it's all of these different basis on which they can even cancel the service. We're not even talking about that; we're talking here about relay. So, again, I'm not sure that I see what the - you know, it'd be great if we - if every service provider had a set of platonic guardians who would weigh the validity of every relay request that was received and determine by some absolute standard whether it was right or not.

But in our world I think we have to look at what would be the harm that would be inflicted on the customer if a - notice were relayed that subsequently turned out not to be well founded. And it just doesn't seem to me that that harm is that great and it - at the same time neither James nor Volker has really come up with what - they agree there should be some standard but I'm not sure - still not clear on what they think the standard should be for the obligation to relay.

So again I think we should just keep the consequences in mind here. The consequences here are very different than under the RAA because here we're just talking about receiving a message. Thanks.

Don Blumenthal: Yeah, I think you did understand the question. I appreciate building some context around it to clarify. Holly.

Holly Raiche: Just a comment in reply to Stephanie. I don't think it's a problem not relaying spam. I think if you do relay spam - and certainly we've got anti-spam legislation as well. The party that's liable is never the ISP, never the person in the middle, it's always the person who actually provides it in the first place.

But I don't think there's - I just don't think it's a worry. I think if people get very good spam filters everybody's happy all the way around except for the person trying to send it. Thanks.

Don Blumenthal: Yes but contracts are nice just to remove any doubt.

Holly Raiche: Yeah.

Don Blumenthal: Speaking as one of the resident attorneys. James.

James Bladel: Hi, Don. You kind of a put a capstone on it there is that I agree with Holly. I don't think that the - there is a real concern from the perspective of the service provider that those sorts of relay notifications will they themselves become considered to be spam. Because of the contracts, you know, we certainly have to require registrants to agree to ICANN - to abide by ICANN policies and certain that any sort of terms of service of a privacy proxy - accredited privacy proxy terms of service agreement would have some similar language requiring them to agree to accept those types of emails.

And also I don't believe or anticipate that this would be happening in bulk. I think it would probably be a targeted exercise specific to a case by case basis for each domain name.

Going back to Steve, I think that - I think that we're actually closer on this than it sounds although I'm sort of taking a hard line just as a thought experiment on this particular issue.

Because I think that we do agree that we do agree that there should be some standards or some test. I think that where service providers are now today, and, you know, citing the example of Domains by Proxy, is that we have a lot of leeway to make those determinations on our own.

And I think that the two choices that face this working group is do we take that discretion away from service providers and essentially, you know, give them very prescriptive procedures and definition on what they have to do in any given scenario or do we, on the other side, do we sort of maintain that discretion with the understanding that the good actors in this space will

always, you know, take responsible actions here and that the bad actors will become, you know, will stick out like a sort thumb and then we'll have some contractual basis to take action against them, they have to change their behavior or get out of the space.

And I think that's where I'm coming from on this is that we have a lot of discretion right now. We would hate to see that turn into a, you know, a binding of the hands type situation. Most especially because that would also require a lot of definitional work and the building and procedures into contracts and I think that would be a heavy lifting scenario too.

So I don't really think that we're - at least I'm not - and I don't want to speak for Volker - I'm not taking this hard line because I actually want to be able to disregard these types of requests. I'm thinking more along the lines of when this becomes a contractual obligation that a service provider's ability to stay in business is predicated upon then I think that we need to either be as clear as possible or we need to give that - the discretion to operate responsibly.

Don Blumenthal: Thanks. Volker and then I'm going to refocus. We've got a lot of sub questions here and I'd like to at least take a stab at them.

Volker Greimann: Thanks, Don. Volker speaking. I think James is right on the money, we're not looking for something that says you don't have to forward it all. I think we're looking for a certain amount of discretion here. For example cases where forwarding would be abused, cases where someone says I explicitly do not want any emails from person X, the cases where we filter out spam-like complaints or spam-like communications.

So what we're looking for is the discretion of the privacy proxy service provider to say, no, I will not forward this for whatever reason, that is understandable.

Not for any old reason but there should be a discretion here that certain messages or certain types of messages or certain types of senders should be excluded from the privilege of being able to use the service just as ICANN takes the privilege of saying no, you cannot use the Whois abuse - Whois inaccuracy complaint procedure in email because you abuse it, that's the same thing that we're looking for here as well.

Don Blumenthal: Okay. Thanks. I think we've gone back and forth on this quite a bit. And not seeing anybody new - Steve, I would like to move on but...

Steve Metalitz: Go ahead. Go ahead. No, I'll hold off.

Don Blumenthal: Okay. Appreciate it. I think a lot of this discussion has spiraled in and out of E1 and that's kind of what I expected. It would have been nice to have a cleaner cut.

To be honest - and I'm just throwing this out - we have what we have in terms of language but one of the issues that has been raised here is what's illegal, what's no in what jurisdiction and that's going to be a challenge. And at least from my background there are a lot of reasons you might want to identify a beneficial registrant that really don't relate to illegal activities as such.

I don't know how free we are to expand how we define where the communications should be forwarded. But I just want to plant that thought that there are reasons to want to know the holder of the domain that don't necessarily involve illegal activities for example, just trying to resolve a commercial dispute.

With that tossed out for consideration, because it's a little off the edge, I would like to go through the questions that we have here. You know, we've touched a little bit in the past about obligations to do the relay and whether they should cover paper or just email. You know, should the - excuse me. But

what we haven't gotten into - and I'm not sure we resolved that - but should the complainant be identified?

Arguably - Mary, could you bring up - I probably should have asked this before, could you just bring up the template questions, not the template questions, the questions as we posed them in our list that was sent out a long time ago.

Mary Wong: Did you mean this document, Don? Or the charter questions?

Don Blumenthal: No, the - no the group's charter questions in E2.

Mary Wong: All right, give me a couple of minutes. I'm going to need to upload that.

Don Blumenthal: Okay. Yeah, like I said I should have - sometimes looking at those kind of focuses things. It's easy to get lost in the templates. You know, there are some questions in here about - excuse me - I think may be just - may be covered by the discretionary discussion we just had. But there are a couple that aren't.

But I do want to bring this up to maybe frame some of the discussion we've already had an also identify something that - a couple things we really haven't talked about.

And one thing we - and I'll add something else we haven't talked about is part of our discussion today was, well, if something isn't forwarded what recourse does the requestor have? Well, are we going to require that the requestor be informed that something hasn't been forwarded? Kind of in that - left by the wayside in talking about this notion of not forwarding.

Steve.

Steve Metalitz: Yeah, thanks. This is Steve Metalitz. I agree with you that those - there really are a couple of questions that flow from the position that the service provider should have discretion to do - on what to forward.

By the way, that's the status quo as James pointed out. But that's - we're here to actually come up with standards that may change the status quo. Hopefully they would reflect good practices that are existing now but there is - the whole idea of having an accreditation system is a change from the status quo. So, you know, I think that's kind of part of the landscape here.

I think if there is a - again, if we follow the route that James and Volker have suggested then I think we need to, you know, what's the recourse if the service provider is going to have discretion to refuse to forward an allegation of illegal activity or abuse activity then we need to know - obviously the requestor needs to be informed of that and we need to know what recourse they would have.

So, you know, I just think it's - a though experiment is fine but at some point we need to try to come up with the standards that we think should apply in the accreditation context. And I think it would have to address those questions if we went down the route that James and Volker are advocating. Thank you.

Don Blumenthal: Thanks. Mary, could you scroll down to E2? You know, key Volker up and I just heard a crash that I've got to go investigate. I'll be back in about a minute.

Volker Greimann: Okay, Volker speaking. And I would like to respond to - I hear an echo of myself, sorry. I would like to respond to what Steve said with regard to the status quo. I disagree kind of with the - with the point he was making that we need to change the status quo. We need to look at the actual status quo and see if there's problems with that status quo.

And if there are problems with that status quo then we might look at fixing them and how to best fix them. But if most privacy proxy service providers provide the service in a way that's already - that's already in position that the status quo is fine for those privacy proxy providers and only a certain amount of bad actors need to be filtered out then we should look at what the minimum standard should be and what kind of behavior we do not want.

So I don't see that the status quo is necessarily a problem. If there is a problem then that should be analyzed and brought to the forefront.

Steve Metalitz: Is Don back? In his absence, this is Steve, let me just respond to Volker. Yeah, I agree, there's a place to look at what are the good practices that are going on today. But right now the status quo is that there is no recourse in this setting. I mean, there is no way to weed out bad actors.

If a service provider has a policy of not forwarding and if they state that, you know, if they're affiliated a 2013 RAA registrar they have to post their policies. But if their policy is we won't forward these things that is the policy - some stated policy of some service providers at least under some circumstances then there really isn't any recourse.

So even if there, you know, if we go down the route that you and James are advocating, if we want to weed out bad actors there has to be some test by which they can weeded out. So I guess we're just - we would be waiting what your proposal is on what that recourse would be and - or what that standard would be on the basis of which some entity would be labeled a bad actor for refusal to forward. Thanks.

Don Blumenthal: Okay, I'm back. It was worse than I thought. Somebody went off the road and is in my neighbor's living room. Not somebody - somebody in a car.

Steve Metalitz: Oh wow.

Don Blumenthal: But there's plenty of neighbors there so I'll - I'll refocus here. Is everybody - if folks could scroll down to E2 I guess we have automatic - I was hoping we wouldn't go back to the question kicking around.

I'm looking at this list under E2 and I think we have, at least indirectly, addressed many of the questions here. But again, a while back we discussed forwarding email or paper. Did we - what are folks' thoughts on whether we came to a resolution on that? Should paper be forwarded? Volker.

Volker Greimann: Yes, two points. One, to respond to what Steve was asking and one to your point. The first one, I'm going to say I don't think that paper should be forwarded at all provided email is forwarded. Steve has been asking about minimum standard. I think that in some form the provider must offer a way to forwarded communications.

But whether that be by email, automated, manual, that's the provider's prerogative. If a provider says everything has to be sent by notarized letters that might be going a bit too far. But if he says, I don't forward email, I just forward postal messages that would be another acceptable way of forwarding messages.

If that is abuse there has to be a certain way to disable the forwarding. For example, if somebody is known as a spammer or if the registrant explicitly says I don't want to have any communications forwarded of a certain nature that should also be a possibility of providing the service. But then the responsibility would be on the provider to tell the complainant that this is not being forwarded because of Reason X.

Don Blumenthal: Okay. James.

James Bladel: Hi, James speaking. So I kind of disagree with Volker - no, wait, I'm not sure I do. Let me just - I have a very nuanced though on this here regarding the forwarding of paper of physical communications, let's call it.

I believe they should be forwarded. However, I do not necessarily believe that that simply translates into a line in the contract that privacy proxy provider shall forward these communications - physical communications. So I think that this is a much bigger issue than just simply, you know, checking that box and making it a requirement and moving on.

For example, we should be very clear about what types of physical communications we're talking about. You know, I have seen, you know, crank mail that has numbered in - is not measured in pages but in pounds. We should not, as a working group, discount the idea that there are some very - we could say passionate or we could say unhinged people who feel very strongly about the Internet and like to talk about it either via email or printed documents.

So I think that by setting some basic standards, for example, something is delivered via registered mail or courier or something along those lines I think that is, you know, some sort of bar that must be passed in order for a - to trigger a forwarding requirement.

And then I think to allow the service provider to recover a reasonable cost associated with that from the requestor I think that if, you know, if someone sends us a FedEx and says, you know, you must forward this to Turkey, you know, and it weighs 37 pounds or whatever, you know, I feel like there should be some guidelines there that say - that allow a service provider to say, okay, then, you know, if you want us to do that it's going to be $57 and here's the bill; we're not making that up and adding a profit margin, we are entitled to recover our costs for that. And that should not be burdened on the privacy proxy customer because that could be abused as well.

So those are just my thoughts here on physical forwarding. I think that it is a good idea but there need to be some controls to ensure that we're not

opening the door to someone burying a - either a provider or their customers burying them in paper or burying them in shipping costs. Thanks.

Don Blumenthal: Thanks. That's helpful. Volker and then Mary.

Volker Greimann: Well, I think I do disagree with James a bit here. I think that paper is an option but it shouldn't be a requirement. So if a provider says, I will forward paper, then that's prerogative but it shouldn't be a requirement to forward paper.

If a provider says, I will trash any paper communications which I receive because you can use email and email will be fulfilling the same purpose then paper communications would be then that's his prerogative. He can - if he can say I got this paper communication from you, send it again per email and I will forward, that should fill the requirements. So, yes, paper should be trashable, paper should be forwardable but there shouldn't be a requirement either way.

Don Blumenthal: Okay. Thanks. So many questions, so little time. Susan.

Susan Kawaguchi: So we're talking about paper now but I don't think we've ever come to the decision on relay so if you're relying - if you're not going to forward paper and you haven't agreed that everyone should relay - the minimum basic requirement is that a proxy provider relays the email then what is our - how do we contact the registrant or the licensee?

Don Blumenthal: Are those really the same things? You know, you can't - can't we look at paper versus email in the extract without having - it's a threshold issue of being able to decide what should be forwarded based on substance?

Susan Kawaguchi: I don't think so...

((Crosstalk))

Susan Kawaguchi: I think that...

Don Blumenthal: Okay go ahead. Go ahead.

Susan Kawaguchi: I mean, I just feel like - okay we sort of tabled one topic and now we're going on to another topic. Well, you know, my viewpoint on the forwarding of paper would be - is guided by the relay of the email, you know, what we've decided on that.

And if we haven't decided that all emails will be relayed or that email addresses should be good for at least a month instead of a day or two weeks that, I mean, there's a lot of issues there and, you know, Carlton was - and others were calling out for let's write down all the issues or, you know, discuss all the issues, then how can we make a decision about paper? I'm just confused.

Don Blumenthal: Okay. All right well we're up at 11 o'clock. Very quickly we could theoretically decide that there is absolutely - that proxy providers have to forward everything that's email but nothing that's in paper. I mean, that's on the table. Mary and then we'll have to fold.

Mary Wong: Thanks, Don. Just real quickly I wanted to take a step back approach and just remind folks that wherever we go with this that this set of questions came out from the recommendations of the Whois Review Team and what they wanted was for us to look at a standardized process hopefully with standardized time frames so that the goal is to have something that's clear, consistent and enforceable and this goes to some of the comments people were making in the chat about there not being a standard practice.

So as folks got thinking about these different questions I just wanted to put in that reminder. Thanks.

Don Blumenthal: Appreciate it. We're just a little bit after 11:00. I know quite a few people on this call I expect have to jump to the Name Collisions Webinar, including me. So we'll be in touch before next Tuesday but let's close this one down. Thanks for participating.

James Bladel: Thanks, Don.

Volker Greimann: Thanks, Don.

Mary Wong: Thanks, Don and everyone.

Terri Agnew: (Andre), if you can please stop the recording.

Coordinator: Thank you very much.

END