GNSO Working Group on Privacy and Proxy Services Accreditation Issues
28 May 2015

Mary Wong: Hello, everybody. And welcome to this webinar which is being presented by the interim co-chairs of the GNSO's Working Group on Privacy and Proxy Services Accreditation Issues.

You'll notice that in the chat pod Nathalie has put in a few instructions and pieces of information that we hope will be helpful. Particularly the fact that we have muted everyone's mics for the presentation portion and that we will unmute the mics at the end for the question and answer.

As I said earlier to those of you who came in early, it would be helpful if you are in Adobe Connect, if you're not yet and you're just on the audio bridge because we do have some slides that might be helpful in following along.

The slides as well as the transcript and the recording of this webinar will also be made available on the Website shortly after today's webinar.

So on that note I just want to welcome you all on behalf of the interim co-chairs, Steve Metalitz, and Graeme Bunton, as well as this GNSO PDP working group. Several of these members are also with us here in the Adobe Connect room. And I wanted particularly to recognize Don Blumenthal who was our chair but had to take a leave of absence. And, Don, we're very glad you're able to be here with us today.

On that note then I'm going to hand over to Steve and Graeme. And, Graeme, I believe it's you who's going to kick us off today.

Graeme Bunton: Thanks, Mary. Indeed it is. And let me echo those thanks yous very briefly. I appreciate everyone that's attending today and members of the working group especially and staff as well for all their hard work and especially that nod to Don Blumenthal who guided us through some dark and murky waters over the past year and a half or so.

So here's how this is going to work is that Steve and I are going to be sort of switching off sections as we work through the slides. We expect that's going to take about 30 minutes, maybe 35 or so, and then we should have plenty of time for questions at the end.

So let's get going. We're going to give you a bit of background first. This PDP came out of the 2013 RAA. There's a interim specification in the RAA that governs how privacy and proxy services should work and it also has an expiration date of January 1, 2017 meaning the work we're doing here needs to be completed by that date or the interim specification drops.

The sort of enforcement stick for compliance to ensure that any accreditation regime is followed is that registrars would not be able to knowingly accept registrations from an unaccredited privacy and proxy service. And so that's insurers that registrations using them are accredited.

The date that the bottom there are useful to note. The Council chartered this working group in October 2013. We've done about 60+ meetings since December 2013. And we published our initial report on May 5. And the public comment period with open for 60 days and I think closes July 7, someone will correct me on that one. So that's what got us going and got us to here.

There is a considerable amount of other work that this working group look at as we move forward, the Whois review team, Expert Working Group, a

number of different studies. And we also have representatives in this working group from a number of different stakeholders.

And we also have representatives in this working group from a number of different stakeholders, so all of the constituents of the GNSO, we have members of the At Large/ALAC, law enforcement and GAC and a number of individuals as well which has been exciting because it's been a very diverse group with lots of different interest.

So we're, I think, going to move on now from that background to some preliminary recommendations and the remaining open questions so this is the meat now of the - of this presentation. And I think I'm handing off to Steve to get us going on some of the stuff that we've all agreed on up to this point and then we get into some of the contentious questions a little later on.

Steve Metalitz: Yes, thank you, Graeme. This is Steve Metalitz. And thank you for kicking off the webinar. And thanks also again to the staff and all the working group members. We had a very diverse group as was suggested in that previous slide. And a lot of disagreements and strong debate but we are - were able to reach consensus on a number of charter questions.

And I think hopefully to frame some of the other questions in a manner where we can meaningfully get some public input from the rest of the community. And that of course is what's due July 7 as Graeme noted in his introductory remarks.

In terms of the initial report while it is 98 pages, perhaps we can make it a little bit more digestible by referring you to the executive summary first which lists all the preliminary recommendations and the major open questions.

Obviously we are interested in comments from the public on any aspect of this report but that may help to orient you to some of the major questions that were discussed and are still open. And that really is about a 17 - well it goes

to Page 17 so it's much shorter document, Pages 3-17. And that can give you I think a pretty good orientation to the whole process.

I'll call your attention to two annexes to the report which we will talk about later in this presentation. First in Annex E there's an illustrative framework for handling disclosure requests from intellectual property rights holders. And as we'll discuss then we intended this as kind of a template or an illustration of how these requests for disclosure of information on customers who used a proxy service or a privacy service is intended to be illustrative. We're welcoming comments on it. We also recognize there would be a number of other instances where similar frameworks would need to be constructed.

And then on Annex F one issue on which we were not able to reach a consensus was on permissible uses of domain names that were registered through a proxy or privacy service and in particular whether they could be used for financial transactions. So we'll get - again, we'll get to that later but Annex F gives statements from two groups of working group members with diverse perspectives on that unresolved question.

Let me turn now to the general recommendations and these are the ones on which we had general agreement within the working group. First, we were able to build on definitions of privacy service and proxy service that were found in a lot of previous ICANN work, particularly the Whois - some of the Whois research that's been done over the years.

So this was the - were the two definitions. We did ask on each of the points that we'll talk about today is there a need for a different accreditation standard for a proxy service or for a privacy service. In other words whether all or just some of the identity information on the actual registrant or the customer is masked.

And we weren't able to find any place where that distinction was needed. So we basically recommended that proxy and privacy services be subjected to the same accreditation standards going forward.

We did have to come up with some new definitions. And we had some difficulties with some of this. And we found ourselves even confusing ourselves when we referred to reveal or relay so we decided it was probably important to really kind of spell that out. And you'll see the definitions in the executive summary on Pages 6 and 7.

Basically relay is the question of forwarding electronic communications to the privacy proxy customer from a third party which could be, you know, could be law enforcement, could be - it could be an intellectual property rights holder, it could be simply someone who wants to be able to communicate directly with that customer.

Then reveal we concluded there really are two species of this. One is disclosure where the contact points for the privacy proxy service customer is revealed only to a third party that requests it. And that's where we worked out some proposed more detailed standards.

And the other is publication basically that information becomes public, it's published in Whois. Another way of putting this is that someone becomes ineligible for the privacy proxy service that's offered or that service was terminated that we're calling publication so we're trying to distinguish between those two things.

And then law enforcement authority, there are several references to this in our charter questions. And we decided to recommend that the definition that's already contained in the 2013 RAA be used for law enforcement authority. Again, those are laid out on Pages 6 and 7.

And then if you continue we have some other definitions and areas of consensus or general agreement within the working group. First that basically anybody should - the situation now is that anybody can use a privacy or proxy service if the registrar offers it. And we thought that that should continue, in other words, commercial organizations could also have a legitimate need to use a privacy or proxy service.

But it gets more complicated when you talk about how those services can be used or how those domain names can be used and that's addressed in Annex F and we'll talk about that later on in the presentation.

Some other areas of agreement that it should become clear when you look at a Whois output, whether it's a privacy or proxy registration, and we recommended some ways that could be done. That's an implementation issue.

The third bullet here I think is quite important and that was that the customer information for privacy proxy services should be validated and verified in the same general way as non-proxy registrations are done under the Registrar Accreditation Agreement and particularly the Whois accuracy specification.

And right now there isn't any such requirement but this was commanded general support. And today of course all of these services or most of these services are affiliated with registrars so we have that provision in there that says if you've already verified this information as a registrar you don't need to do it again with your hat as a proxy service.

But this is an important aspect of it. It increases the likelihood that if there is a reveal of information, a disclosure or publication under the accreditation standards, that that information will be accurate.

We also talked on Pages 8 and 9 of the executive summary about some provisions that should be included in the privacy proxy service terms of

service. The interim specification calls for some of those terms to be published now but we went into some more detail about things that should be spelled out in the terms of service so that customers know the grounds on which their information might be disclosed or published, the terms and conditions under which their service might be terminated and basically what their rights and responsibilities are.

And then we agreed on some best practices in areas where we weren't quite ready to recommend specific standards. But in particular we had a lot of discussion about how privacy and proxy registrations are handled in the transfer of domains from one registrar to another.

And we recommended some best practices in this area so that those transfers could take place and so that the privacy proxy status could be maintained to the extent possible.

Then the last area of general recommendations, which are kind of spelled out on Page 9-11 of the executive summary, and they're listed on this slide, Slide 8, some of these are building on the situation now with the interim specification so for example ICANN should maintain a public list of all the accredited providers with their contact information just as it does now with registrars.

It should become clearer than it is now when a provider is affiliated with a registrar and both providers and registrar websites should indicate that. We decided to recommend that providers have a designated contact point for receiving abuse complaints as opposed to a dedicated contact point which might suggest that this person could not be allowed any other duties but just someone who was designated to do this function.

And that these designated contacts be capable and authorized to handle these abuse complaints and we reference a standard that's been brought in under the Inter Registrar Transfer Policy.

And finally, we - while we didn't come up with a definitive list of the types of abuse or malicious conduct that should be handled by these contact points, we did refer to some indicative lists that already exist in the registry agreement, GAC safeguards and so these are already in place. And this would be a starting point for a more complete list of the types of malicious conduct that the abuse points should be capable and authorized to handle.

So I'll stop there and pass the baton back to Graeme who will talk about our recommendations and our open questions on standards for relay.

Graeme Bunton: Thanks, Steve. So Steve did mention the definition for this earlier but let's just refresh to make sure we know what we're talking about here on relay. Relay is about the obligations of a service provider to act as a sort of middle man for communications between third parties and registrants. And those third parties could be law enforcement or intellectual property or just someone who's interested in the domain or spammers.

And so we spent considerable time and energy on this question. And there's still an open piece that we'll go over. But we did come to some good preliminary conclusions here.

So the first one there you can see is that it's mandatory to relay or forward to the customer all communications required by ICANN consensus or the RAA. And so that's pretty straightforward, stuff that people need to get WDRP notices or what have you, have to be forwarded.

And then we have an option here that's up for discussion but let me come back to that in a moment. Actually, you know what, I changed my mind, let's go to that.

So service providers must either relay all electronic communications but can apply commercially reasonable safeguards against spammer abuse or all

electronic communications from law enforcement or third parties alleging abuse.

And perhaps the distinction between those two is a bit subtle but it's more about how a service provider sits in the middle and protecting their registrants from communications that they may or may not be interested in. But both require that law enforcement and third parties alleging abuse must be sent on to the registrant. And so that's a place that would - we would welcome some input into.

The requestor will be notified of persistent delivery failure of electronic communication so the requestor in this case is the person trying to communicate with the registrant through the privacy and proxy service.

They may not know if the delivery is failing between the service provider and the registrant so if a service provider is aware of a persistent delivery or failure they need to notify the original requestor that that failure has occurred.

And as would make sense in a persistent delivery failure the service provider must perform a reverification or validation for the 2013 RAA Whois spec. So if that email address is failing it's bouncing back, for example, and the service provider is aware of that then they need to reverify that email address.

So the big open question - there's a couple pieces in here and you can see the brackets in this text and I'll read through that in a moment. But we have some options here and how we've explored this and this is another place that would be excellent to get some feedback from in our public comments.

So the text reads as follows: "As part of an escalation process and when the above mentioned requirements concerning a persistent delivery failure of an electronic communication have been met, the provider should or must upon request forward of further form of notice to its customer."

So what this is saying is we have some text here to choose from - should or must - in whether the service provider is obligated to use a different form of communication to the registrant. And they may have alternate contact methods being the service provider, they may have email like different email or phone or fax numbers, something of that nature. And this is whether there is a obligation or a recommendation to follow through there.

The text continues, "A provider should have the discretion to select the most appropriate means of forwarding such a request and to charge a reasonable fee on a cost recovery basis or any such reasonable fee is to be borne by the customer and not the requestor. A provider shall have the right to impose reasonable limits on the number of such requests made by the same requestor."

So that last piece is just that, you know, a requestor can't send 100 emails a day or 100 requests a day to a registrant and the service provider is not obligated to send all of those through.

There is considerable debate about those two options earlier in that sentence around cost recovery. This comes from the potential costs in forwarding perhaps its physical mail from the - that's received by the service provider to go to the registrant which may have costs and it could be that the only other address that the service provider has is a physical address so then they're taking an email and printing it and packaging it and mailing it.

And we don't have clarity at the moment on who should bear those costs and if charging a fee is reasonable to recovery those costs so I'd encourage people again to have a look at that text and think about that and provide us with some insight please.

And I think that takes us to the end of relay. And I'm going to pass it back to Steve to talk a bit about reveal.

Steve Metalitz: Okay thank you, Graeme. I'm not actually in the room or maybe I'm getting back in the room now so I may have to ask someone to - or Mary to advance the slides for me. But we should be on Slide 11 now, recommendations, open questions on reveal.

As mentioned one thing that the group did - by the way this was an area that was probably the - one of our longest periods of discussion within the working group, I don't know exactly. And I seem to be back here so hopefully I can advance these slides.

This was an area of a great deal of discussion and consideration of different proposals so it's obviously an area that I'm sure the public should be looking at closely and its public comments.

We did come up with some definitions, which we talked about earlier and also some - a requirement that an accredited privacy proxy service had to disclose in its terms of service the grounds for disclosure or publication of the customer's information. And remember, disclosure is simply to a requestor with limitations on use; publication is general publications in the world.

Several people said - took the view that providers should offer an option when a reveal request is made that it may be more important for a customer to retain his or her anonymity rather than even retain the registration on which the - which was made under the privacy proxy service so in other words should the registrant have an option - customer have an option of either having a reveal take place or cancelling the domain name registration.

So, again, that was not made - we don't recommend that as a requirement but we do say that if that is an option then that should be disclosed to the customer in the terms of service.

Now there are a few general questions here which we'll get to but there's also an illustrative framework about disclosure requests from trademark and

copyright holders. And the reason we did this was to see if we could come up with a fairly detailed framework for one type of situation in which a reveal or rather a disclosure might be sought recognizing there are other situations where a disclosure might be sought for other types of abuse and so and so forth, law enforcement requests.

But we didn't have all those folks who had expertise in those areas at the table. We did have a good contingent of representatives of trademark and copyright owners, we had the registrars, we had the representatives from - of individual users and ALAC and so forth. So we felt we could go ahead and try to come up with a template on this.

And you'll find that template on Annex E beginning on Page 84. And, again, it's intended to be illustrative and your comments are certainly welcome on it. This slide runs through some of the main points. I would reference to begin with on Page 84-85 there's an explanation of what we're trying to achieve with this illustrative framework.

And really it's to strike a balance among three interests. One is from the viewpoint of requestors to have more predictability as to when they will be able to gain access to this information which if they need that to try to resolve an intellectual property rights dispute.

Second is to preserve a corporate level of discretion for service providers to act on these disclosure requests. And third is to include safeguards for the legitimate interests of the registrants or the customers so all those factor in here. And what you see in this annex is an attempt to balance among those three main interests.

I should also say there was a lot of discussion about - in contrast to reveal which in most cases is kind of an automated process and we tried to craft the standard so that it could work in an automated environment if a registrar chose to do that, there was a general consensus that reveal probably is more

- much more difficult to automate and there might need to be human intervention but - so the idea was to come up with this as specific set of criteria as we could.

This slide lists the main points of the Annex E framework - the detailed criteria of what should be included in a disclosure request and that's set out - it's a lot of pages, 86-90, but it's fairly repetitive for the different kinds of disclosure requests for trademark and copyright.

There's a listing of the steps for what the provider should do and within what time they should do it. That's on Page 90. There's a non-exhaustive list of reasons for not disclosing, again to preserve - try to balance the need for predictability in these requests and the need for discretion on the part of the service provider.

Including the service provider - if there is evidence of it the service provider could say, well you may have a legitimate intellectual property claim here but we think there's evidence that you're actually using this request as a pretext for some other reason to find out who the customer is. And I think from a privacy standpoint this was viewed as quite important to try to include that type of safeguard.

And then finally on Pages 92 and 93 there's some references to review or dispute resolution processes, what should be done if there is a situation where the contact information has been wrongfully disclosed or it's been misused by the requestor.

I will say that I don't think these are as well flushed out as other aspects of this framework. So, you know, we do welcome comments on this but this is probably an area where more work is needed. And we were very aware of the need not to encumber the process with a lot of complicated additional steps or ancillary processes so that's obviously a factor to be taken into account

here as well. But we hope this illustrative framework is helpful simply as an illustration and we welcome your feedback on it.

Then this lists some of the open questions about disclosure and publication more generally. As I said we had very little law enforcement participation in our working group and we recognize that that's an area that still needs to be filled in including in law enforcement it's sometimes necessary for a request for a disclosure not to be notified to the customer.

I should say that under our proposal in the non-law enforcement area the customer would always be notified of any request for disclosure. But in the law enforcement area obviously there could be other factors at work in the middle of an investigation so that's an open question.

It was - the issue was raised of whether there are some types of abuse for which publication, in other words, kicking the registrant out of the privacy proxy service should be mandatory for certain types of abuse or illegal activity. That's an open question.

As I noted remedies, if any are needed with this framework for unwarranted publication is an open question. Of course this all preserves the ability of any party to go to court where that's feasible but should there be any remedies within the framework here.

And then obviously there are a number of areas in the IP disclosure framework itself. And I'll just highlight one of them here on the next page which really has to do with a couple of - I'm not going to read through all this but there are a couple of different formulations about when - when the provider could refuse to disclose even when they're presented with a request that meets the template that's set out in the annex.

So I'd encourage you to look through those and express your views on that and really on any other aspect of the Annex E or the open questions on the preceding slide that you feel you can make some input on.

I think at this point I'm going to turn it back to Graeme for his next slide and then we'll get to the summary of the questions. Graeme.

Graeme Bunton: Thanks again, Steve. So this is a topic that has come up a number of times over the past year and a half within the working group and we've never been able to put it to bed. So we've spent lots of time here and energy and would love other people to put some more in there so we can hopefully make some progress further with this.

So this is all around the limits of use of privacy and proxy services. There are some working group members who feel that privacy and proxy services should be open to any and all registrants. Actually let me back that up for a second.

The status of a registrant is not important in this distinction. So whether they're an individual or an organization, a noncommercial entity, that doesn't preclude anybody from using a privacy and proxy services so that's open for everyone.

Where we did get into possible limitations is where domains are being used for financial transactions and whether they would be eligible for privacy and proxy services.

And so some members didn't think so; some members think that the privacy and proxy should be able - should be available for use for any domain regardless of what the domain is doing or what the resolved content is doing while others disagreed and suggested and the language is careful here that domains used for online financial transactions for commercial purpose should be ineligible for privacy and proxy registrations.

So that means they are doing transactions on that Website and those transactions are not for personal reasons but for commercial purposes. And that's important there because that, you know, tries to narrow the scope I think of who would be limited from using privacy and proxy registrations. Financial transactions for commercial purposes, asks Amr in the chat, I would think it would.

So I will point you - so I think some of this discussion happens on Page 97 and 98, the last couple - the last two pages of the initial report. But there is also two annexes submitted by members sort of describing different perspectives on this issue. And I would encourage you to go and read those and consider them and also include feedback on this question informed by those perspectives in your public comments.

So that's about where we are on online financial transactions and use of privacy and proxy. And then I think we go back to Steve now for a summary of all of the big open questions.

Steve Metalitz: Okay thank you, Graeme. There we are, okay. Yeah, very briefly what Graeme is referring to is if you go back to the earlier slide we flag Annex F as a place where the two groups of - starting on Page 94 where the two groups of working group members - there's no group put in a full position here but the two groups of working group members kind of laid out their views on that question for permissible uses so I'd encourage you to review that.

And this question is the one that was formulated out of that whether registrants - whether privacy proxy registrations can be used for online financial transactions, domain names associated with commercial activities and if so then obviously there are some words there that would be need to be defined.

And that may not be a simple task but we're asking people where they come down on that - in that debate and if they come down in favor of saying that certain uses of - certain uses of domain names that are registered under proxy services should not be allowed then we'll need those definitions about spelling out what's out of bounds.

We've already mentioned on relay about escalation after there's persistent delivery failure. We look forward to your comments on that. And that's really, you know, what are the circumstances under which the provider would be obligated to provide some additional form of non-electronic delivery if the electronic forms have persistently failed.

Then on reveal we had a slide about the standard for refusal of disclosure but as noted - I noted in my presentation there are a number of other open questions as well dealing with law enforcement and other areas that still need to be flushed out as well as what appeal process would be appropriate and what process for dealing with the case of possible improper disclosures or improper use of the information that was disclosed to the third party requestor.

I would just conclude by saying we really welcome comments on all aspects of this report. While we flagged some areas where we're particularly eager to have the community weigh in, we certainly are open to your views on any other questions as well. It's probably safe to say - I think Graeme would agree - that there's probably no one in the working group that is enthusiastic about every aspect of this draft report. And many of us have concerns about some of it.

But I think there was a very good effort by a very diverse group of working group members to try to come up with a product that could be put before the community for comment and input so that's what we were able to achieve at the beginning of this month. And we're looking forward to your input over the next five or six weeks before the comment deadline of July 7.

So with that let me turn this back over to Mary who I believe will be taking charge of our question and answer period.

Mary Wong: Thank you, Steve. And thank you, Graeme, for fairly concise but very clear explanations of the substantive discussions of the working group so far. So everyone we'll now enter the Q&A portion and (unintelligible) some time left. I'm sorry about the ringing phone but all your lines should be unmuted so if anyone who's on the audio bridge has a question we'll go to you first and so just speak up and we will take your questions if any.

Following that we'll then go to the questions that were typed into the Adobe chat. Not hearing a big rush to the microphones. I guess we will start with the various questions that have been typed into the Adobe chat. And, Graeme and Steve, I don't know if you guys want to be the tag team in answering them but what I will do is read them out and we could also have other working group members who are on the call contribute if they wish.

The first question or set of questions I should say because Jeff Neuman, I think your first set of questions were related. It has to do with essentially what is a privacy or proxy service provider. And what I will say here is that earlier in the presentation Steve mentioned that the working group took as a starting point the working definitions that had been used for other work.

But you had more specific questions, particularly whether or not there is an implication that law firms may not register names on behalf of their clients if their clients are financial service providers. And I think that goes to the last substantive topic about the online financial transactions distinction. And you followed that up also by asking whether more generally law firms designated agents and others considered proxy providers.

Steve and Graeme, I don't know if - which one of you might want to take that.

Graeme Bunton: I'll start first maybe and I'm sure Steve will have something to add. This is a topic that certainly came up within the working group as part of these discussions. And I don't believe that we came to any strong conclusion specifically around law firms.

So the definitions for the privacy and proxy are in like how we've chosen to define them is in the report although I don't have the page in front of me. But your question is an interesting one that I don't think we've resolved.

Steve Metalitz: Well, yeah, this is Steve.

Graeme Bunton: Go ahead, Steve.

Steve Metalitz: Yeah, Graeme is right this was discussed a lot. I don't think it's that - well first of all Jeff asked whether law firms may not register names on behalf of their clients if their clients are financial service providers. First of all, who the client is irrelevant, I mean, we've already said that there was a consensus that there isn't any status - there isn't any status bar on who can register using a privacy or proxy service whether or not a law firm is a privacy or proxy service. So I think that answers that question.

On the second, are law firms designated agents and others considered proxy providers? Well I think the short answer is probably not. But if you look at the definition of a proxy provider or the privacy provider and these are the ones that would need to be accredited in order for registrars to do business with them there ones that are substituting information - masking information about the actual registrant.

If a law firm is registering the fact that it has a client on whose behalf it's registering the law firm is still the registrant if it's listed in Whois. And of course there is a provision in the Registrar Accreditation Agreement dealing with situations in which use of domain name is licensed to others and this would not - would not change that.

So I think, you know, again we're dealing now in an environment where most entities that consider themselves or hold themselves out to be privacy or proxy services actually are affiliated with registrars or are the alter egos of registrars. So that is kind of the model we're looking at now.

One byproduct, if you will, of having an accreditation system is that you could have a fully independent privacy and proxy service not affiliated with the registrar. And if it met these criteria and operated in accordance with accreditation and achieved accreditation then it could also register domain names. And that may be a route that some of the registrants may want to take. But there's nothing specifically about law firms I don't think in this - in this report.

Graeme Bunton: Let me add a sort of brief rough way I think about it. And I'm not 100% sure if this is helpful or not but the way I try to come at it is if I try to sue Whois in the Whois and they say okay or they go, no, it's actually someone else's is kind of the distinction for me. So law firms I suspect would accept responsibility whereas most actual privacy and proxy service providers would not. Food for thought. Mary.

Mary Wong: Thank you, Graeme. Thank you, Steve. And I suppose just to try to follow up and sum up, it seems to the staff supporting this group that there was some discussion of these questions that Jeff raises fairly early on in the process including I think at one or two ICANN meetings.

But as you see from the recommendations and the report itself the focus really rather than on saying, you know, this is a closed group of who or what types of providers might be considered privacy or proxy providers it's more a question of the function as in what exactly is being done.

And I note in that the chat there Amr did try to give an example of what other sorts of providers might unknowingly be classified under ICANN's definition

as privacy or proxy service providers and I guess a follow up I would have for that is that, you know, that might, if that is true, make them eligible for accreditation if the is the appropriate path.

Steve and Graeme, the next question or set of questions go toward the online financial transaction question. And it has to do with presumably what line can be drawn. There is (unintelligible) that Website is advertising could be considered commercial.

And I believe also that Amr asked a specific question as to whether the working group has made a distinction between financial transactions for a commercial purpose versus for a noncommercial purpose. Also, and in this context, is this determination then to be made at the time that someone attempts to register the domain name?

Graeme Bunton: I went first last time, Steve, so all yours.

Steve Metalitz: Okay. Sure, well the question of whether - remember the threshold question is should certain activities be considered inconsistent with status as a privacy proxy registrant - activities involving transactions, for example. If the answer is no then you don't need to, you know, in other words if anybody is allowed to register a privacy proxy - as privacy proxy and use it for whatever purpose they wish, at least from the standpoint of the accreditation system, then you don't need to answer the question about whether having adds on the site constitutes a commercial transaction.

If you think that there should be some limitations then people need to say whether they think that the presence of advertising by itself is enough to take it outside the scope of what should be a permissible use of a privacy or proxy registration.

So the group does not have a view on that. If you look at again on Annex F, the proponents of a more restrictive approach if I could call it that, have a

statement on Pages 94 and 95, and they talk - they give some description of what they think should be in bounds and out of bounds for a privacy and proxy - for a domain name registered using a privacy or proxy service.

And then on 96-98 there's a number of questions raised by the group that takes the opposing point of view which is that there shouldn't be a limitation and they raise some questions about what would constitute, you know, a transaction or commercial activity. So there is not a working group consensus position on this. And we welcome the public's input. I hope that's responsive to that question.

Graeme Bunton: The only thing I'll add is to the second bit of that question which is around when - whether it would have to be declared what the purpose of the domain for what is at the time of registration. And this is certainly a problem with this question that we've encountered and have no resolution for it. Domains change obviously purposes after registration and that makes this difficult.

Who is next?

Mary Wong: Graeme, Steve, there was actually an earlier question by Stephanie that I thought we would try to cover all the related questions first. And Stephanie asks the question about timing as to whether the intention is to have this accreditation program implemented (unintelligible) or at least in time with the expiry of the current interim specification or if there's another timeline in mind.

Steve Metalitz: This is Steve. I think that's certainly our goal if we can. Recognizing that there is - even assuming there was a fairly quick approval of the overall accreditation framework there are a lot of implementation questions to be answered. So this is one reason why we were eager to get the interim report out and get people's responses on it in the hope that we could in fact have an accreditation system up and running by the end of next year which is really the deadline under the interim specification.

Graeme Bunton: Yeah, nothing to add.

Mary Wong: Thank you. And, Stephanie, I hope that answers the question. I see that there is some back and forth in the chat that is I think arising from the earlier discussion that obviously not being phrased as a question (unintelligible) I won't read. But I will encourage everyone to submit public comments because, as Steve and others have said, that not only are there some open questions that Jeff noted in the chat that this maybe requires some work.

And the working group would, I would say, (unintelligible) the input of the community especially those who may be impacted by some of these recommendations in order to complete the work and, as Steve said, in good time because we would like to have this completed so that we can have at least the major elements of an accreditation program in place before or at the expiry of the interim specs.

I don't actually see any more questions in the chat. If I missed it please raise your hand if you're in Adobe - well if you typed in the chat I guess you are in Adobe, sorry, or type it back into the chat.

In the mean time we do have a few minutes left and Steve and Graeme, I see that Stephanie Perrin, who is a member of the working group, has her hand raised. And so I'm going to call on her. I don't know, Stephanie, if you have a question or a comment but go ahead.

Stephanie Perrin: Hi there. Can you hear me? Is the phone working?

Steve Metalitz: Yes.

Mary Wong: Yes we can hear you.

Stephanie Perrin: Marvelous. Thank you. I just wanted to comment on this issue of whether law firms should be accredited. From the perspective of civil society it's a really

important point. As discussed in the chat, the issue of solicitor client privilege looms large in that discussion. And from civil society's perspective we can't have a situation where rich companies can afford to hide behind their lawyers.

I realize I'm using inflammatory words here but where those that can afford it can use law firms and those who can't are going to be forced into a regime where if they accept any kind of funds, if they're a charity, if they're a community group, they may in fact lose the ability to use privacy proxy services because they are engaging in rather trivial commercial transactions.

Since we've yet to define commercial there isn't a whole lot of confidence that these groups are indeed going to be able to continue to use privacy proxy services. So I just want to flag it as a very fundamental two worlds kind of a regime we would be entering if we accredit some and we don't accredit others. Thank you.

Graeme Bunton: Thanks, Stephanie.

Steve Metalitz: But - yeah, this is Steve. My only comment on that is that could go to who's covered by accreditation could also go to this question that, you know, the last slide as to whether there are certain activities that aren't permitted in the privacy proxy world. But I - thanks for that contribution, Stephanie.

Mary Wong: Thanks, Stephanie. Thanks, everybody. And we do still have a few minutes left so I guess what I'll do is ask everyone attending this webinar that we will - this is the last call for questions either on the audio bridge or in Adobe or at least the last call for today and remind folks that we have the public comment period open through the 7th of July which is our chair Don Blumenthal's birthday apparently.

So as you can see from the questions and some of the discussions in the chat there are some points that would probably benefit from public input. And

on that score I would also like to point out that the working group plans to have a session at the upcoming Buenos Aires meeting in June. So if you could get comments in or even if you wanted to follow up there's another opportunity there as well.

Steve and Graeme, I don't know if you want to pick up on some of the points that either you or others have raised or make some concluding remarks?

Steve Metalitz: This is Steve. No, I'd just like to thank everyone for their participation and encourage everyone to send in your comments. Obviously you don't need to wait until July 7. I understand, you know, I've been around ICANN long enough to know that that's - most of the comments will come in at the end but you don't need to wait. So we're looking forward to getting - to getting your input.

Graeme Bunton: I'll just echo those sentiments and thank everyone for coming.

Mary Wong: Thank you, Steve. Thank you, Graeme, for being our presenters today and for guiding this group to the publication of this initial report. What I will add as the last note here is that these slides and the recordings will be posted as I mentioned, and there are links on these slides to the public comment forum as well as to the report.

The executive summary of the initial report has been translated into the various official UN languages so hopefully that helps the community as well. If you have any questions either about the webinar or how to access the report or contact the members of the working group or the chairs please feel free to contact me or any of the other policy staff.

And on that note I echo the chairs' thanks to everybody for taking the time to attend this today. And we look forward to receiving your comments. Thank you all very much.

END