

**ICANN Transcription  
Privacy and Proxy Services Accreditation Issues PDP WG  
Tuesday 09 September 2014 at 1400 UTC**

Note: The following is the output of transcribing from an audio recording of Privacy and Proxy Services Accreditation Issues PDP WG call on the Tuesday 09 September 2014 at 14:00 UTC. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.

The audio is also available at:

<http://audio.icann.org/gnso/gnso-ppsa-20140909-en.mp3>

On page:

<http://gnso.icann.org/calendar/#sep>

Attendees:

Steve Metalitz - IPC  
Graeme Bunton – RrSG  
Griffin Barnett – IPC  
Tatiana Khramtsova – RrSG  
Frank Michlick – Individual  
Volker Greimann-RrSG  
Don Blumenthal – RySG  
David Heasley-IPC  
Jim Bikoff-IPC  
Chris Pelling – RrSG  
Tobias Sattler – RrSG  
Kathy Kleiman – NCSG  
Justin Macy - BC  
Susan Kawaguchi – BC  
Kristina Rosette – IPC  
Darcy Southwell – RrSG  
Amr Elsadr – NCUC  
Paul McGrady – IPC  
Libby Baney – BC  
Phil Marano – IPC  
Holly Raiche – ALAC  
Sarah Wyld – RrSG  
Christian Dawson – ISPCP  
Victoria Scheckler - IPC  
Michele Neylon – RrSG  
Lindsay Hamilton-Reid – RrSG

James Bladel – RrSG  
Osvaldo Novoa – ISPCP  
Val Sherman – IPC  
David Heasley – IPC  
Kathy Kleiman – NCSG  
Luc Seufer – RrSG  
Keith Kupferschmid – IPC  
David Hughes - IPC

Apologies : none

ICANN staff:

Mary Wong  
Marika Konings  
Mike Zupke  
Amy Bivins  
Daniela Andela  
Maryam Bakoshi  
Nathalie Peregrine

Coordinator: The recordings have now started, you may proceed.

Nathalie Peregrine: Thank you very much, (Damon). Good morning, good afternoon, good evening everybody and welcome to the PPSAI call on the 9th of September, 2014.

On the call today we have Graeme Bunton, Chris Pelling, Volker Greimann, Holly Raiche, Tatyana Khramtsova, Steve Metalitz, Tobias Sattler, James Bladel, Michele Neylon, Frank Michlick, Don Blumenthal, Libby Baney, Darcy Southwell, Christian Dawson, Griffin Barnett, Keith Kupferschmid, Sara Wyld, Susan Kawaguchi, Justin Macy, Luc Seufer, Vicky Scheckler, Val Sherman and Kathy Kleiman. We also have Jim Bikoff who has just joined the audio bridge.

We have received no apology for today's call. And from staff we have Marika Konings, Mary Wong, Mike Zupke, Amy Bivins, Danielle Andela, (Maryann Bakashi), and myself, Nathalie Peregrine.

I'd like to remind you all to please state your names before speaking for transcription purposes. Thank you ever so much and over to you Don.

Don Blumenthal: I like that no apologies for today's call. Not yet I guess. Any rate just a reminder as usual to update your SOIs if there have been any changes.

Why don't we dive right in? We've talked a lot about accreditation on the policy side but thought it would be useful to step back and have a presentation from staff to get an idea of the implementation issues that they're working on to help frame our discussions.

So with that I'll just turn it over to Amy or Mike, whoever is taking the lead here, and step back.

Mike Zupke: Great. Thanks, Don. This is Mike Zupke, Director of Registrar Services for ICANN. And I really appreciate, you know, you all giving us an opportunity to come and talk to you because I think that from our perspective this is, you know, at least as much a listening experience as it is a talking experience for us.

And so we'd like to kind of give you an idea about what we've been thinking in terms of the way that accreditation might work from an implementation standpoint and then hear, you know, thoughts of the group and of course answer any questions that you might have, you know, we'd be happy to do that.

And I think, you know, there may be probably plenty of questions you'll have where the answer might be, you know, that's a good question, we'll think about that.

But we'll, you know, but we'll do our best and so by all means please feel free to, you know, interrupt with any questions that you have. And so Amy Bivins, who is also on the Registrar Services Team, put together some slides but I didn't really want us to necessarily read the slides to you so feel free I think they're unsynced so feel free to browse them if you like. It's really kind of a list of what we thought were the, you know, sort of the overarching considerations about how we want to think about implementation going forward.

But, you know, I was hoping we could have a little bit more of an unscripted sort of a discussion. And so - and I'll just sort of admit right off the bat here I'm not the best at monitoring the chat room so if somebody needs to, you know, tell me to shut up and wait for a minute, by all means you won't hurt my feelings.

So having said all that, you know, we've been thinking a lot about sort of how this, you know, program might be implemented. And Amy has been really closely, you know, monitoring the developments of the working group and sharing those with me and with the rest of our team.

And, you know, I'll say I don't really envy a lot of the questions that you all have to answer. You know, I think we've got our own set of difficult questions but I think, you know, most of yours are probably the hardest ones.

And so, you know, we've been kind of thinking a lot about sort of in parallel some of the questions that you're thinking about and how, you know, how does that affect what implementation looks like.

And so, you know, an example that comes to mind is, you know, there's this kind of recurring theme of - by the working group of, you know, who should be accredited or, you know, who can be a proxy or a privacy service in this program.

And, you know, from, you know, my own personal perspective, you know, that question is less material to me is the question of who practically could be accredited because, you know, we look at this and think, you know, you could define a proxy service to be every post office - a post office box service or, you know, every prepaid cell phone provider or any mailbox rental facility or any law firm.

And there's, you know, there's endless, you know, there's an endless list of people who might qualify as a proxy service depending on how you start to define that.

And we were really thinking about that and saying well, you know, how reasonably could you accredit these people? And I think saying that we're going to post office level or going to the prepaid cell phone company, you know, level that's probably, you know, more than anybody really would envision or had intended.

So, you know, not only that but we're thinking about a lot of these, you know, things that could potentially be considered proxy services. And even with law firms, you know, there's generally protections in place for registrants and we think that, you know, there's likely to be a de minimus impact on other stakeholders such as rights holders for a lot of these services.

So, you know, if you're a mailbox company - your mailbox rental company goes out of business, you know, the alternative is you just update your address to the new one; there's not, you know, there's not a substantial, you know, risk to the registrant of a failure the way there would be if it was more tied up the way, you know, proxy services currently typically are with registrars where if your proxy service failed you might also not have access to your registrar.

So that's kind of, you know, where we were as our starting point and thinking about, you know, what we really want to come up with is, you know, what the practical way of looking at this. And so we came up with a few questions and I think kind of the, you know, you'll see sort of the short versions of those in the slides that are available here.

But, you know, from my perspective, you know, our number one concern I think is the protection of registrants and then, you know, obviously all the other stakeholders who have an interest in these domain names. And so, you know, and part of this is, you know, my history with ICANN dealing with, you know, registrar failures pretty, you know, regularly that's always kind of the first thing on my mind is, you know, what happens if they fail.

And so that was sort of our first attack at this, I think we've spent a lot of time thinking about well what happens if the service fails or what happens if they're out of compliance and we need to take some sort of enforcement action.

So, you know, thinking about that, you know, my mind first kind of goes to, well, so what happens if we have to put one of these services out of business? You know, what's the ultimate punishment of a noncompliant or a, you know, actor or bad actor in this business?

And, you know, as we think about it, you know, the answer is sort of inevitably well, you know, the customers get punished, right, I mean, if you say to a proxy or a privacy service, well, you know, you're bad, we're putting you out of business.

Well that means that we're turning off the service and the registrants who are, you know, the customers who are using these services could suddenly find themselves, you know, without the privacy expectations that they had.

So, you know, that's obviously one of the things that we're trying to think about, you know, how do we mitigate against that sort of harm. And we kind of came to this realization that, you know, the registrar is inevitably going to play a very critical role in the privacy and proxy sort of accreditation regime no matter how you look at it because enforcement is always going to happen at the registrar level.

So whether it means, k a proxy service, you know, having its service taken away from it or forcing the public reveal of data in Whois it's ultimately sort of always there's a registrar touch point there.

And so we're kind of keeping that in mind and thinking about, you know, what's the most reasonable way to implement something with that kind of a - I don't want to say a choke point but, you know, it sort of is. Maybe that's the pejorative term, maybe it's the access point, let's say.

So, you know, what we kind of came to was this notion that we want to be able to apply the rules, you know, in a way that's efficient. And so, you know, to us what comes to mind is that, you know, we're thinking we should be applying the rules that come from this program really, you know, through the sales and contracting chain.

You know, we think that that would allow for, you know, the sort of notion of self-policing or self-enforcing or maybe more likely registrar-policing, registrar-enforcing sort of a compliance regime that can really be backstopped by ICANN's compliance enforcement program.

And that would be consistent with sort of the, you know, the status quo; what we're currently doing in terms of enforcement frameworks like as an example, the way resellers are accountable to their registrars and the registrars are accountable to ICANN for, you know, potential noncompliance by the reseller.

And so that's sort of the conclusion that we came to. And, you know, it occurred to us, you know, meaning all of us, in talking to Mary and Marika and of course Amy and I, you know, that might not necessarily be the way that the working group was, you know, sort of - they may not be operating with that assumption, there might be kind of an assumption that what we were really thinking was this could be a, you know, anybody comes to ICANN to be accredited as a proxy or privacy service the way they do to become a registrar.

And, you know, while we're not necessarily opposed that it seems like because there's this registrar access point for every, you know, possible, you know, interaction that might happen with proxy or privacy service it seemed to us that really the more streamlined, the more efficient approach is, you know, that we come up with policy that could be implemented the way any other policy would.

And that it becomes incorporated in the registrar accreditation agreement, becomes binding on registrars and then it becomes really about registrar enforcement of how they interact with their privacy and proxy services that they choose to do business with.

And then to the extent that the registrar is not, you know, started enforcing any obligations that would come from this program on their privacy and proxy service that they've approved, you know, been that could potentially be an enforcement matter for ICANN.

So anyway that's kind of the - that's kind of where we sort of have been. And, you know, I don't want to create, you know, a perception that this is our, you know, done deal, this is definitely the way we're going to do it. It sort of, you know, this is kind of, you know, where our mind is right now and there some other considerations that we, you know, had about this that we'd be happy to, you know, talk to you.

I think having said that...

Don Blumenthal: Mike?

((Crosstalk))

Mike Zupke: ...there's probably some people who would like to ask some questions now.

Don Blumenthal: Yeah, I was just - you've raised some interesting points right there so I was going to suggest may be taking questions okay now.

Mike Zupke: Yeah.

Don Blumenthal: All right. James.

James Bladel: Hi, Don. This is James speaking for the transcript. And thank you, Mike, for presenting that. And, you know, I can see that you guys have put some thought into this and I think, you know, what you're saying makes a lot of sense.

However I would just maybe caution - put a little bit of caution on this a little bit about the idea that this is closely linked to registrar accreditation; that privacy proxy services are closely linked to registrar accreditation.

I think that one potential - and I'm not saying this is economically or commercially desirable or not, I don't know, but I mean, one potential outcome from this program would be the concept that does not exist today of an independently accredited privacy proxy service provider that may be is affiliated with multiple registrars or none or is a reseller.

So I just - I want to just maybe push on the brakes a little bit about the idea that this should be handcuffed to the accreditation - registrar accreditation

program and maybe look at it more as a model of what could be done as opposed to a, you know, a required linkage between the two.

That's just my off-the-cuff reaction, otherwise I think this is good stuff, I just wanted to put that in the discussion. Thank you.

Mike Zupke: Thanks James. So this is Mike again. And, you know, kind of to respond to that, you know, I think I'm understanding what you're saying. And, you know, I also, you know, I don't mean to create an impression that we think only registrars could operate, you know, a proxy were a privacy service, you know, in the future under this sort of, you know, regime.

You know, we are more thinking about, you know, suppose a proxy service is put out of business by ICANN for noncompliance. You know, in order for us to transfer those customers to another proxy service, assuming that that's possible, assuming there's no proxy service that will take them, you know, we don't do like we normally do for a registrar failure where we, you know, tell a registry move all these domain names to another registrar and there seems to be kind of a clean, you know, bulk process.

What happens instead we're talking about, you know, going to a registrar and saying no you need to pick out all of these, you know, domain names that are affected by this which we, you know, we may or may not, you know, even be aware of. And say now you need to somehow transfer them to some of the registrant of record.

And that might be one under the registrar's control or it might be some other third party. And, you know, if we sort of follow the way that we've done these transitions in the past, you know, there's the potential that ICANN may end up having to choose a registrant through some competitive process and that might be somebody the registrar would prefer not to do business with.

And, you know, and so, you know, we're kind of mindful on this notion of, you know, how can we do this in a way that's also sort of not disruptive to, you know, business practices that exist in the marketplace, you know, as we know it. And so I think, you know, if we were to do this right I think you could still have, you know, the players who, you know, we sort of expect in this business, you know, can continue - or would be able to be a part of it.

So I think resellers can still do it and I think, you know, if you're just some third party proxy service - and I think there might be a couple who are out there who are probably affiliated with registrars but also make their services available to others.

And I think, you know, I think the notion isn't that they have to be tied to one registrars but I think that there would need to be some agreement between that proxy and whatever registrar they're doing business with so that there can be some meaningful enforcement.

I think about it especially with privacy services where the privacy service is not the registrant of record and so if they determine that they need to reveal data in Whois because that's required by the program, they might not have a mechanism to do that unless they have a relationship with the registrar because it's really the registrant who's controlling what goes on and who isn't.

So, you know, that was sort of a technical limitation that we were thinking about that kind of, you know, sort of puts a wrench in the general notion that anybody can come along and do this.

But anyway, you know, like I said I think I understand what you're saying and I think we can, you know, continue to work on sort of refining the approach to make sure that it, you know, sort of accounts for that.

James Bladel: Thanks, Mike.

Don Blumenthal: Thanks, Mike. Volker.

Volker Greimann: Yes, thanks Don. I think Mike has touched on a very important topic that we have discussed yet so far. And that's something that we should bear in mind going forward which is what happens when this actually the accreditation is terminated.

And I would like to point out that amongst our resellers we have resellers that do business with multiple registrars but have one privacy service for all registrations that go through them. So having just one registrar having to deal with this may not even be sufficient for all registrations of a certain entity that is being deaccredited.

So because there is independent providers that may be doing business with multiple registrars, having this linkage to what the registrar actually has to do in there in our policy is critically important to ensure that privacy services are carried forward when a service is deaccredited on the behalf of the - so the registrant remains protected.

Mike Zupke: Thanks, Volker.

Don Blumenthal: Great. Okay, Kathy.

Kathy Kleiman: Great. Thanks. Can you hear me, Don? Okay. Mike, thank you and Amy as well. So let me ask the question of protecting registrants is a good one; it's one that the working group has talked about at length, although we haven't kind of come up with exactly what to do.

We've been talking about the disclosure or the inadvertent disclosure of registrants during transfer periods so if you're trying to transfer a proxy domain name from one registrar to another how do you keep that protection during that transfer process.

But let me ask you, you know, I think - I've been doing a lot of antitrust work in other areas recently, I think we have to be careful not to dictate business plans of the future now.

What if proxy privacy providers, I mean, what stops us from treating them like resellers, you know, as Volker mentioned, I think, and bringing them kind of through either contracts directly with ICANN and/or contracts directly with the registrars but allowing them some of their independence because we may have proxy privacy providers that emerge in the future that are not registrars, that are just offering that service.

So why is that a problem? And let me ask you a question whether you've thought about escrow and whether you think we should be thinking about escrow of the proxy privacy data so that if there is a problem and a registrar folds or a proxy privacy service provider folds we can - ICANN can recover that data. Thanks much.

Mike Zupke: Kathy, so, yeah, so I think there's some good points in there. I think, you know, I mean, the point about not sort of foreclosing, you know, potential future ways of doing this is well taken. You know, and we're very conscious of that.

You know, on the other hand, you know, I'm sort of aware or at least my impression is that, you know, this group's, you know, primary concerns were how do we create, you know, sort of uniform, you know, minimum standards for privacy and proxy services, you know, that'll be good for registrants, it'd be good for other stakeholders.

You know, really, you know, this wasn't about trying to create new market opportunities. And so, you know, we're also not trying to force that either. This isn't, you know, I'm not trying to build up a new department within ICANN where we can have thousands of new contracted parties just to, you know, create employment.

But, you know, so I understand. I think that there's a bit of a fine line between allowing for future developments and, you know, sort of disrupting what's a fairly well-functioning or fairly competitive marketplace already let's say.

You know, and I think - but I think, you know, the way that resellers are sort of addressed by ICANN is, you know, currently - it's not directly but it's through the registrar accreditation agreement and I think while, you know, while people may have differing views on this I think that the 2013 Registrar Accreditation Agreement is, you know, really a long way toward, you know, making sure that everybody is kind of on the same page in terms of understanding that relationship and also making it meaningful and enforceable.

So, you know, I think it's possible to address, you know, most of the people who are already in this, you know, sales chain who are probably already in the, you know, business model through, you know, a consensus policy that kind of gets pushed down from registrars to resellers or to, you know, proxy services.

Obviously there's still a lot, you know, details to work out and that. But I think at least conceptually, you know, we addressed most cases. And I think, you know, to me I just - I don't, you know, I don't - and maybe I'm just limited but I don't see a way for a proxy service or a privacy service to do business with a registrar without really having some, you know, form of agreement between that service and the registrar.

It's just, you know, the obligations on both parties are so closely intertwined I think there just kind of has to be. And that's partly why I'm, you know, in favor of looking towards this notion of kind of a traditional consensus policy instead of a brand new accreditation regime with applications and everything that would, you know, basically create standalone accreditations. But so that was

- so I think I sort of addressed your first point. And part of it, you know, part of it is I think it's kind of just to be determined.

And then I think the second point is about escrow. And so, you know, this is - so it's not something that we have an answer for today. In my mind the way I would, you know, personally like to see this sort of unfold is that the way I think a lot of proxy services currently are working and that's if they escrow the underlying customer data through the registrar - through the registrar's escrow agent as required under the RAA.

And I know that, you know, registrars who are running their own or have an affiliated proxy or privacy service should be doing that under the 2013 RAA. I don't think the resellers' privacy or proxy services are necessarily addressed by that and I think that's where there's probably more work to be done. But, you know, in my mind that would be an ideal path; it would be the - sort of the simplest implementation from the ICANN perspective.

I have heard from, you know, some in the community they say well, you know, a reseller might not necessarily want it's registrar to know who its customers and, you know, while I, you know, I take that point, you know, most customers, through resellers, are known to the registrar. And, you know, I don't hear a lot of complaints about registrars actually ticking of their clients; that's bad for business.

So I'm not, you know, I'm not sure whether that's a real consideration. I'd be, you know, I'd be interested to hear from, you know, maybe registrars either on this call or, you know, as we kind of continue toward implementation, you know, their thoughts on that issue.

Don Blumenthal: Appreciate that, Mike. As Kathy said in the chat, very helpful. Volker.

Volker Greimann: Yes, just three points. One is that we will - we don't have, as a registrar, contracts with the privacy proxy services that we're not affiliated with so channeling this through existing contracts is simply not possible.

In many cases we don't even know who the privacy service provider. We see an address that's provided by a reseller. That might be a service that's provided by the reseller, it's might be a service provided by a reseller of a reseller, if might be an independent service that the registrant has contracted independently or as a registration.

In some cases escrow, was the second point, might not be possible because the registrar might be in a position where the would be required to share his - any data that the government wants with his government therefore the sharing of private data might be a data protection perspective be something the reseller who is in a - would be in a regime that has stronger data protection mechanisms, might even be prohibited from providing to that registrar.

So the privacy proxy service provided by the reseller might serve such purposes of protecting the private data of the registrant.

And the third point, a bit offside but some registrars, not us but some registrars, charge for other things than what ICANN charges; for example, ownership updates, updates to the Whois data.

And if such a registration is with such a registrar there would have to be some consideration for the cost that is charged by that registrar to his registrant. If a privacy proxy service change required amended by ICANN would incur costs that the registrant has not foreseen at the time of the registration.

Mike Zupke: Thanks, Volker. Yeah, I've actually got a question for you as a registrar. And, you know, I realize I'm putting you on the spot here so feel free to tell me you're not prepared to answer. But, you know, how would you feel about an

arrangement where, you know, the - let's say your reseller's proxy or privacy service could either, you know, provide the underlying customer data to you as the registrar or they could enter into an escrow arrangement with either registrar as the beneficiary.

And I'm thinking because really ICANN has no use for the data. It's not like we can just give it to another registrar, it's really, you know, your registrar as the, you know, as the sponsoring registrar is really the only entity who has any use for this data or another privacy or proxy service might.

But, you know, is that something that, you know, registrars find feasible is having escrow arrangements with their - either their resellers or their privacy or proxy services they choose to do business with?

Volker Greimann: Well I would have to mull that over. But like I said in many cases we don't even know who the privacy service provider is and who is affiliated to so putting us in the situation where we might have to conclude contracts with parties unknown to us that we don't choose as our customers but that happen to be a service provided by - chosen by the registrant.

Having to have an additional check like that in place might be cumbersome and not something that we would like. But I would have to see suggestions to that effect how that would look like to analyze that deeper.

Mike Zupke: Okay. Thanks. You know, and I'm just kind of thinking, you know, the model probably looks sort of like what the current requirement is in the 2013 RAA so there's this idea that, you know, registrars can't knowingly accept registrations from a - I'm saying this backwards. If they, you know, if they offer through their sales channel a privacy or proxy service, you know, they're required to follow the requirements set out in the spec. And it doesn't necessarily apply to resellers.

But, you know, I imagine we could have a, you know, we could have a contractual requirement through consensus policy that says registrars contracted resellers are only allowed to use, you know, a privacy or proxy service that does the following things like, you know, either escrow their data or give it to the registrar.

Volker Greimann: Like I said, the problem here being that in some cases, for example, a European reseller would be very hesitant to provide underlying data that is not public in the Whois to an American registrar which would be a competitive disadvantage for the American registrar because the American registrar can always be asked by its government to share that data with them and so therefore not making them a safe haven, not being eligible to receive that data.

And that may be a problem that will have to be looked at from data protection perspectives.

Mike Zupke: Okay, thank you.

Don Blumenthal: James.

James Bladel: Hi, Don. Thanks. James speaking for the transcript. And just as kind of a side note or a footnote to this conversation, on behalf of myself and Kathy and Susan, the idea that this problem or issue would be tackled via an accreditation program for privacy proxy services and not, you know, a separate consensus policy was born out of the Whois Review Team.

And I guess I think it was not really ironclad; it said it was one possible way of approaching this issue. But it would just maybe put into the conversation that if we are going to turn away from an accreditation program and move towards a binding consensus policy on existing contracted parties that we should do so within this working group and not - and please don't take this the wrong way - but not as a - that decision should not be made by staff.

And I'm just pointing that out because that was a community decision that kind of gave birth to this idea and we have to kind of have the community undo that decision if we're going to move it back into a more traditional framework. So I'm just putting that out there as something that I think this group should consider. Thank you.

Don Blumenthal: Thanks James. Appreciate it. Michele.

Michele Neylon: Thanks. Michele Neylon for the record. A couple of things. Volker touched on some of the stuff with respect to some of the data privacy concerns. I mean the problem we are talking about - anything involving privacy and ICANN is like a red flag to a bull. At present, ICANN does not have a comprehensive privacy policy nor does it have a privacy officer even for its own internal stuff. So the very concept that the underlying data that is being provided to a privacy proxy provider could be escrow scares the hell out of me.

At present, the entity that handles the bulk of data (scroll) for ICANN accredited registrars is (unintelligible) which while they are big enough and ugly enough to have datacenters in multiple jurisdictions haven't bothered and all of the data is being escrowed only to the U.S., which is problematic. Other companies offering data (scroll) have no way of being given the same access to registrars and their data because the reasonable process in place at present within ICANN to give them a fair whack at that service. So that really does need to be addressed. If data were to be escrowed, that's fine, but as a registrar based in the European Union, I would want my client's data to be escrowed within the European Union. And for the love of God, please don't say Safe Harbor because we all know that that's not going anywhere.

The other thing as well is with respect to some of the points that James rose and others have touched on as well. I mean there is a lot of this that has - is tightly interweaved with registrars and their reseller's business models. I

mean the reality is that if I wanted to theoretically completely screw with eth system, I could set myself up as a reseller of a registrar and simply register all domains for all of my clients with my details and effectively act as a “privacy proxy service” and there is nothing that the registrar could really do about it.

So a lot of these kind of finer details I think need to be flushed out and I think you know ICANN staff at this point really needs to engage with us and have some kind of meaningful dialogue moving forward. Thanks.

Don Blumenthal: Thanks Michele. Your points are well taken and just one - since we are on the record, I just want to clarify one thing. We have kind of had these conversations before so mostly for the record. You know I was sort of envisioning that registrars can set up their own escrowed arrangement with you know privacy or proxy service that they want to do business with. But you know with regard to the registrar data escrow program, you know you are correct that you know (unintelligible) mountain because that’s a service that ICANN pays for, but you know there is a registrar that pays option available that you know registrars can use and some do mostly because they have you know these very you know privacy law concerns that you cited.

Michele Neylon: Michele coming back to you on that. Yeah but the thing about that is that that’s not a fair and level playing field. Because by forcing registrars who want to protect their clients privacy and have the option of escrowing the data within the European Union or elsewhere, we are being put at a competitive disadvantage to registrars who don’t have such concerns. That’s something I think that does need to be dealt with.

Don Blumenthal: Thanks Michele. Understood.

Don Blumenthal: Okay, we are at a bit past 10:30 here and I guess I kind of lost track a little bit. Amy did you have a separate discussion or you and Mike working together? Is see you listed as a presenter and that’s why I am asking?

Amy Bivins: Yeah at this point I was just here to field questions as needed.

Don Blumenthal: A step back form (unintelligible) okay. Well we are about halfway through which is pretty much we had allotted for this. I want to just make sure. Double check if there any additional questions now. There has been (unintelligible) here that we hadn't quite anticipated as we were going forward, so I want to make sure everything is covered before we move back to our regular discussion.

Okay, not hearing or seeing anything. Really appreciate your help Mike. Like I said, a help in general but also some interesting new wrinkles here that I don't think we had considered so far, so this gives us a lot to consider as we move forward in framing what we are talking about.

Mike Zupke: Well thanks Don and thank you all for your time. And I just want to also add that Amy and I will be in Los Angeles when you meet again, so you know that might be a good place to meet you again if you've got you know follow-up questions or you know if we could get more input from you. We would be happy to do it then obviously sooner if it makes sense.

Don Blumenthal: I think you can count on at least some of us finding you if you are not fully visible. I appreciate that.

Mike Zupke: All right thank you.

Don Blumenthal: Okay lets I guess move back to - and I see the screen changing here. Back to framing - I am using that word a lot. Back to looking at the issues form last week. Just a second please. Sorry, major throat clearing there. (Unintelligible) some common terms that we've discovered that have been sent to us. We thought it would be useful to send around and I guess it did go to help come to some conclusions as much as we can on just your basic baseline issues.

What we would like to do if we can is finish up that discussion today and then move on to some of the considerations.

My turn to - okay I am going on mute a lot. I want to just I guess at this point throw the discussion out on two levels. And I wasn't on the call, but I did listen to it to see if there any follow-up based on what was left unsaid or new thoughts from last week's discussion or (unintelligible) that this common contractual terms, so this might help us flush out our discussion. Flush out a strong (unintelligible) type approach like Volker did in our earlier discussion to create a model that we can really work with in advancing the discussion.

And that was (unintelligible) and quite broad, so I hope I didn't leave it too wide open. I mean it sounds like - sorry about that. Let me ask you this. Based on this last week, are there things we should focus on first to make sure that we have this solid baseline. There were a lot of discussions about - a lot of talk about what proxy privacy providers could do versus should do. And I am curious if people who were involved in that conversation - I don't want to call anybody out. I have considered it further in terms of trying to distinguish the could versus the should which would be the baseline.

Okay help me here folks. I was hoping to avoid just going down the list here, but (Steve) thank you.

Steve Metalitz: Yes hi, this is Steve Metalitz. Just two observations. First on the document that (Mary) circulated. I think that this really goes to publication more than to disclosure because it talks about the circumstances under which currently some of the services are terminating or have the right to terminate their customers. So it is obviously quite relevant to publication because that is the result of terminating the customer out of the service. The customer's contact information would become available through Whois.

So disclosure might have a different standard. It is a narrower remedy if you will. If it doesn't make the information available to the world, it makes it

available to a party that has complained about abusive behavior. Let's say that.

Second, in the discussion last week, what I came away with is a couple of conclusions about - again about describing the status quo. One is that these decision about disclosure are not automated. They are done on a case-by-case basis. The providers look at the requests that come in. There are some exceptions to that. You know if it is an anonymous complaint or something like that, but in general, they are looking at these.

That there is some - they - in the discussion last week, were weren't really able to articulate what standard they apply or at least I didn't think there was a standard articulated as to what they apply for deciding when to disclose and when not to disclose in response to such a request.

I think there was a sense that I think Kathy's phrase. A mere allegation is not enough. There has to be some evidence or some assertion. You know some details backing up the request, but again, not clear what those you know would be.

And I am - I was struck by the fact that it would be helpful to have an articulation from the providers as to what they think the standard ought to be. What level of evidence ought to be provided before they would agree to disclose this information in response to a complaint about abusive behavior? So I am - I think it would be helpful to have a straw man or a proposal on that from the providers and I think I would agree with you Don that that was - it was very helpful when Volker did that in the relay context. And I think it would be helpful to have something like that here in the disclosed context. Thank you.

Don Blumenthal: And I am not pointing at anybody in particular of course. Kathy.

Kathy Kleiman: Let's see. I think Steve's summary of last week makes sense. Steve raised a question about something in the chat so we will have parallel conversations going on. I just wanted to - somebody said something and I just wanted to respond on a very narrow point, which is that, the termination of a customer's privacy proxy service.

It is my understanding based on our discussions in this working group that it does not necessarily mean publication. That there may be other options under the terms of service that a proxy privacy provider has chosen including takedown. So and this goes back to what we talked about several months ago. So I wanted to raise that and make sure that we talk about that as - it is in the notes but not necessarily in the main body of the text. What happens upon termination of proxy privacy? You know what happens when someone is found - when there is an issue of disclosure and publication and what other options there might be.

That was not very articulate. Thanks. Bye-bye.

Don Blumenthal: I think I caught up towards your end there and I think we have discussed the issue of whether a registrant - a beneficial registrant. I am not sure which term (unintelligible). We have an option of either - of pulling the (registry) rather than full disclosure but I don't think we've come to an agreement on that. Michele.

Michele Neylon: Well thanks. Yeah I think you know if you are terminating the service the you are talking about terminating the Whois (unintelligible) service so that would lead to publication of the data. I can think of a multitude of situations in which we would terminate the service and through that there was no way on earth that we wouldn't terminate the service because the domain name in question could be used for all sorts of interesting things which is leading to us being dragged through courts or God knows what else. So I mean I am not going to keep the domain "protected" by (unintelligible).

As for the termination of the domain name that opens up an interesting can of worms. The privacy proxy service may or may not be contracted at the same time as the domain name is registered or transferred. And you know if from the business perspective if we are selling the privacy proxy service for a nominal fee, I am getting into kind of messy kind of things about what to do with the domain name and offering people options and everything else. It just sounds to me incredibly messy.

I wouldn't want this group to force providers to go down a particular route unless it is in our case we would just keep it at the simplest level. But if somebody is offering a service - some kind of super-duper gold plated service and is being paid real money for it, then they might want to offer other options. But I don't think we should be the ones to decide that. Thanks.

Don Blumenthal: Okay just some clarity. I think when we are talking about terminating the service here we are talking about terminating the services to a particular registrants and that accompanied (unintelligible) by the same proxy program.

Michele Neylon: We are talking about removing privacy proxy on a domain or domains only.

Don Blumenthal: Right. Just want to clarify for this discussion because we have addressed the other possibility I mean in our calls. James.

James Bladel: Hi, James speaking for the transcript. And I want to go back just a couple of steps maybe to the comments from Steve. I don't want to shoot too much from the hip but our service provider does have a standard procedure including documentation, submission requirements and I think that can be an excellent model that can probably be used in other jurisdictions as well.

I will circulate that to the list, but in general, it involves submission of evidence of the infringements from the third party rights like you know a screen shot or a link to the infringing content and then some you know - also evidence of registration of the trademark whether it is a link to USTCO or

some other service or registration number or something like that. And then usually you know those two things coupled with a you know - I don't want to say an affidavit but some sort of a statement on the behalf of the claimant that they believe all of this to be true, then we would usually take action the privacy customer either by disclosing the name or by canceling the service depending on the severity of the infraction.

So you know I am kind of shooting from the hip here a little bit. This is a complicated question and the answer is equally complex. And I will circulate a link from our existing terms of service to the mailing list and maybe that will get us something to push off on. Thank you.

Don Blumenthal: Okay yeah that would be really helpful. You know concrete things - definitely useful. I just want to address something you raised in the chat. I guess where we - what we have discussed is whether a beneficial registrant should be given an alternative of we are going to publish or you can (unintelligible) domain (unintelligible). And I guess the issue is there sort of (unintelligible) process acquiring disclosure for publication with giving the domain up in effect. Meaning that the registration details (unintelligible) published. And we talked about it but I don't think we've come to a conclusion on whether that alternative should be provided, but it is out there as a possibility.

And I am just checking the - James.

James Bladel: So building on that, maybe what would be helpful for this group to define would be some sort of an escalation task. So for example, there is - I think we understand that disclosure to a single complainant is probably less impact than publication, so I think we can put you know -and you know I am just envisioning off the cuff you know one discloser being the first step and then disclosure being an escalation step for being a more egregious type of (unintelligible) for (unintelligible) behavior. And then you know understanding how you get from one to another. How you get from a misdemeanor to a felony you know sanction. And then also I think

what we could discuss is giving - what are the registrant options. Well the registrant and/or privacy service customer. What are there options? Do they have the opportunity to cure if they receive a complaint? Is there a window where they can say look I need to infringe on this. I thought it was (unintelligible). I am going to take it down now and therefore my privacy details remain intact.

Or you know do they have the ability to cancel the entire registration before their name is disclosed or published. So I think you know it might be helpful for this group to work on what we believe to be the - kind of the graduated sanctions and what the possible actions on behalf of the customer might be and lay those out, and I think that might help us navigate some of these questions. Thanks.

Don Blumenthal: Thanks James. (Unintelligible) for a field (unintelligible) that we would focus on baseline issues but these are things that we will - I agree. We addressed but we have to address more formally. As (unintelligible) suggested (unintelligible) and we do circle back quite a bit and I don't want to go back over old ground too much. (Unintelligible) back and forth and sometimes it is hard to remember exactly what we (unintelligible) or didn't. Steve.

Steve Metalitz: yeah, this is Steve. I think those are useful suggestions from James and I think that it - I am happy to start with the intellectual property areas, copyright and trademark, but we do need to be aware that there will be other kinds of abuses. And at some point if we are coming up with the standards and the evidence and escalation and so forth we will need to kind of - I think we will need to bring in perhaps those who are more familiar with other kinds of abuses besides the copyright and trademark infringement. So it is just kind of a marker here that it would be great if we could come to agreement on - in those areas but that might not be the whole picture that we need to address. But I am looking forward to seeing you know the (unintelligible) James is going to circulate and see what ideas - further ideas he has on that. Thank you.

Don Blumenthal: Okay I appreciate that Steve. I was having trouble during the - my mouth (unintelligible) on the unmute button. I am just checking the chat. You know I just want to (unintelligible). I just want to (unintelligible) specific - your specific (unintelligible) categories because they are definitely not going to translate across jurisdictions, but there are some kind of guidelines. (Unintelligible) useful and (unintelligible). Now (unintelligible) is what we are looking at to try to come up with standards that are useful under legal frameworks around the world whether it is privacy frameworks or just how we are defining what specific types of behavior should be part of the publication considerations (unintelligible).

(Unintelligible) and just making sure okay. Well we didn't - like I said, we didn't get to the baseline issues but we have covered a lot of important things that will be a part of it. I think it might (unintelligible) and Amy raised some really interesting possibilities and (unintelligible) consider. And I think we really need to spend some time thinking about as I mentioned in chat. I am going to try to pull together some - to address one question and pull together some names of unaffiliated privacy proxy providers.

I think (Christina) mentioned that point too so if you have some (unintelligible). You know I work in the abuse (arena) fairly heavily and I think that (unintelligible) frequently fill up in that context, which means we probably should mention any of the ones I know because people might draw conclusions.

Let me just throw it out here. I mean we are at what two minutes of. Let me see if there are any final comments and maybe wrap the call a minute or so early to make up for all of the times we run over.

Sorry I just threw myself back on mute there. Okay let's give it a second and see who else is in chat here before shutting the room down. But when we end the call and - a lot of good stuff here today. Move forward next week hopefully with some straw concepts which the (unintelligible) promised to send out and

then build on what we've kicked around. Thanks for your time and talk to you next Tuesday.

END