ICANN Transcription

Privacy and Proxy Services Accreditation Issues PDP WG
Tuesday 10 November 2015 at 14:30 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 10 November 2015 at 14:30 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.

Recording: http://audio.icann.org/gnso/gnso-ppsa-10nov15-en.mp3

The audio is also available at: http://gnso.icann.org/en/group-activities/calendar#nov

Attendees:
Alex Deacon – IPC
Chris Pelling - RrSG
Darcy Southwell – RrSG
David Hughes – IPC
Frank Michlick – Individual
Graeme Bunton - RrSG
Griffin Barnett – IPC
Holly Raiche – ALAC
James Bladel - RrSG
Kathy Kleiman - NCSG
Lindsay Hamilton-Reid – RrSG
Michele Neylon – RrSG
Paul McGrady - IPC
Phil Corwin – BC
Roger Carney-RrSG
Sara Bockey - RrSG
Sarah Wyld – RrSG
Stephanie Perrin – NCSG
Steve Metalitz – IPC
Susan Kawaguchi - BC
Terri Stumme - BC
Todd Williams - IPC
Vicky Sheckler - IPC
Volker Greimann – RrSG

Apologies:
Don Blumenthal – RySG
James Gannon – NCUC
Osvaldo Novoa – ISPCP

Christian Dawson - ISPCP
Carlton Samuels - At–Large

ICANN staff:
Aysegul Tekce
Amy Bivins
Marika Konings
Mike Zupke
Mary Wong
Terri Agnew

Terri Agnew: Good morning, good afternoon and good evening. This is the PPSAI Working Group Call on Tuesday, the 10th of November, 2015. On the call today we have Graeme Bunton, Chris Pelling, James Bladel, Holly Raiche, Stephanie Perrin, Steve Metalitz, Todd Williams, Kathy Kleiman, Griffin Barnett, Sara Bockey, Darcy Southwell, Sarah Wyld, Terri Stumme, and David Hughes.

We have apologies from James Gannon, Osvaldo Novoa, Christian Dawson, Carlton Samuels, and Don Blumenthal. From staff we have Aysegul Tekce
, Marika Konings, Amy Bivins, Mary Wong, Mike Zupke and myself, Terri Agnew.

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, Graeme.

Graeme Bunton: Thank you kindly. I think there was an email from (Paul McGrady) saying he would be on the phone but not on the Adobe. If anybody else has that scenario knock politely and we'll get you inside the queue. I did notice that there was a couple of people mentioned in the roll call that I don't see in my Adobe connect and I don't know if Adobe is being weird and someone please let me know if I'm not seeing a hand. (Unintelligible).

So thank you everyone for joining us this morning that is a half an hour early. An extra welcome to Amy and Mike from ICANN staff who are going to talk to us a bit about operational concerns. Before we get there, just need to check if anybody's got updates to SLI. Hello? Good? Friendly reminder to go and check those and make sure they're all up to date.

So I think it's probably best to jump right into - it looks like we've got a presentation here from Amy to get us going. So this is going to be about some of the concerns they had as they looked at our initial report I believe but I'll let Amy introduce it. So Amy, go ahead.

Amy: Hi, this is Amy for the transcript and I'm here with Mike as well. (Mary), do I have control of these slides? I think I do, hold on just a second. Okay, yes, I do. So thanks for having us back and we want to talk to you again about some of the outstanding question that we have related to your draft final recommendations.

And there are two specific topics that we want to talk about, transfers and de-accreditation. And we've got some other questions from you guys as well that we'll talk about and anything else that you want to talk about that's not already been discussed we're available to talk about as well.

With effective transfers and de-accreditation, these are both really huge topics and we had some significant questions about these issues and how these would work under the recommendations as they're written. Currently, since we were hoping to get some more clarification from you about these topics, I know that this is moving quickly toward being complete. But we think we need some more information before this can be passed on to us to implement.

Okay, so just jumping into transfers. You guys had asked us to go through how we think transfers would work under the working group's current recommendations. And the short answer to that is that --okay, sorry - the

slides at this point on the transfer slide, I just heard from somebody that they're not synched.

Graeme Bunton: They were not from me. We might have to get them manually.

Amy: Okay. We'll just skip forward. I think it's the third slide on the first one related to transfers. Okay, so the one group asked us how we think transfers would work. Just based on how the recommendations are written today and the short answer is we've gone through the recommendations and honestly we really don't know how this would work. And so we really want to turn it back to the working group to get more information about how you see transfers working.

We think we need more clarification. And we have some questions about the current recommendations and your intent underlying them. So the recommendations currently require privacy proxy services to relay all communications required by the RAA and consistence policies. And this recommendation, the way that we read it, we read it to also include FOAs. And we have some questions about that because we don't really understand the market, who works that way right now. It seems that - I don't know where the slide went, hold on - it seems that currently the way we understand it is that privacy proxy services they're not forwarding FOAs.

Sorry (Steve) - (Steve) asked for me to define that. FOAs is the form of authorization for transfer requests. So when the transfer request comes in this - the FOA is on to the transfer contact at the - for the account for the transfer process. So the way the transfer process works is it has to be accepted and also it has to be put into the FOA and sent back in order for the transfer to work.

And so we think the recommendations would require as they're written for privacy proxy services to forward all of these on to their customers. So in effect it would require the privacy proxy service to allow any transfer that the

customer wants. And so we want to hear from you about this. I mean, is this what the working group wanted or do we have a good understanding? Anybody have any comments now? I don't see any hands. (James)?

(James): Hi, Amy, thanks. (James) speaking for the record and hope you can hear me okay. I think this is an important question and I think perhaps something that the working group needs to spend a little bit more time discussing. Because as it works today, privacy services just simply rejects transfers on behalf of their customers and puts that in their terms of service.

And the reason for that - there's a number of reasons for that - I mean, I think primarily because the underlying customer information is not posted in Whois so there's really no way to validate or verify whether or not the privacy service actually obtained the authorization second hand. And then of course when the domain name actually shows up at the new registrar, the gaining registrar's doorstep with the contact information of the privacy service of the losing registrar can create some confusion over whether or not that transfer was actually legitimate and authorized by the appropriate contacts.

So I feel like this is - I think you guys have correctly identified something that we need to spend a little more work on. Thanks.

Amy: Thank you, (James). Does anybody else have any thoughts about that? Steve?

Steve Metalitz: Yes, this is Steve Metalitz. I just have a dumb question about this. Is there a requirement in the RAA or consensus policy that FOA be forwarded to the registrar?

Amy: Sorry, Graeme, you had your hand raised?

Graeme Bunton: Yes, did you not hear Steve's question there?

Amy: Sorry, the question was is there a requirement to forward FOAs? And I believe Mike can probably answer the question for me because I don't have the exact wording. I don't know if you want to address that one now.

Mike Zupke: This is (Mike Zupke) speaking. I hope you can hear me all right. So what the transfer policy says is that in order for transfer to maintain the gaining registrar must transmit this form of authorization to the either the registrar or the administrative contact. And then either one of those must affirmatively acknowledge that FOA before the transfer can proceed. There's no mention of forwarding it because the transfer policy wasn't written with this notion that there was going to be proxies or privacy services involved.

And so what Amy has really raised for you is that, you know, what we read literally in these recommendations is that we thing the recommendations are saying we want the proxy and privacy service to forward that form of authorization to the underlying or beneficial customer that could affirmatively make that acknowledgement to the gaining registrar. I think, you know, that raises, you know, a lot of potential operational issues for the proxy service and for both registrars involved.

Since, you know, today generally the proxy who is a proxy at a registrar is known by that registrar and probably has, you know, some sort of, you know, fairly close relationship. In the future this might mean the proxy service ends up with a registrar it doesn't know or doesn't care to do business with. And so that's, you know, sort of some of the thinking underlying that questions. Hopefully that helps.

Amy: Thank you, Mike. Graeme?

Graeme Bunton: Yes, I was just going to point out it's been a while since probably north of a year since we've talked about transfers in any sort of depth within the working group. So I find it unlikely we're going to dig into this or have all of our knowledge about transfers in our head at this exact moment. It would

certainly cause us some concern at the time. And I know registrars have thought in the past a little bit about how to make privacy and transfers work but I think that it's good that we've raised this. We might have to take this back and think about how we're going to address it but it's a good question.

Kathy Kleinman: Graeme, this is Kathy. I'm not in the Adobe room. Can I ask a question?

Graeme Bunton: You may. Please go ahead, Kathy.

Kathy Kleinman: Terrific. First, and I'm sorry if I missed it, can somebody define exactly what FOA means? What would the acronym mean so that we know for the future? And from staff perspective, would it be that hard to add to the messages that are forwarded to the customer of a proxy privacy service to transfer message. In our work on this working group so far we've extended a number of messages like renewal will go through the proxy privacy provider to the customer. Is it a problem to add an FOA, whatever that stands for, to the kinds of messages that would go through the proxy privacy provider to the customer, from a staff perspective? Thanks.

Amy: Hi, Kathy, this is Amy again, and FOA is the form of authorization and it's the form that has to go to the registrar, the administrative contact, when a transfer request is put in for a domain to be transferred to a different registrar. And I think the concern that we're trying to raise here isn't the actual, you know, the prospect of forwarding on the form. It's more the issue of whether the privacy proxy service wants to forward on that form because of what it would mean for the privacy proxy service.

Because if they forward it on, the registration could be transferred on to a different registrar that the privacy proxy service may not have a relationship with. And so we just wanted to flag that for you guys to think about.

Kathy Kleinman: Okay, so it may also mean a change of registrar it may mean a change of (unintelligible). Okay, thanks.

(Paul): Can I be in the queue on this?

Amy: Yes.

Graeme Bunton: Yes, (Paul). Go ahead.

(Paul): Thanks, I guess I'm trying to understand practically what the peril would be. I can think of a few. One is scenario one where the registrar themselves, the underlying beneficial customer -- whatever we're calling them -- wants to transfer this domain name from the current registrar to a replacement. In which case, that registrar -- if they want to maintain the privacy information -- I think the spirit of what we're asking for is there be a mechanism that could do that. So that the privacy service doesn't have to terminate on one end in order to do the transfer that customer can set it up - the new privacy service on the other side so that it goes from privacy in the name of privacy service A as the first registrar to privacy service B as the second registrar.

And since that customer is doing all of that they can be responsible to work with both providers to effectuate that. So we need a mechanism for them to do that. And then the other scenario is that the registrar is telling the domain name or whatever and so it's going to be moving from, you know the first registrar as the first private proxy service to a second registrar and maybe the new buyer wants a privacy proxy associated with it or maybe they don't, who knows, right.

But that's up to the buyer to arrange in advance and the problem in that scenario is - there's two problems instead of one. In the first scenario the problem is how do we get approval and the transfer without disabling the privacy proxy service at, you know, the first registrar. And then the second scenario, carry that problem forward but there's a second problem in that after a transfer happens from the underlying - the new customer, how do we

make sure that the old privacy proxy Whois record doesn't travel with the registration as it ordinarily would.

So that's where - those are the two issues that we have to sort out. I would say, though, that in light of Herculean implementation issues, this is - I think this is something that could be done but I don't know - this smacks more of implementation than a policy thing. But obviously if others have a different view then I'll be quiet and listen to that. But I think that what we're asking for, you know, could be working out by the implementation team but I think it's important to a lot of people on this call that we do work that out or else we'll end up in a situation where, you know, identify (works) because every single time it may make the transfer (sync). I'm sorry this is so long.

Graeme Bunton: Thanks, (Paul), I see (James) has his hand up.

(James): Hi, thanks, just briefly (James) speaking. I just want to amplify what (Paul's) saying. He's identified I think a couple of important issues. But it's not just a concern necessarily for implementation. I want to be clear we are not creating a new vulnerability in the transfer of authorization process that is essentially a hand hijacker -- a new tool -- that allows them to say, of course I authorized this name. I'm just using a privacy service you don't recognize. Please give it to me immediately and, you know, that registrar is bound to follow - to check those boxes.

And so, you know, I think that's one of the concerns I have isn't just the operational concerns but what are we doing to the security around the transfer process. But I agree with you it's something that we need to look at a little bit further.

Graeme Bunton: Thanks, (James). My sense is we're going to have to take this one out of this particular moment and talk about it later a little bit. Which we can carve out of implementation and see if we can offer guidance to that. All right, Amy, back to you unless there are other questions.

Amy: All right, thanks. This is Amy again for the transcript. And thank you guys for taking this one back and thinking about it. And, you know, I mean, some of this may be implementation but we reviewed this and it seems like very significant change that we just feel like we need more guidance in terms of he does before it gets over to us. Because it really - it's really going to be a major change. Does anybody else have anything on transfers before we move on to the next point?

Okay, I don't see anything so I'll move on.

Graeme Bunton: Well a quick...

Amy: I'm sorry, Steve?

Steve Metalitz: Yes, this is Steve Metalitz again.

Graeme Bunton: Okay, Steve and then - go ahead, Steve.

Steve Metalitz: Again, just to put this in context. The question is whether this is something that's required by a consensus policy. And looking at the intra-registrar transfer policy it says that it has to be sent to the registered name holder or the administrative contact. I mean, when there is a proxy registration, there is a registered name holder or an administrative contact. So, I guess I'm not that clear on how this is handled today. But I agree that we need to be clear whether this is a communication that is required to be forwarded.

I think people may have been thinking more of like who is data reminder policy or other policies like that rather than this. But this should probably be clarified one way or another.

Graeme Bunton: Thanks, Steve. I think I heard (Chris Pelling) in there, too?

(Chris Pelling): Yes, thank you Graeme. One of the other things I also thought of was regards if you've got somebody who's not a contracted party, the lawyers who wish to do this without being credited, what's to stop them from simply declining an FOA request for transfer? What's the comeback there? There is no comeback. As Steve quite rightly just asked the question. You know, he feels it should be forwarded on after the registrars would forward it to the contact we have in Whois and that is already all registered in the contact. But there may not be or we wouldn't know if it was forwarded to the actual legitimate registrar as per the records show, or the record test.

I think it opens up that den of questions again with regards to, you know, having a data escrow of data that can be proven a show. I'll be quiet there. Thank you.

Graeme Bunton: Thanks, Chris, and I think that's probably a reasonable segue to what might be next. Would that be escrows, Amy?

Amy: Yes, you right. So the next point on this slide that we wanted to talk about is data escrow. You guys had asked us how conceivably escrow data could work and that - in thinking about it, the most logical method it seems to us would be to have data escrowed by the privacy proxy service through the registrar where the name is registered. You know, in this instant separate deposit could be required for each registrar where the service - where the privacy proxy service could help with registration.

And the reason - one of the reasons why we're thinking that this may be a preferable way to go is that creating an entirely new data escrow program would be a very significant undertaking. It's not something that we can just do and it would be particularly very expensive to create because the privacy proxy services, most of them are likely to be affiliated with (buyers) and resellers. The cost may not necessarily be worth what the benefit would be of having a completely separate program.

One point that we just wanted to make as well is that in certain places data held in escrow may not be reliable. And we say this not because data is not of value or that we don't think it's needed but because registrars who get brief notices often do have compliance notices related to data escrow. And when we do audits on data escrow the registrars we generally see improvements in the quality and completeness of what's there. But there's no way to audit privacy data in escrow.

So we fear that compliance may not be ideal. Does anybody have any back or comments for us on that line of thinking with respect to data escrow?

(Paul): This is (Paul), can I get in the queue?

Amy: Sure.

Graeme Bunton :(Paul) please go ahead.

(Paul): The memory that used in my mind and I want to just say, and I'll make it brief, is a preview of an upcoming discussion which is in the event attorneys get wrangled into this what we're talking about with data escrow is having to expose client confidence to data escrow providers. And then compounding it with having to disclose that through a registrar. And it just underscores the problem with trying to inflate (warriors) with private proxy services. That's all I'll say about that.

The second issue though the trade is a competition issue in my mind which is if we presuppose that the marketplace that the privacy proxy model will most likely will be or will always be through a registrar and its closely held affiliate or whatever. That - and if you set up the marketplace to work that way, for example, by requiring data escrow to be through a registrar rather than directly through an escrow provider. You know, we could in fact inadvertently - you know, the difficulty of entry into the marketplace, say in the situation

where somebody wanted to be a private proxy provider that practices (unintelligible) applying to become a registrar accredited for them as well.

And so this one sort of is - this idea sets off, you know, alarm bells and red flags in my mind and something I think we should give real thought as we go down that path kind of things together.

Graeme Bunton: Thanks, (Paul), I see (Bolcu) has got his hand up.

(Bolcu): Thank you, Graeme. Just one thought, I mean, what we're always hearing is the lawyer-client confidentiality. So that only goes a certain way. I mean it can be waived by the client and this would only cause each lawyer to disclaim his confidentiality in this client agreement when it comes to privacy proxy registration. So if you want to offer this service to the client you must say, well this is not covered by our confidentiality - by our client's lawyer confidentiality and that would do the trick. Unless I'm mistaken or it's different in the U.S., but it seems like a very simple solution to what is made to be a very big problem which I don't see it as it is.

Graeme Bunton: Thanks, (Bolcu). I think we're going to get to the lawyer issue a little bit later. I hope we're going to get to the lawyer issue a little bit later on relatively shortly. So let's see if we can put that discussion off for now and see if there are any thoughts specifically around data escrow. And I'm not seeing any hands. I am hearing some typing, though. Someone's typing that should mute their microphone. My only thought is that we need to be a little bit careful that we don't limit the existence of unaffiliated privacy proxy service as sort of a rule. But I think there are some points here to think about. Amy do you have anything else on this one?

Amy: I think we're good on that one. Basically we just wanted to emphasize, you know, that privacy proxy data escrow, it's not a magic bullet or, you know, it's not going to solve all the issues around trying to get to the beneficial customer data. So we just wanted to emphasize that and just lay out what we

were thinking on this point. Does anybody else have any questions for us related to data escrow before I move on to de-accreditation?

Okay, I don't see any so I will go ahead and forward the slide. Privacy proxy service de-accreditation is a really major issue in terms of thinking about how we would implement and try to come up with a de-accreditation process. Some of the issues that we've thought about and we don't really see answers to in the recommendations including the proposal that was talked about last week are, you know, if a privacy proxy service is de-accredited you guys had recommended that the customer be contacted. But the question is, you know, who would do that and how.

You know, you could require potentially the privacy proxy service to do it but if the privacy proxy service is being terminated they may not be cooperative. If, you know, the service is being terminated or de-accredited it's possible they may have issues with the data that's held in escrow. And then another issue is even, you know, if the data is in escrow who's going to get it. You know, if the service - they could have multiple deposits and you know that somebody's going to have to go through and notify these customers.

And you know, who's going to touch that personal data that comes through. It's really tricky issue. As I mentioned it's possible customers could be across multiple registrars and, you know, another issue is that, you know, the way it works with current registration is that by maintaining registrar and they transfer but, you know, in this instance with the working group recommending that we do something similar with privacy proxy services the question becomes, you know, what if nobody else would have known of the privacy proxy service once it's named. What - can you forward someone else to take the names and how will we do that.

And what if the registrar doesn't want to work with another privacy proxy service after the existing service is de-accredited. And then also this becomes complicated and this is the same with transfers if to a different

extent if the name is transferred over to a different registrar privacy proxy service, you know, how would a new privacy proxy service gain access to that account in a way that would be able to satisfy their requirements of being a privacy proxy service including potentially disclosing information and doing who is labeling. So I'll stop there and see if anyone here has questions about that.

((Crosstalk))

Graeme Bunton: ...question...

((Crosstalk))

Graeme Bunton: Have any of the what if problems you have occurred in the registrar the accreditation context? Or I see Steve has his hand up. You can say those (word again) if you like Steve.

Steve Metalitz: Yes. Yes. This is Steve. I mean, you know, so my question is what if no other registrar volunteers to take the names of a registrar that's been de-accredited? What if, you know, they don't want to work with those registrants? Has that arisen before? I mean again, I'm just trying to find out what the precedent here.

Amy: Hi Steve. This is Amy again. And Mike probably has the information and experience in this than I do. I don't know of a situation where this has occurred. But Mike can probably shed more light on that than me.

Mike Zupke: Thanks Amy. Thanks Steve. It's Mike Zupke again. So we've been fortunate that we haven't had a case where, you know, we couldn't find the gaining registrar to take some names.

We've had some close calls. We've had some let's say mercy cases or pity cases where we've had registrars say I'll do this for the good of the industry

where they said, you know, there's no value in this to me. In fact, this is nothing but work for me and probably headaches.

But they do it because they know it's good generally for the, you know, domain name ecosystem. And like I said, a reputation of the industry. We are though getting closer to that point where it's getter harder to find - getting registrars with new TLDs.

It used to be, you know, when the registrar got to get credit, they probably had names in, you know, three, four, maybe five different TLDs and the odds of finding another registrar who was accredited though is, you know, were pretty good.

We're now getting to a point where we have to do some serious matching of registrars. Say, oh, you know, can you take the one that has these 300 different TLDs.

So although we haven't had that issue, it is actually on of the things that keeps me up at night with regard to registrar de-accreditation. And I think it's just as possible with privacy and proxy in terms of the accreditation.

I think about, you know, some of the uses of proxy registrations that have concerned people in this group. You know, issues related to let's say freedom of speech.

You know, if the registrar is a proxy service and it may be that one registrant is perfectly willing to put its name as registrant for a particular type of Web site or, you know, particular usage of a domain name that others in the world would say no, that's too offensive to me. I refuse to be the registrant of that.

So, you know, we think there is a - we think there is a legitimate problem. It's more than just theoretical. We think, you know, there's a risk of this

happening. It's also sort of conceptually - it's really a change of ho2, you know, business would be done.

You know, we've never forced - we being ICANN - the data ICANN, not staff. But, you know, we've never forced any registrant to take a domain name. And that's potentially what we're talking about of doing here.

And so we just want to make sure that if that's really the path that we go down with implementation that, you know, we do this with the understanding and blessing of this working group. So hopefully that kind of helps to address the gist of the question.

Steve Metalitz: Well let me just follow up on that. This is Steve again. So I'm not sure how you're going to resolve that problem that keeps you up at night if it occurs in the registrar setting.

But this is not a case of forcing a registrar to take on registrations because the registration wouldn't necessarily change. Again, in an unaffiliated - in the unaffiliated setting, right. So it's not really comparable.

I mean I agree with you that this could happen but it is, you know, at some point we can't anticipate every possible problem. And since this is a problem that has to date not occurred in 16, 18 years of registrar accreditation - and not to say it won't because it might.

But when it does, then it'll have to be addressed there. And are you going to address that as an implementation issue or are you going to have a PDP on it? So I just think let's try to keep this in context.

And the other point I would make about context is that every point you've raised I think in this presentation deals with the problem of unaffiliated registrars. Registrars that aren't affiliated with an, excuse me, privacy proxy services that aren't affiliated with an accredited registrar.

The sense I get form the presentation is that you don't anticipate as major problems with implementing this in the case of providers that are affiliated with accredited registrars. Is that a fair conclusion and that the problems are all in the space of unaffiliated privacy proxy services?

Mike Zupke: So thanks Steve. It's Mike again. And maybe I didn't articulate what I was trying to say very well. You know, so the concern with registrars, you know, I (barely) think, you know, we could manage that.

I think it's a little bit different with registrants. You know, the privacy proxy being a registrant. I could see, you know, a case where we have domain names that we say okay, we're going to give them to another proxy service. And that proxy say I'm not putting my name on that.

So, you know, I think with registrars it's a little easier because they don't have a, you know, a legal duty with regard necessarily to the content of the domain name where a registrant does, the registrant here holding itself out there as being the person responsible - directly responsible for the domain name.

But if, you know, maybe I'm not quite understanding your question. So that was what I'm trying to say. With regard to the unaffiliated (work to the) affiliated proxy and privacy services, I think it can sort of work both ways.

If we de-accredit a registrar's proxy service meaning one that's affiliated with the registrar, there might be a good chance that registrar doesn't do business for any other proxy services as to how could we bring another proxy to that registrar if there's no such relationship.

That becomes important kind of in the more operational technical part of the implementation. So to the extent that that a proxy service has an obligation to publish data about a customer in Whois, they need to have some affiliation

with the registrar in order to do that. Otherwise they can't control the Whois output.

And I think there's probably some other, you know, similar kids of operational issues that might arise that we probably haven't even, you know, gotten to. But so that's kind of the gist that - I think we can be kind of agnostic to whether it's affiliated or not for the purposes of at least, you know, which is beyond this slide.

Graeme Bunton: Thanks Mike. Unless Steve has a response, I've got (James) and then Kathy in the queue.

Steve Metalitz: I'm not - the only response I'd make is I think the first bullet here it says major challenges to de-accreditation of PP services that are not affiliated with an ICANN accredited registrar. Now I'm hearing that bullet is not offered. Is there - and the same challenges if it is affiliated.

Mike Zupke: I got it. So this is Mike again. Just a quick clarification. I think what we're saying there is, you know, how do we find a new proxy service if it's not affiliated with that particular registrar in any way. I'm not sure if we necessarily meant in the contractually or in the ownership sense where it's (called by registrar).

I think we're more about what happens if, you know, this registrar has a bunch of proxy customers and they all get, you know, that proxy gets de-accredited. So there's no other proxy who does business with that registrar, what do we do? That might be what we were thinking there.

Graeme Bunton: Thanks Mike. (James) and then Kathy.

(James): Hi. (James) here. Thanks Graeme and looks like things have moved on a little bit from the point I wanted to raise. But in response to Steve, I think that that first bullet (form) is maybe perhaps an over simplification of what Mike is

alluding to because we shouldn't assume necessarily the de-accreditation of a privacy service and the accreditation of affiliated registrar are necessarily linked.

So for example, someone could lose their registrar accreditation but still maintain a privacy service or vice versa or they could both be, you know, executed by ICANN at the same time.

And I think that those difference scenarios are probably going to require different - a different implementation plan because in that particular case an affiliated privacy service would then quickly become an unaffiliated or an independent privacy service and would then be sort of floating looking for a new registrar to call home.

And I think that that extends also to the transfer problem because when a private registration - registrant using a privacy service wants to transfer between registrant - registrars, then they are essentially asking the gaining registrar to accept the old - to accept unaffiliated privacy services. And I think that's part of the reason why we were concerned about the legitimacy of the authorization.

So I - these things are really difficult questions necessarily to fix. I agree with Graeme. I don't think we're going to solve some of them in the course of this slide deck. But I do think that we need to flag them and circle back for some additional work because there are some important dependencies that are happening, you know, thousands of times an hour in our industry (unintelligible). Thanks.

Man: Thanks (James). Kathy.

Kathy Kleinman: Yes. I wanted to ask Mike and Amy about Bullet Point Number 2, which is how to or who will contact the customer because I think in some ways we were asking you. And now you seem to be asking us.

But so I'd love to know who in the end is going to - how we're going to get to the answer on this because let me explain the reasoning, which is that the customer should definitely be notified when there's a change of proxy privacy providers, when there's a de-accreditation.

And that's because we have the sense in the working group that particularly if they can't - if the proxy privacy protection can't be transferred, they should be given the option of deregistration of the domain name rather than global publication of their underlying data.

I don't know if that makes sense. Let me say it another way. Rather that - so if I'm a privacy customer and I'm losing my privacy protection, rather than that mandatory exposure in the Whois, I want to know and I want to be able to tell someone presumably ICANN that I would much rather not have the domain name than have my home addressed published and my home phone number and my cell phone number and all that.

How difficult is this? And then what steps do we need to do to protect what seems to be kind of the agreement of the working group? Thanks.

Graeme Bunton: Thanks Kathy. Any response from Mike or Amy on that one?

Amy: Hi. This is Amy again. And I don't know if Mike has anything additional on that. I think that there are a couple of different ways that this might work. But I think that we would want more guidance from the working group in terms of what you think. You know, where do you think as a matter of policy those obligations - that the - or, you know, how do you think that this should work? Mike, do you have any thoughts on this?

Mike Zupke: Thanks Amy. Mike again. I mean I think it's a really good question and it's one that, you know, there's a lot of implications to how you answer it. And so,

you know, while we could say yes, you can deal with this, you know, and this implementation you'll figure it out.

I guess, you know, I feel a little bit more comfortable having more guidance. You know, you know, with the registrar context what we do is the gaining registrars notifies the customers that there's been a change. And we post something on the ICANN sites the registrar can point to.

And, you know, what I'm hearing you say Kathy is that, you know, there might be other alternatives such as three's no gaining proxy service here (unintelligible) published or with enough notice you could try to find your own and you could make changes.

And so I think, you know, I guess I'd like to give some more thought to that but I also would, you know, also encourage the working group to kind of think through what the different, you know, sort of ramifications might be if we go down one path or another and there you're willing to leave it staff and the Implementation Review Team to figure this out or if you want to give us more guidance.

Kathy Kleinman: Great. Thank you.

Graeme Bunton: I see (Chris Pelling) has got his hand up too. And there's a comment to Kathy in the chat from Steve that's kind of interesting. It could be up to the customer (upon) notification. (Chris).

(Chris Pelling): Maybe really - just really all - this is (Chris) for the transcript. Thank you Graeme. This is really just all for Kathy in the fact that if a domain or the customer wishes their domain to be deleted, as an operational thing it still enters the - in your grace period and Whois has to be active for that period.

So if the underlying information is still there, it has to be changed by the registrants before (unintelligible) of the privacy proxy service because

obviously if it's privacy proxy service is stable and all the (unintelligible) information is then being released, the remaining information well that should be the registrant's information as (owned) by the PP service.

That's something that will stay in Whois for at least - well most registrars it's 30 days or 38 days with your grace period and then a further 30 days for redemption.

So, you know, either that has to be potentially put into (work) somewhere. That the accreditation would have to happen after say a set period of days, maybe 50 to allow Whois to simply be annulled by the end of that period. I'll put my hand down now. Thank you.

Graeme Bunton: Thanks (Chris). So and Kathy, your hand is still up unless you have a new comment. So (James) is making a pretty good suggestion in the chat, which is we're going to have to put together a few (words) for staff because (unintelligible) can put some high level proposals.

And that's not a bad idea. Do we have more in your deck? Is there a couple more slides? Is that correct?

Amy: There's just one more slide and that's it. This is Amy.

Graeme Bunton: Okay. Well let's have at it.

Amy: Okay. All right. And so the final point we wanted to raise today - we just wanted to flag this issue for you. It relates to account holder data verification. And I believe it's Recommendation 5 in the draft final recommendations.

The recommendation says that the privacy proxy services validate and verify the account holder information since it's they way with the RAA requirements.

And we just wanted to point out for you guys, and I'm sure you're aware, but the account holder data is something to verification. But if verification fails for some reason with respect to account holder data, there's no requirement that the domain be suspended if the verification fails.

And so in thinking about this, we just thought it raised an interesting question about the value of this recommendation just because there's no consequences if verification is not successful based on how the recommendations were written today.

Graeme Bunton: And I see (James) has his hand up. (James) please.

(James): Hi. (James) speaking. Thanks. And I wonder if this is just a case of crossing our terminology a little bit here. I think when we say account holder in the context of a privacy service, we're saying the underlying customer of the - or the (benefit) registrant whereas the account holder that's referenced in the RAA is the account holder at the registrar, which may be different than the registrant.

So maybe we just - we can work - and I may be grasping at a mirage here but I think that if we used some more precise language in this recommendation, we can address this fairly quickly.

Graeme Bunton: Thanks (James). I think that's helpful. Anything from maybe Mike or anybody else on this particular one?

Amy: This is Amy. There's nothing else from me on this (slide).

Graeme Bunton: So thank you for your presentation. I think you guys have raised some interesting problems that we're going to have to think through and some of which was we may end up pushing a little bit of you guys on.

But I do think (James) had a very good suggestion that we put together a small team to work with you guys to see if we can come up with workable scenarios to answer some of these questions. And that activity is going to have to happen pretty darn quick.

So I'll appreciate your work on that. And we'll sort of - we're going work on that on the list I think in the short order. I think that's all from you guys. So I wouldn't mind and I think it's possible we wouldn't mind some of your input on a discussion that I think it's up next, which is centered around those language concerning definition of privacy and proxy service providers. And this also goes to the - what we've been calling the lawyer issue.

And we need to think a little bit about how this will work in context and how this may come back to service providers when complaints come in. So we've - (Chris) has spent some time on this and we've looked at specific carve outs from the (two) lawyers although I don't think we've had the reverse, which was to include lawyers.

And the text we're sort of currently looking at is the additional language for definitions, which is registrars and (unintelligible) registrations. I would think proxy service providers who are not accredited to the process (dissolved) by ICANN. And I think that language originally came from Kathy. And then we adjusted it slightly to ensure it accepted all the different models of registrars.

And so there's a couple of thoughts that I wanted to include or exclude lawyers specifically and we want to see if we can live collectively with this (test).

And then we need to think a little bit while we have staff on the line I think about how the process might work if someone complains that a registrar is really a proxy; if a registrar is accepting registrations from a non-accredited privacy proxy service.

Maybe the best way to get this going is Kathy you're saying it doesn't look like your language anymore. And we can go back and find your original piece and we can talk about how we got to this. Although that might be a (Mary) question.

I also see (James) has his hand up too. Maybe we'll go to (James) and sort of see where this language came from. (James).

(James): Hi. Thanks Graeme. And I think that this - well at least one of the several origins for this idea was through the Whois Review Team and the RAA negotiations where we came up with this temporary specifications.

And the reason for that was because of the challenge of how do you - as ICANN, how do you regulate a non-contracted party? And I think what we identified was that the concept that those who fall under ICANN's governance do so willingly by entering into a contract either with ICANN directly or with a contract party.

And so that there needed to be this arm's length effort to control effectively for the first time in ICANN's history controlling registrants, not folks that have singed a direct contract but, you know, I think, you know, I guess you could make the argument that the UDRP was the first time that trail was laid.

I think that we need to think carefully about this here because there are some considerations like you were saying is that, you know, first of all, the word that I see here that's being - that's missing is knowingly.

Registrars will not knowingly accept registrations from service providers, things like that. I certainly don't believe anyone on this group is setting up the intention where someone could trick a registrar into accepting private registrations from a service that was not accredited because it just, you know, just launched that afternoon or something along those lines.

So I think first off we got to - we need to insert some sort of awareness. And then what do we do when a registrar or when ICANN is notified that a, you know, let's say a batch of 1000 registrations that their customer that they're dealing with is not actually their customer but an illicit - well potentially a rogue privacy service.

And then I think that the registrars would need to have some mechanism for confirming that or auditing that. And then having some contractual steps that they can take to address that situation once it's reported to them.

And then I think then ICANN compliance steps in to say, you know, we think you handled this correctly or we think you dropped the ball or we don't think you did enough to ferret out the privacy services - the unaccredited privacy services that are on your network.

So, you know, I think this is a bigger question and I'm sorry if I'm taking this down a couple of different paths. But I think generally this arises from the question of how do we reach through the RAA and the whatever we're calling it, the PPAA to get at the behavior of these services and their customers.

Graeme Bunton: Thanks (James). I think there was a piece of that that is relatively easily solvable, which was you said knowingly. And I think that text is in the RAA. And I think - just see if people are opposed to including it in this definition would be something along the lines of registrars will not knowingly accept registrations from privacy proxy service provides who are not accredited. (Unintelligible) by ICANN.

I think that solves some problems. Thoughts? Are we all very quiet because we think we solve the lawyer issue? (Paul).

(Paul): This is (Paul). I'd like to go in the queue.

Graeme Bunton: Good. I'm glad to have you in the queue. Please go ahead.

(Paul): I guess I don't understand how this addresses the issue. I mean I understand it's how to address who's concerned for registrars not to get in trouble in got you situations, which I think is fair enough.

But I don't see how it addresses the underlying issue of requiring - essentially regulating lawyers, requiring them to require their clients to waive fundamental rights, confidentiality in order to participate. And it's the particular Internet that ICANN is running.

And, you know, to (Volker)'s point, I guess sure. If that - if it's set up that way to where all clients have to waive the right - to their attorney client privilege. And that solution then, you know, there's also - there's a far easier solution, which is for everybody on the call that believes that there's a right to privacy that we are all working here to protect in some way through allowing privacy proxy services in general.

You know, likewise everybody could just waive all their rights to privacy in order to participate in this Internet. And I don't think anybody - well I shouldn't say anybody. I think most people eon this call would not think that was a great idea.

So I don't think taking, you know, 95% of the working of the group to be to preserve a privacy right and 5% of the work of the group would be to take away a right to your attorney client relationship, the confidentiality of that, I don't think that that's a good outcome. And I think that the suggestion has flipped.

I would like to get to the real issue, which is are we going to propose to ICANN that they begin regulating lawyers, which is what we're talking about here. And I would also - and now this is - we're getting towards the end of this conversation I hope. So I'm going to be a little bit blunt.

I would like to dispatch with the fantasy that there is nothing particularly special about the relationship with attorneys and clients. All of that's enshrined in almost every human rights treaty that you can think of. It's enshrined in case law in almost every civilized place in the world.

So I do think that conflating the two and considering them on the same plane of parity is a fantasy position and I think we need to move beyond the fantasy position and talk about whether or not ICANN really wants to be in the business of regulating attorney client relationships.

And if so and if there is widespread preference for ICANN regulating lawyers, then this is the part where we have to start talking about minority reports because there's just no way that I - that I could go along with the part of the report that says ICANN should be in the business of regulating lawyers.

So there it is and I'll be quiet and we'll just let the chips fall. If we can - if we can get to a real solution, terrific. If we can't, then we need to start talking about how we can make note of the disagreements either in the report or if I'm a minority of one and in a minority statement and how all that works. Thanks.

Graeme Bunton: Thanks (Paul). Appreciate the input. What I - the place I think we're at by not doing the inclusion or the exclusion is we're almost pushing it back onto ICANN itself to say what would you do in the case where a registrar has 1000 registrations from a particular law firm and someone complains about that - is why I'm kind of curious to see if Mike or Amy had thoughts. But I've got (James) and then (Phil) in the queue. (James).

(James): Hey Graeme. Thanks. (James). And actually thanks to (Paul) for just kind of laying it all out there. I actually find that really refreshing and encouraging because I, you know, I'm not sometimes the most elegant person in what I'm trying to say.

But I think that there are - I actually agree with the idea that ICANN should not wade into these waters of regulating the relationships between lawyers and their clients.

I would point out that one of the fears of a legitimate privacy service that goes through all the trouble to set up this accreditation service and monitor their customers and set up all these mechanisms for reporting and disclosure reporting, all the stuff we talked about is that some - let's say some less than scrupulous lawyer will find a less than scrupulous registrar and go set up shop offshore somewhere and create - call themselves a law firm/registrar/privacy service and basically undermine this whole program.

I don't believe that's a theoretical or rhetorical concern. I do believe that that is a - that is something that we have to be mindful of as we work through this. And so I think we all just need to be as imaginative as possible because we're all - all of the folks who come to ICANN I think are good players and I don't know that we are always comfortable putting ourselves in the mindset of what people will do to work around the rules that we work so hard to create. So I just wanted to put that out there as well.

One thought that I had over the weekend, and it's not fully baked yet so I would beg your indulgence just a little bit, but, you know, one of the things that keeps coming up with regard to privacy services that we have today, which is a fairly unregulated climate, is, you know, this idea of how -- and bear with me for a second -- it's one of the sections of the RAA which where a registrar is offering a privacy service and there is a note in there that basically gives the registrar a limited window to disclose their underlying customer if they are not - if a registrant that's listed in Whois is not actually the customer. I think it's 377 something.

Anyway, the point here is that there's a carve out for registrars that are operating on behalf of their customers. And I think about how this program, this accreditation program is actually - yes it's creating all these new

obligations for service providers, but we could also explicitly state -- because I think we're implying -- that it's creating new protections for privacy services as well. If you're an accredited privacy service and you're operating in accordance with these rules that, you know, are free from that kind of intermediary liability for what your customers are doing, which is I think the goal of all the service providers at all levels.

So my question, or my thought, is where do - if you do have a law firm that is acting as a privacy service and registering large numbers of domain names on behalf of their customers, where do they fit in that? Do they still enjoy the protections that are offered? Or do they say, "Look I'm a lawyer, I'm taking responsibility for my customer.

That relationship is covered by various privileges and right to privileges and so if you have a particular issue with this domain name or this client, I'm their agent, I'm their representative" and kind of stand out there in a way that registrars and privacy services don't want to do for their customers.

So I'm kind of - just kind of throwing some spitballs out here and hoping that some of the folks who are maybe on the other side of this equation or maybe looking through this from the other side of the mirror can help me understand where they would be - law firms falling under that framework. Thanks.

Graeme Bunton: Okay. I understand. I think there's a whole bunch to take in from that. I think there's an interesting (unintelligible) in there and I would be curious to hear maybe back from (Paul) about that is that if we state explicitly that, you know, if you're not operating as a privacy and proxy accredited provider then are you taking responsibility for those domain names? And if we make that explicit in our work, does that solve some of this problem for us? So I've got Phil and then Susan Kawaguchi in the queue.

(Paul): And I'm happy to reply if you'd like, at whatever point in the queue you want me in.

Graeme Bunton: Well let's have you reply directly now I think if Phil and Susan (unintelligible).

Phil Corwin: (Paul), this is Phil. I think you might find it useful to reply at least after I speak on this.

(Paul): Okay. I'm happy to defer to Phil and Susan both.

Phil Corwin: Okay.

Graeme Bunton: All right. So let's do Phil first and then Susan, and then we'll come back to (Paul).

Phil Corwin: Phil Corwin for the record. Listening to the discussion, I have to say I feel like I've gone down the rabbit hole and through the looking glass. Because at seven this morning I was on a CCWG call where there was a one-hour debate without resolution about what language would be adopted in ICANN's mission statement to make it clear that ICANN enforcement of its contract with contracted parties was not to be considered regulation but how to and then, you know, going around, "Well what is regulation, how far can ICANN go through consensus policy in dealing with things that are public policy implications?" That's a very current and hot topic in the CCWG.

And here we're talking - and it's all about preventing mission creep and giving ICANN power to censor content for those who are concerned about it. And here we're talking about ICANN in effect regulating parties who aren't contracted parties, which sure looks like mission creep.

So it may not - now I recognize that there is a potential loophole and that there might be unscrupulous lawyers who set up rogue PP providers that offer services, but on the other hand, I got to say by what practical means would ICANN determine that a law firm is - has become a P/P service provider, which goes to the language before us on the screen.

There's a big difference between a rogue law firm/privacy proxy provider which holds itself out to the public as offering that service and a law firm which has an occasional client accommodation where the client says, "Hey

I've got a new product coming out and I want to register a domain name associated with it. You're doing the legal work on the product. I'd like you to register the name so nobody connects it with my company until we want to go public." How would ICANN even know that that's going on when a law firm registers a particular domain name?

So I think there's policy aspects here that go to mission creep that have to be considered and there's a practical implication of how do you differentiate between the legitimate law firm that are doing this per a legitimate client accommodation and the - a rogue lawyer or law firm that might seek to circumvent whatever rules we put in place there.

I don't know the answer but I wanted to raise the issue.

Graeme Bunton: Thanks, Phil.

Phil Corwin: Thank you.

Graeme Bunton: And I've got Susan up next. Susan and then we'll come back to (Paul).

Susan Kawaguchi: So in my work at Facebook I use outside counsel frequently to register domain names for us as Phil mentioned, you know, for a new brand rollout or sometimes we want to defensively register offensive domain names that include our brand and not necessarily be associated with the registration.

There's a lot of reasons, and I try desperately to not ever launch a live site with content with a proxy registration still in place, whether it be the, you know, our law firm or domains by proxy, for example because I don't think

that's a good practice. There's been times when I've had to do that just momentarily and then reveal it later. But, you know.

And I also sometimes will instruct our outside counsel to use a proxy service, a reliable proxy service like Domains by Proxy. So not only is it a Domains by Proxy mass registration, then it's if there was a reveal then it is our law firm. But at the end of the day, and I think this point goes to some of (James)'s thinking, is I feel that those registrations registered by our outside counsel are much more - would be much more responsible and responsive to any inquires than a normal just using a proxy service.

You know, they - we have certain agreements with the law firm and if something - if the domain name was to be in use for a short time still with that masking, then of course we would respond. We would not, you know, if anybody reached out to us at all and was asking question about the registration. Of course I try desperately to never register a domain name that includes somebody else's trademark too, but.

So I think the law firm is a much higher bar and has - is much more responsive, and I pay for that. There's, you know, there's a definite choice when I go to register domain names is how valuable is this domain name to our company and to protect it in a way that needs to be protected, I need to pay more money to get the service of a law firm to do it. If it's a throwaway domain name that I just don't want people to see just yet because we're not sure what we're doing, then I'll use a mast, you know, a regular proxy mass registration service.

But we - all of us who use law firms are paying more for that service because we're asking for more service in return. So I think if to include law firms in this would - well I think we would be going down a rabbit's hole and I also think that if, you know, I know that I can get my outside counsel to agree to be responsible and be the registrant of record for a domain name, if we want to put that information in the - if we want to include that as a requirement that if

you are not an accredited proxy registration service then you are the registrant of record. Then I mean I know that I can pay extra for that service, and I think law firms would do that.

Graeme Bunton: Thank you, Susan. And I think that end piece is getting at what (James)'s suggestion was. (James) also made a point in the chat, someone complained a registrar would be obligated to investigate. That's kind of a curious scenario to think about too. How would a registrar ever prove that someone isn't the registrant domain name if the name is on it. I have a tough time visualizing what that would look like.

But, (Paul), you've been very patient. Please go ahead.

(Paul): Thank you. So just a couple thoughts and reaction. First of all, I agree with Phil that this is not only mission creep but it's wild mission creep. And, you know, the - attorneys are already, you know, regulated plenty by the supreme court of their jurisdiction in most states and standards and rules that are place, and if you don't follow them, you're in trouble.

And so I just don't think this is an area that ICANN has any business in. And importantly, it's that (unintelligible) even if ICANN should be in this business for estimating well you're - I can't think of a worse time to be in this business with everything else going on.

Secondly, (James), yes you hit it right on the nail head, which is, you know, there are different standards here. Privacy proxy services can argue whatever they'd like to argue about whether or not they're responsible for what their customers do. And I don't think we have to, you know, I don't think we need to wade into that particular issue to highlight the fact that attorneys are in a completely different boat.

If I have a client and I'm the registrant or domain name for that client and they're using it for a nefarious purpose and I find out about it and do nothing

about it or, you know, I don't know - even know what happens if, you know, even if I don't find out about it, right, you know, I'm in trouble, you know? I'm in trouble six ways to Sunday, right? And there, you know, we - there's just different standards. The - it's a different, completely different framework, right, as it should be.

And so I don't think (unintelligible) to do really makes any sense, because I don't see privacy proxy services wanting to take on the same level of responsibility that attorneys have in this context. And so I don't think that they're really the same thing at all.

So I think that, you know, we could easily dispatch with this issue and we can say either nothing in our report, you know, should result in ICANN regulating, you know, attorneys and the attorney-client privilege. Another option is to say that there's no obligation to - for attorneys to become accredited service providers so long as any registration on behalf of their client is done ancillary to providing other legal services for that client, right?

I don't know. There's all kinds of ways to get there from here. I prefer the first one. I just don't think ICANN should be in this business and should be commenting at all other than to say that nothing here affects lawyers and their attorney-client relationship.

But I don't think there's going to be any real traction outside of this particular rabbit hole we find ourselves down, any particular appetite out in the real world for the notion of ICANN regulating attorney-client relationships and requiring people to waive fundamental rights to counsel in order to participate in this particular Internet that ICANN has - is set up and running. Thank you.

Graeme Bunton: Thanks, (Paul). I see Volker's hand. I have a gentle optimism that there is some common ground between what (James) is suggesting and what (Paul) is hoping for there. And that might be the case that we need to get some

language together and we can all sort of take a look at that and move forward.

We have about 11 minutes left and we still haven't gotten to the IDS, and so let's hear from Volker and see if we can have a few minutes more on that. Hopefully that conversation will be brief. But Volker will be brief in his comment here, please. Thank you.

Volker Greimann: Not that brief. When we are talking about regulation of lawyers, that's U.S. lawyers. There are lawyers in every country of the world, some more regulated, some other regulated, but which then state lawyers in some small island state doesn't have that much of a regulation would be treated different than lawyers in the United States just because you higher regulation on that.

I think by proposing different standards for different categories of providers of this service, we're just talking about this service as in providing privacy proxy for domain names, not the ancillary lawyer services that you provide to your customers on the side.

Just for this service, everybody needs to be treated the same way. Otherwise I don't think we will get to the consensus agreement here. And that's I think fundamental from when we started this that we wanted to have a system that would apply to all registrars, all providers of the privacy and proxy services that are out there in the world.

I mean from us at the registrar perspective, the entire deal here was that we have one sort of one policy covering everybody who is providing the services. Otherwise if you exempt lawyers, why don't you exempt doctors who have clients or patients confidentiality if they provide something in proxy services for their patients on the side because they have the same right to privacy, if priests, journalists, there's different classes of people who also have the same confidentiality rights that lawyers have. Would you have to create exemptions for all them? I don't think so.

We have to have a rule that applies to all the same way. Otherwise you will create loopholes and these loopholes will be exploited, and you will create an uneven marketplace. And we cannot accept that -- at least I cannot accept that. And if you propose to do that, then I will have to say that we will not reach consensus, at least from my perspective.

Graeme Bunton: Thanks, Volker. All right so maybe it's time to move on from that discussion, and I think the way forward -- and I'll have a chat with Steve about this -- is to take a look at that 377 language and what (Paul) has been saying and to see if there's a way that we can move forward where we're not trying to regulate lawyers specifically but we're not also building loopholes. That is what we've been trying to do for some time but maybe there's a bit of a window here.

So that leads us on to - we've got about eight minutes left and maybe we can have a brief discussion here about the draft language for option two of the illustrative disclosure framework. Now I think this is close to Kathy's heart so I might lean on her a little bit here.

But this is mostly around, from my understanding, is jurisdiction and options for arbitration or going to court. So we have some draft language here in front of us. I wonder if I can get - oh I see Mary's got her hand up, and then I might see if we can get Kathy to respond. Mary, first please.

Mary Wong: Thanks, Graeme. And I just wanted to clarify that Todd and Kathy and other members of the sub team are on the team, but I just wanted to clarify that the sub team is working on this and the draft contains language that has been circulated to the sub team based on suggestions made by Steve from last week. But I don't think that the sub team has come to a consensus on this language or indeed on the question as to what the specific purpose is regarding customers would be for option two. Thanks.

Graeme Bunton: Okay. Thanks, Mary. I still see considerable debate going on in the chat around the lawyer issue. So maybe I moved on a little bit prematurely. Volker, your hand is still up or is that an old hand? That was old. Was it Todd and Kathy that were working through this language? Does either one of them wish to speak to it?

Kathy Kleinman: I'll give it a shot, Graeme. It's Kathy.

Graeme Bunton: Please.

Kathy Kleinman: Okay, first this is not the language that was circulated. That's not what's up here. The language that was circulated was similar but different. You know, when you change an and to an or, things get different. But what was circulated to sub team three and to the working group last week was, you know, was this concept that was very similar actually to the UDRP waiver, which is when there's a problem where can the customer go to sue the requester for some kind of abuse of the process, particularly here some kind of publication that let to (doxing) or swatting or something like that.

So let me read the language the way it's probably intended to be, not the way it is up there. But in making a submission to request disclosure of a customer's contact information, requester agrees -- and the requester should really agree to do this is the affidavit so that it's a knowing waiver of jurisdiction -- to submit to jurisdiction of the court. And it should probably say in the location of either the customer or the provider of -- in this case provider's primary place of business.

And then this was language proposed by Steve solely for disputes arising from alleged improper disclosure caused by false statement made by the requester, so false statements by the requester to the provider, or from the requester's knowing misuse of the information revealed to it in response to the request. And that qualification probably makes sense.

But it's really important that the customer be able to reach the requester as the complainant in the UDRP proceeding can reach the registrant. So I don't know where this language came from but there's an or instead of an and, and we really need this to be the jurisdiction of the customer and the provider. You know, the requester can't go off to Panama, submit the request, and kind of be unreachable to the customer. Thanks.

Graeme Bunton: Thanks, Kathy. Todd and then (James). And given that we don't have much left, let's see if we can get some brief responses and hopefully we'll have some wonderful agreement in four minutes.

Todd Williams: Todd Williams for the transcript. Thanks, Graeme. So, you know, most of the discussion in the sub team three this week has been on not this particular language but on kind of the pros and cons of the two options to the extent that it appears that more people are favoring option two to option one and we are going to kind of dive into this specific language.

The quibble that I would have with what Kathy just said is I don't think asking the requester to agree as part of its request to the jurisdiction to where the customer is located has ever been on the table for the precise reason that the requester at making - at the time of making the request has no idea where the customer is located.

And I thought we had kind of agreed a long time ago that that, you know, was just not on the table but that, you know, asking them to submit to a jurisdiction where the provider is located, which they at least know, is kind of what has been contemplated. So just to wrap up, to the extent that we're going with option two, I think the language that's in front of us is fine. Thanks.

Graeme Bunton: Okay. Thanks, Todd. And it sounds like - so do we need to hear back - so there's still work going on within your sub team. And do we have a sense if you guys will be coming back to us again in the near future with some more work? I'm just asking anyone there.

Kathy Kleinman: I'm not sure the sub team is going to be able to reach consensus. This is Kathy.

Graeme Bunton: Okay. Thanks, Kathy. I've got (James) and then Stephanie. With two minutes, you guys each get one.

(James): Hi, Graeme. (James). I'll try to wrap it up in 30 seconds. I don't like the restriction -- and I think we discussed this previously -- I don't like the restriction of specifying location of the provider or location of the customer. You know, for a global business, if some of the registrars and providers are getting to be quite large, you know, will have multiple locations and for tax or legal purposes maybe serving customer for example in India with their Indian affiliate, or customers in Brazil from their Brazilian office or something like that.

I think more importantly it should just state something along the lines of that the jurisdiction that will be used for disputes arising from alleged improper disclosures will be disclosed by the provider, and then just let the provider say, "Hey look, you know, you're filing a report, that's great. Just to let you know, if you misuse this information, disputes will be resolved in the jurisdiction of blah." And then let us fill in that blank because, you know, it's too restrictive to say location, and I'm not even sure what location means when you have 13 offices in the U.S. and 20 around the world. Thanks.

Graeme Bunton: Thanks, (James). That seems like a reasonable option to me too. You know, that would be disclosed up front so the registrant would be aware of that. And I think that could be something that could be disclosed to privacy and proxy providers.

I've got Stephanie and then we'll wrap the call up. Stephanie?

Stephanie Perrin: Thanks, Graeme. Stephanie Perrin for the record. I'll try to be quick. I put this in the chat just in case I don't get a full explanation. But we discussed the possibility of a bond for bad faith activity the last time. I appreciate the changes to the language that's been proposed here, and I think that helps but the jurisdiction doesn't necessarily solve the power and balance problem.

For those people that are at risk, recognizing that it's very difficult sometimes to ascertain when one is being gamed for the purposes of finding someone in life and death situations, I think it's important that the beneficial registrant has the ability to request that a bond be put up. At least that would slow down things and put some skin in the game for the requester. Thanks.

Graeme Bunton: Thanks, Stephanie, for the suggestion. That brings us to 11. I'll wrap this up relatively quickly. So thank you first and foremost to Amy and (Mike) again for your presentation. What I'd like to see on the list in the very near future, right after this call, is people who want to work on a team with staff to try and come up with some solutions to the problems they presented. That would be great to see some volunteers for that.

And then we also need to take back that language on lawyers and that section of the RAA and see if there's a hybrid solution there. We do not have lots of time left this time to get our work done for the GNSO call in December. And so this is your reminder that we need to look at the draft final report and have a careful read of that. This is an obligation for all of us so that we can flag any remaining issues that we're not still currently talking about.

With that I'll leave you all. Thank you very much for the call today and the discussion.

Man: Thank you.

Man: Thanks, everybody.

Man: Thanks.

Man: Bye everyone.

Terri Agnew: Once again the meeting has been adjourned. Thank you very much for joining. Please remember to disconnect all remaining lines and have a wonderful rest of your day. (Claire), please stop the recording.

END