Transcription ICANN Buenos Aires GNSO Privacy & Proxy Accreditation Services Issues Policy Development Process Working Group

Wednesday 24 June 2015

Note: The following is the output of transcribing from an audio. 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.

On page: http://gnso.icann.org/en/calendar/#fjun The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page

Steve Metalitz: Good afternoon and welcome to the meeting of the Privacy and Proxy Services Accreditation Issues PDP Working Group. Breathe. Exhale. This is a group that - I'm Steve Metalitz.

I'm one of the Co-Chairs of this group - Interim Co-Chairs. Graeme Bunton is my colleague with the same role. And we have here many of the people who have been active participants in the Working Group, but there are still a few seats.

The seats are not reserved for members of the Working Group, so if you would like to come up to the table and particularly if you're planning to make a contribution that might be easier to come up to the table.

You're welcome to do so. I think our plan for this afternoon is to move fairly briskly through the main points of the initial report of this Working Group, which was published early in May I guess -- I don't remember the exact date -- and is open for public comment until July 7.

We have received I'm told 6000 comments so far of which 5999 are virtually identical. But we are hoping for a robust public comment period and to get a lot of input on our initial report so that we can - Graeme and I were just talking about getting back on schedule for our weekly meetings next month so that we can hopefully drive this promptly toward a final report that would be able to go to the GNSO Council.

So anyway our plan was to kind of walk through some of the main issues in the report, and my suggestion is that if people have questions or comments they could raise them at the point that we talk about that particular item, and we'll keep an eye on the time and make sure we cover everything.

And one other element that we may bring in here at least a little bit is we've received a lot of helpful input since the report was published from the Staff, looking at this kind of from an operational perspective raising some questions.

A lot of these are implementation questions but I think it's very valuable to have that input now as we move toward a final report so that we get a sense of what, you know, some of the implementation issues are.

So it's possible we'll ask the Staff to comment a bit on that and at least let people know that these operational questions are also, you know, kind of in the mix.

So unless Graeme has any opening comments maybe we should just get started. And I think you were going to start I think on the slides. I'm happy to if you wish...

((Crosstalk))

Graeme Bunton: What is the first slide?

Steve Metalitz: Well I'm - we'll ask for the first slide.

Graeme Bunton: Oh sure. So I don't have any more general opening comments. That was an excellent introduction. Thank you Steve. A bit of background for those of us who haven't been traveling all the way down the road of this Working Group.

So there's the 2013 Accreditation Agreement. It has a interim specification that expires January 1, 2017, which means we need to complete this PDP and get implementation completed prior to that date or the status quo will reign.

And we're at the moment very much aware of that timeline. So it was chartered in October. We began our first meetings in December of 2013 and have been 60 plus meetings since then.

As Steve said we published our initial report May 5 - open comment period till July 7. Please read the report and provide us with your input. We need it very much.

Let's keep going. Next slide. Thank you. So there's a list there -- I'm not going to read for you all -- of other pieces of work that we've looked into and brought on board in our discussions.

The Working Group's been made up of all the GNSO Stakeholder Groups/members of At-Large. We've had some input from law enforcement as well as just individuals so it's been a great array of people and voices inside the Working Group.

Often interesting times. Right. There we go on our initial report. So the initial report has a - is a pretty broad summary and we're going to go through that now.

But the key bits are some really large open questions that we've put forth to the community and we'll discuss a bit I'm sure here today, and those are really what we're looking for input on. Yes thank you. Yes please.

Steve Metalitz: Thank you. This is Steve Metalitz again. And by the way I know we have people - I'm assuming we have people in the Adobe room so Mary if you will just let us know if people there have any questions that they want to ask and I'll - we'll manage the queue here for people in the room and please feel free if you have a question.

So our group which was very diverse and also hardworking I'd have to say did reach consensus on a lot of the charter questions that we were given, and this just gives you a little bit of a summary of the initial report.

You know, the whole document is very thick but if you read the Executive Summary you will get the - all of the recommendations and you'll also get pointed to a couple of annexes that are quite important.

And I'll just mention two of those. One is Annex E, which we'll talk about later in the presentation and that is an illustrative framework for handling disclosure requests from intellectual property rights holders.

One of the main issues in this whole area is what are the circumstances under which a privacy or proxy service provider if it's accredited should be revealing the - to - or disclosing to the - thank you - and disclosing to the - to a requester the information on its customer; in other words the kind of information that would appear in publicly accessible WHOIS but for the fact that the registration has been made as a proxy registration or a privacy registration.

So that's a - obviously the - an issue we spent most of our or much of our time on and this annex gives an illustrative framework - just one example of how these - this could be handled for one type of disclosure request from

intellectual property rights holders and as we - we'll discuss when we get there.

There are obviously a lot of other entities or interests that might make such request. Annex F is also important because it lays out two viewpoints within the Working Group on an important question about whether proxy - whether customers who use proxy registrations should be prohibited or restricted from carrying out certain kinds of activities, notably commercial transactions using a Web site to which that domain name resolves for example.

So we will get to that but that - there's some brief statements from various members of the Working Group that kind of lay that out, and that's certainly one big issue on which we are seeking comment.

Next slide please. Oh you got it. So we are using the terms privacy and proxy service, which were defined in some of the earlier research that ICANN commissioned.

And you'll see that we basically decided that both of them - both these types of services should be treated the same but this is the definition. And then we have some new terms that are quite important to understand.

One is relay. Again that's a term that's been used a lot in this context but it really refers to a situation where a third party wants to send a message electronically to the customer; in other words the proxy registrant if you will or the customer of the privacy/proxy service and they can't contact them directly because that information is not in WHOIS.

So the relay process is - which Graeme will talk about in more detail I believe - that's what that refers to. And then we came into this exercise using the term reveal - relay and reveal and it was soon revealed to us that many people couldn't - that term still required greater definition.

So here's what we - how - what we came to and we tried to use these consistently throughout the report, which was a challenge but with the Staff's help I think we've succeeded in being consistent.

And disclosure we're using to mean revealing the contact information of the customer to a third party requester, but only to that requester and with restrictions on how that information can be used only to resolve the issue that gave rise to it for example.

And publication would be publishing it; in other words putting it in the WHOIS. It's tantamount to ending or terminating the customer's privacy and proxy service and then it becomes public.

And law enforcement authority - we just copied the definition that's in the Registrar Accreditation Agreement, which again refers to - it's got a jurisdictional aspect to it so that's another definition that we just shamelessly adopted from other work that had been done.

Next slide please. Okay I've already mentioned that we wouldn't - we didn't really find any place where we needed to treat privacy services different from proxy services.

Obviously if you think of one please let us know in the public comment process. The - this whole issue of permissible uses - really is a threshold issue, which is are certain entities or certain registrants allowed or not allowed to use a privacy and proxy service?

And where we came out as a consensus matter I believe on that is really the status quo, which is whether you're commercial or a non-commercial, an organization or an individual you are eligible to use these services.

Where we didn't reach agreement is whether there are restrictions on what you can do once, you know, with that domain name once you have it so we'll get to that.

With - we did adopt a recommendation that the domain names that are involved here would be labeled as such in WHOIS so that people who access the public WHOIS would be able to know whether they're dealing with proxy registrations, privacy registrations or not.

And this is one area where the Staff in its - their operational feedback has raised a good question, which is who has the responsibility to ensure that the labeling is done?

Is that the registrar or the service provider? This is a good question because right now of course we're looking at this through the lens of a situation in which the service providers are virtually if not always entities affiliated with registrars.

But that might not necessarily be the case in the future. We could have an unaccredited - excuse me, an accredited privacy or proxy service provider that's not affiliated with a - an accredited registrar.

So that's an example of the kind of question that we're - we appreciate the Staff bringing up. And I'm not going to put this - put Owen and other Staff members on the spot here, but there are Staff folks here who may be able to answer questions if people have it about some of their observations.

One important recommendation I think is that the privacy/proxy registrations are to be validated or verified in the same way that the - that non-privacy registrations are for - under the WHOIS accuracy specification.

Again to the extent that these services are operated by accredited registrars this should not present that much of a problem. It's just a question of what

you call the customer whose contact information you need to validate or verify could get more complicated obviously in the case of an independent accredited privacy/proxy service provider.

And the Staff pointed out that the WHOIS accuracy specification might change. I know that there's - that's being discussed right now. I think personally it would be a terrible mistake if the WHOIS accuracy specification were changed, but it would not be the first time that ICANN had done something that I thought was a terrible mistake.

So, you know, all we're saying is let's keep it simple. You have to do with these what you would have to do if you were a registrar and it was just a standard non-proxy registration.

And then we talk about some mandatory provisions that have to be included and published in the terms of service. I - Graeme mentioned that we now have an interim specification in the Registrar Accreditation Agreement to deal with these - some of these services.

And that includes a requirement that certain types of policy information and terms of service be published and be abided by. So this is similar in that sense but we - I think we do list specifically that you - that they have to - the services have to tell the customers, you know, what are the grounds under which there could be disclosure or publication?

What are the circumstances under which their service might be terminated? What are their rights and responsibilities and so on? So that's again another one of our consensus recommendations.

I think we can - oh we - and we - already on the next one. Thank you. We recommended that ICANN maintain a public list of all the accredited providers.

You know, ICANN does that now with registrars. It doesn't do it with these services so that - this would be helpful for anybody trying to figure out, you know, who is the service and who runs the service and everything and that the providers would - excuse me.

We'd have to have greater transparency about when a provider has an affiliation with a registrar. Again that's the norm today that most of these services are provided by affiliates or subsidiaries of registrars, so we wanted to facilitate that as you can see.

The provider has to maintain an abuse contact point and publish that on its Web site. We did have some discussion about whether that had to be dedicated with the implication that this person would do nothing else but this or just simply designate it.

You know, this person does this. They may have other responsibilities. We came out for designated and then that they had to be capable and authorized basically to deal with the problems that might arise, and that is defined in the Inter-Registrar Transfer Policy.

So once again we've tried to repurpose some of what ICANN policy development has already dealt with rather than trying to reinvent the wheel. And again, you know, if this is a topic where you think that's not the right definition we would love to hear that from members of the public.

And then what do these contact points do? They need to respond to reports of malicious conduct and that - while we don't have a - an exhaustive definition of that we do have some starting points that are listed there from the Registry Agreement, from the GAC safeguards and I think there's actually a little more to that slide.

But you'll see the - you'll see this all in the report to indicate what this designated - yes designated contact point is responsible for. So I think that brings us to relay, which does not appear on the title of that slide.

It's - but it does appear on - it does appear in the report. So let me turn it back to Graeme to talk about that.

Graeme Bunton: Thanks Steve. I put you on the hook for a lot of talking there. So Steve gave the definition earlier for relay but let's just make sure we're all on the same page there.

So relay is a third party is sending communications via the proxy or privacy provider to the registrant, and so they are relaying some form of communications.

So we have a number of agreed recommendations here and then we still have a couple of open questions on relay that are - we post to you guys here and is also in the report and we can have some discussion there as well if there are questions.

So the service provider has to relay to the customer all communications required by ICANN consensus policies or the RAA, which makes perfect sense, so that's WDRP notices and renewal notices and those sorts of things.

We have an option here and the distinction might be a little bit subtle, but service providers must also either relay all electronic communications but can apply commercially reasonable safeguards against spam or abuse or all electronic communications from law enforcement or third parties alleging abuse.

So that gives you the ability to just relay everything or you can just relay law enforcement and abuse requests, and how you choose to implement that sort of thing is up to you.

And so what you're essentially trying to do there is remove unwarranted communications or unwanted communications from your registrant. Requester will be notified of a persistent delivery failure of electronic communications, so this is in the scenario where the registrant email might be failing for instance and the provider is aware of it; that they would then have to tell the requester that the delivery notification has failed or the delivery of that communication has failed persistently.

I don't think we've defined that in any more detail. Now that would almost certainly kick off the registrant verification procedure as well probably in the background if privacy and proxy providers have to abide by that standard, which we said they should.

Right. And that's the next bullet point. I'm getting ahead of myself. Right. Actually we can go on. Thanks Mary. So we have a pretty big open question here and I'll read this out and post it to the community.

So where you see square brackets is where we have an option that we're looking at. So this is around the escalation process for where relay has failed and the third party wishes to seek another form of communication with the registrant.

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

A provider should have the discretion to select the most appropriate means of forwarding such a request, brackets, and to charge a reasonable fee on a cost recovery basis."

Continuing on with the brackets, “Any such reasonable fee is to be borne by the customer and not the requester. Provider shall have the right to impose a - reasonable limits on the number of such requests made by the same requester.”

So you can’t escalate forever all the time. There are limits on that. The should or must determines the - whether we are forcing the provider to forward a further form of notice to their customer.

And then we have a rather contentious issue of who should pay for that sort of relay, and in many cases we might be talking about physical mail and therefore these processes are not free.

They would certainly have some sort of cost and it’s around who should bear that cost, whether it is the third party who is trying to communicate, whether it’s the service provider or possibly even the registrant.

So that is the sort of main open question that’s out there on relay. I can’t read the - what’s the...

Steve Metalitz: This is review.

Graeme Bunton: Okay. So do we want to pause for a moment on relay - see if we’ve got any hands? I see Volker and (Elliott) and Michele. There’s our queue. Volker you’re up first.

Volker Greimann: I have a more general point to make about the accreditation system, but I’m going to hold that until the open questions are open. With regard to relay and the costs involved I would strongly recommend that these costs should be borne by the requester, if only for the reason if they would have sent the postal mail from themselves to the registrant directly they would also have borne that cost.

Elliot Noss: Elliot Noss, Tucows. Two comments on the relay. The first is with respect to - and all Staff can vote Steve if you could maybe speak with - speak to them.

The first is on the shifting of the cost burden when demonstrably in the - in numerous different community processes previously it's been shown empirically that the vast majority of complaints that tended to be the type of complaint that will be the subject matter here are not successful or not with merit - and with merit's wrong.

With merit's too strong but, you know, our demands that don't actually lead to a conclusion that's asked for. What's the argument for shifting the cost burden, you know? I mean, let me get the answer to the first one and then I'll...

Steve Metalitz: Did you have a second question too or do you just want...?

((Crosstalk))

Elliot Noss: I do but it's totally separate.

Steve Metalitz: Yes. First I don't, I mean, I don't really accept your premise and - about what's been empirically shown but remember where this fits in. This is only in a situation where there's some either - there's some electronic form of communication, either email or a Web form that's used and it's - it doesn't work and persistently doesn't work.

So I think the social contract that we're talking about here is that people who use a privacy or proxy registration should provide a way to be contacted electronically.

And if they fail to do that it doesn't seem fair to assign the cost of that to a third party that isn't the reason for that failure. So it either needs to be built in to the - again I'm providing just the other point of view here.

It either needs to be built in to the cost of the service or it needs to be imposed in some way on the customer, who's basically necessitated this escalation. So that I think is my answer to your first question.

Elliot Noss: Would you be open to or would it be helpful if in the comment period some of that empirical data was provided? In other words, you know, if it was the case that the significant majority of let me call them demands or demand letters for lack of a better phrase, you know, are just that, shot over the bow at first instance, would that change your thinking or influence your thinking?

Steve Metalitz: It wouldn't - I don't think it would change my thinking but you're certainly welcome to include anything of that sort in your comments, and I think that the Working Group would be interested in seeing that.

Elliot Noss: The second question is - well it's maybe more of a comment. It seems that the use of mail here -- and I think, you know, we might go back to that social contract -- feels very, you know, U.S. or North American centric in the sense that - so there's sort of two pieces to that.

One is that globally you're going to have varied, you know, varied costs, very long delivery processes. In parts of the developing world certainly the communication between a service provider and their customer could take many forms including face-to-face and so there - I feel like there's a range to be fit in there.

And the second comment about mail in particular is it feels deeply anachronistic. You know, I think that people would strongly prefer other means of communication today.

You know, mail in North America in the developing - in developed world tends to be, you know, a pile of fliers these days and I'm wondering if there's some other way to think about communication.

I mean, it feels anachronistic and - what would I call it? You know, it's nice for a legal file but probably won't' get your practical point across.

Steve Metalitz: Okay thank you Elliot. I think we would be - the Working Group would be open to alternatives of other means of communicating to customers once electronic mail or a Web from has failed.

And I'm certainly very comfortable saying that this escalation would not include buying the requester a ticket to get on an airplane and meet face-to-face with the customer.

So I think we can probably - we could - we would welcome your suggestions on that and can probably respond to those. I think you're maintaining the queue at this point.

Graeme Bunton: Yes.

Steve Metalitz: Before you do that I just - can I just acknowledge that we have - we do have people in the chat room and I'm sure Mary will tell us - oh okay. Some person is...

Graeme Bunton: Stephanie.

Steve Metalitz: Stephanie who's in the room has raised her hand but also for people who aren't physically here - and I want to acknowledge that one of those is Don Blumenthal who's the Chair of this Working Group and who was unable to travel to - here to Buenos Aires but Don we welcome you and of course if you have any questions or contributions we would welcome those too. Graeme?

Graeme Bunton: Thanks Steve. Actually we're going to Michele next and then Stephanie is the queue at the moment.

Michele Neylon: Michele Neylon for the record. Thanks. I'd just like to go back a little to the previous section that Steve was presenting. On the WHOIS accuracy specification built in to the contract there is a review process and the - we're currently going through that at the moment with ICANN.

It's open for public comment. Some of the changes that we are proposing are just to make the entire thing more workable for all parties involved including ICANN Staff.

One of the issues that arose in the review of this is that some of the terminology translates really, really, really badly and that's causing headaches.

So, you know, the thing is most processes, most policies - reviewing them from time to time isn't a bad thing because see sometimes you will get something that you like - not very often and not when I'm in the room but sometimes.

Graeme Bunton: Thanks Michele. Stephanie?

Stephanie Perrin: Thanks very much. For the record Stephanie Perrin. I just wanted to endorse Volker's statement. I think from a civil society perspective we're deeply concerned that these services will be priced out of existence.

And the fact of the matter is just because an email doesn't go through doesn't mean that the respondent is being unresponsive. This is an untrusted platform.

Email doesn't always work and therefore you have to revert to the other methods. Yes they cost money but we don't see any reason to see why those costs should be transferred in this particular environment. Thanks.

Steve Metalitz: David's...

Graeme Bunton: Okay. We've got Alex next and then David and then we might carry on.

Alex Deacon: Hi. This is Alex Deacon from the MPAA for the record. So like Steve I don't agree that the cost should be borne by the complainant. I think if the issue that we're trying to solve here is to minimize bogus or malformed complaints, then there are other ways to fix that - probably simpler ways.

For example a trusted sender program may be one way to do that. So I think if that's the issue then I think we have options to solve that problem.

David Cake: As those who've been following this...

Graeme Bunton: Say your name.

David Cake: Sorry. David Cake and a member of the Working Group. As - those who've been following this Working Group and participating will know that in fact we've had quite a lot of extensive debates about exactly how and when email fails in its utility and under what conditions you can know that it hasn't been delivered and so on, and early on some pretty interesting examples of the edge cases of physical communication, you know, people sending, you know, several feet of documentation and things like that.

So we have thought quite a lot about all the failure modes but I think the question really is not - is about the - who, you know, who bears the cost. And I think the thing we need to beware of that we may be slipping into is trying to prescribe the business model of the provider.

I don't, I mean, I can understand that if you are the requester you want to have a relatively straightforward means available to you without additional fees.

But whether it's borne by the customer or the provider or, you know, there is some other mechanism - is, I mean, that's something we shouldn't be trying to control the many different methods - business models of proxy and privacy providers in the accreditation process and meddle too much in their internal accounting.

Graeme Bunton: Thanks David. I'm a little conscious. This queue is - just keeps growing and we wanted to keep this a bit short. So if you're still very interested please keep your hand up. I've got Volker and then Michele but let's try and keep it quick and we can carry on and look at the rest of the report please. Thanks.

Volker Greimann: Thank you. Volker Greimann speaking again for the record. Just one comment, which is that if there were no WHOIS privacy for a complainant - for a domain name and the complainant would send an email and find out that it failed, then he would also have to send physical mail or call by their - call by phone or any other - utilize any other means at its own cost.

And we are not talking about unreasonable fees. We are talking about a cost recovery fee here, so I don't see why the costs should suddenly be transferred to the registrant if those costs would've been borne by the complainant anyway.

Graeme Bunton: Thank you. Michele's next.

Michele Neylon: Thanks. Michele Neylon for the record. But just this thing around cost, I think it's a - kind of a ridiculous argument to be having in some respects but not in others.

We're talking about contracts here so we're talking about what we can or cannot do. And I don't - and so the thing is is from my perspective, speaking for my own company, if you read our terms of service you will see that we give ourselves the option to do certain things.

That does not mean that we do that each and every single time. So for example if you have the - if you are clever enough to realize that hosting with us was a good thing to do and you had the misfortune of being reported on by spam cop, within our terms of service we can levy a fee.

But the way we work that in reality is that unless you're a repeat offender and are just blatantly out there to, you know, abuse our service we don't. You know, you did it once.

You screwed up. Fine. I think some - what, you know, I think for some of us the cost recovery thing around this isn't so much a case of saying, "We must be able to do it.

We are all going to charge you thousands of dollars," or anything like that. But we should have the ability to recover the cost because we know some people point out, you know, you don't want these services to become so ridiculously expensive and that they're prohibitive to use.

Or if I want to put on my human rights hat which I was - obviously had on earlier today, if it wasn't for the fact that ICANN blatantly insists on breaking European privacy law we wouldn't have this problem to begin with, but I won't go down that track.

I mean, the reality is that, you know, we need to have options and having the option to pay the charge I think is a good thing.

Graeme Bunton: I've got two more and then - I've got one more and I'm going to - are - were you still in? Okay I got one more and then we're going to carry on. Thank you. Christian?

Christian Dawson: There's some reasonable threshold at which you - oh my name is Christian Dawson with the ISPCP. There's some reasonable threshold at which you

have contacted people through enough means that you have realized that the person is simply unreachable.

When I sign up for a service with my healthcare provider, in order to communicate with my doctor back and forth through digital means I have to provide a - first a email address and then a secondary email address and then a phone number and then a secondary phone number.

And they're never going to send me a piece of mail and all of those tools that they use - some sort of an IP phone in order to access me. It's all digital and so the costs aren't really there.

Can we create some sort of a structure in which there is a no cost threshold to - which is I think similar to what Elliot was saying about using modern means of communication.

Graeme Bunton: Certainly something to consider. Thank you Christian. All right, I think up next is Steve and reveal.

Steve Metalitz: Yes.

Graeme Bunton: Please.

Steve Metalitz: Thank you. This slide deals with reveal which as we told you at the outset is not a term we are using in the report if we could help it. So we have definitions and distinctions between disclosure and publication.

And as I mentioned before also the recommendations include some information that the providers need to publish and also inform their customers of.

And a lot of them have to do with this disclosure and publication including whether the customer will be notified if the disclosure request is received, and

including whether as some providers do or may offer, particularly those that are affiliated with registrars the option to cancel a domain name registration instead of having your contact information disclosed.

Again we're not requiring - these recommendations don't require providers to offer that option but they do require them to tell the customers if they do offer that option.

And in terms of customer notification you'll see later that in the illustrative framework customer notification is mandatory, but recognizing that that illustrative framework doesn't cover all kinds of requests.

That's why we have in here this recommendation that the providers tell their customers, you know, whether they will be notified of disclosure requests. So I did - as I did mention we have an illustrative framework for disclosure requests from trademark and copyright holders, and I would encourage you to look at that in Annex E of the report.

And you'll see that at the outset of that that it's intended to strike a balance among providing requesters a higher degree of certainty and predictability, what level of disclosure they can obtain, to preserve for service providers a sufficient degree of flexibility and discretion in acting on these requests, and to include reasonable safeguards and procedures to protect the legitimate interests and legal rights of the customers of these providers.

So that was our goal and we obviously are looking for your input on whether we have achieved it. I'm not going to go in great detail through these - through what's in Annex E since I don't think we have a slide for it.

But basically it's trying to be as detailed as possible about how such requests would be handled, and if it's successful hopefully it could provide some kind of template for other types of requests.

But because - the reason we chose this is that we had those people with expertise in this area around the table, and we didn't have as much expertise from some of the other requesters such as law enforcement or from anti-phishing or malware.

And we hope that those groups would kind of come up with the right framework for those types of requests, but we don't have that in our recommendations.

So there are a number of questions that are open that we're specifically seeking input from the community having to do with disclosure and publication and some of these are listed here.

I've already mentioned, you know, what should the rules be for law enforcement requests and in particular we know that in the case - you'll see in the illustrative framework that - in Annex E that as I mentioned customer notification is mandatory.

If a trademark owner or copyright owner makes a request for the contact information of the customer they will know. Assuming this is all adopted they will know that that customer will be notified and the request will be sent on to the customer, which is fine for those requests but it's not necessarily fine for law enforcement requests in the middle of an investigation.

They may feel very strongly that this should not be - the customer should not be notified so that - we've invited comments on how to handle that issue. We had a question in our charter I believe about whether there should be certain types of misbehavior on the part of customers that would make publication mandatory.

We didn't again make any recommendation on mandatory publication, recognizing that one of our goals was to preserve the flexibility and discretion for service providers to enforce their terms of service or not.

Michele's absolutely right that just because the authority is there to enforce the terms of service doesn't mean it's always going to be enforced. But we welcome comments on that.

There were some concerns about what would happen if - this is - publications really I think goes to disclosure. What would happen if information was disclosed either based on false pretenses or the information was disclosed and then used in a manner - as I mentioned at the outset any disclosure could only be used in order to address the issue that's - that gave rise to the request.

And what if it were used for marketing purposes or something like that? So what would the remedies be? And then we did have some specific questions about elements of the IP disclosure framework, some timeframe issues and then, you know, how to handle some of these disputes over wrongful disclosures that would result - false information or from misuse.

So there are - we - there are really two options in there about whether you are required to go to arbitration or would there - would you have to submit to jurisdiction in a particular court.

Here are some other questions that arise in the illustrative framework. Of course the customer can object to the disclosure and we're trying to come up with a reasonable, predictable but flexible standard for when that sort of objection should prevail.

And we - you see two different formulations there. One of them is - has three alternate adjectives: whether the reasons have to be adequate, sufficient or compelling and the other is more, you know, a reasonable basis test.

They both get at the same thing as to whether information that's been brought forward that would justify - even though the elements of the request

fully satisfy the requirements of this framework and there is evidence of an intellectual property violation, what are the circumstances under which it could nevertheless be denied?

And there are two different bullets there in bold: one, because the customer might've objected; and the second might be that maybe the customer didn't but the provider decided to refuse to request it and what would be the basis for doing that?

But again the illustrative framework goes into this in some detail about a number of reasons that could justify a refusal to disclose, a number of reasons that could not be relied upon solely to justify a refusal to disclose and we would welcome your comments on any of those.

I think that's the last slide on reveal so let me again - and we can pause here if people have questions or comments that they wish to raise. And - okay and then again if there are any in the chat room you'll let us know. Dick go ahead.

Graeme Bunton: Please.

Richard Leaning: ...Leaning from the Public Safety Working Group. I am a law enforcement officer and I'd just like to echo your comments about the disclosure of a request from a law enforcement service provider that tells the registrant that we've asked for that request, because that will frustrate any investigation that we'd ever have and there could be evidence destroyed and it just can't happen under those circumstances.

So we obviously will be making a comment through the process. And the other issue is about the jurisdiction part and I'm going to comment on that now or we'll come to that later about...

Steve Metalitz: Okay. I think that would be appropriate now if you wanted to talk about that.

Richard Leaning: Regarding the jurisdiction issue, which at the moment the law enforcement requests - and I'll use - change law enforcement to whatever agency you want to use in the public safety arena.

But if we're not allowed to make a request of the service provider outside of the jurisdiction, that's going to cause all public safety agencies a big headache.

It will get to such a state that I'm from Scotland Yard (for our kind) to ask Scotland to reveal the details of their registrants without an MLAT. That is not workable. So there's issues for that jurisdiction.

Now I'm acutely aware of the difficulties of (unintelligible) every law enforcement agency in the world. If you look at America itself, there's 22,000 law enforcement agencies.

Just because that's problematic it doesn't mean that we shouldn't change that and look at some other mechanism that we can credit law enforcement whatever that may be or that type of agency.

So it's not really a question. It's just a comment echoing, you know, concerns that my members in the public sector working group (unintelligible) have over this whole privacy proxy issue.

Steve Metalitz: Thank you very much Dick. And again, we would welcome your comments, those of your colleagues as well on this; how to - I think you've put your finger on a significant problem and how best to resolve that. So we would look forward to you comments on that.

I see (Holly) and then Volker.

(Holly): Just to make matters a little bit worse, some of the comments I've had have been an expansion of the concept of law enforcement agency. For example,

you have - might have a government agency that looks over trade practice issues or financial prudential matters, perhaps in the public interest issues, that kind of thing.

They're not law enforcement. But they are charged with some aspects of I think public safety or public good. We haven't dealt with that issue. But I'm just flagging that that's been a comment that I've received in terms of how do we deal with those kinds of requests as opposed to saying an individual request. Thanks.

Steve Metalitz: Thank you (Holly). I think Volker was next. Does anybody else want to make a comment here?

Volker Greimann: Volker Greimann speaking for the record. In response to the gentleman from the law enforcement agencies, I don't think the working group has in any way foreseen not - law enforcement agencies not being able to request this data outside the jurisdiction.

The only thing that we have discussed is whether they should be given special powers that they do not have under the law. I would submit that a law enforcement agent that would be acting without - outside his jurisdiction without jurisdiction in general would be treated as any other complainant and therefore his complaints be looked at under their merits.

If they wanted to have special powers granted to them, there's always the proper process of requiring legal assistance from law enforcement agencies where the privacy proxy service provider is situated. That is currently the legal government induced process. That's the process that has been followed by law enforcement agencies inside and outside the Internet for decades now. Why should this change?

Steve Metalitz: Thank you Volker. Kirin, I think is next and then Michele.

Kirin Malancharuvil: Before I go, Kathy Kleinman put a question into the chat way in advance of me. So maybe you want to read her question first.

Steve Metalitz: Could you do that Mary? Thank you.

Mary Wong: This is Mary from ICANN staff reading the question from Kathy Kleinman, a member of the working group. What about the very different laws around the world? What is legal in one country is illegal in others. How do we resolve this?

Steve Metalitz: Okay. Well that's a very big question but I think the way we're focused on it in the working group is requests coming from law enforcement agencies - now obviously there are definitional issues there and the issue of, you know, the recognition of, excuse me, of law enforcement agencies from outside the jurisdiction but it's obviously not - we haven't gotten to the point of whether a particular activity is legal or not.

Kirin, I think and then...

Kirin Malancharuvil: This is Kirin Malancharuvil. I apologize for the state of my voice. I'm hoping it lasts for the next 30 minutes. But I'll be brief.

I have two concerns with the jurisdiction section that Dick brought up. My first is that when you limit the applicability of - the ability of law enforcement to respond to certain jurisdictions, then I think that this is going to cause a problem of kind of privacy proxy services (flight) to those jurisdictions where they're almost unreachable.

So for example Frank Schilling may have 1000 new neighbors in the Cayman Islands as a result of this. You know. And so then, you know, poor law enforcement is going to be completely frustrated. And there's no point at all to any of the recommendations that relate to the ability of law enforcement to go after people and criminals hiding behind privacy proxy shields.

I think that on this - well, okay, that's - I think that's all I have to say about it at this point. There's a lot more discussion to come on the jurisdiction issue. So I think I'll wait until we get into more details about this. I think like Steve noted, we haven't really spoken about this in depth. Thanks.

Steve Metalitz: Thank you Kirin. I think Michele is next. Does anybody else want to be - (Carlton) and David. I'm sorry.

Michele Neylon: Michele Neylon for the record. Around this thing around jurisdiction and law enforcement, I appreciate the concern that Dick and others have raised on this matter. I mean I can understand that. The issue and the concern that a lot of us would have is the scenarios that we're seeing at the moment.

I mean I'm actively involved on the international and we've been - we're getting emails almost every single day about bloggers in Saudi Arabia being flogged 60 times or 100 times or more on that. You know, we're looking at, you know, serious human rights abuses.

Now I'm not - but hold on. There's more to it. I mean there's - if you look at how some of the ccTLDs have dealt with this issue, what they've done there is that they provided mechanisms, excuse me -- I have the same problem as Kirin -- mechanisms by which law enforcement agencies can request the data but only under particular specific circumstances for addressing specific types of crime.

So I said something nasty about Volker doesn't make the bar and I'm disseminating child abuse material definitely does. I mean there's a list - you can define a list. Maybe that's the way to look at resolving this.

For us as an Irish company, I have to be - I'm very conscious and very, very sensitive to restrictions around what (these) I can and cannot share but I

have absolutely no interest in running any kind of service that helps serious crime.

Define it narrowly enough and I'm pretty sure a lot of us won't have an issue. Leave it far too open and we're going to be arguing about this in a year's time. Thanks.

Steve Metalitz: Thank you. I think we have a question from the chat. Then we'll go to (Carlton) and David. Does anybody else want to be in the queue or can we wrap up the queue on this?

Mary Wong: Not so much a question but a short comment from (Don) I would share. And he says he's tagging a little bit onto Kathy Kleinman's earlier question. And he says that - sorry, I just lost it.

Steve Metalitz: What is...

Mary Wong: What - I'm sorry. Yes. What is or isn't considered law enforcement will vary.

Steve Metalitz: Good point. (Carlton).

(Carlton): Yes. I wanted to comment follow up on Michele's point. We have to - we have to have a framework in which we consider purpose as a means to determine how we handle extraterritorial requests.

And I would think we would want to go at least give some measure of endorsement to the European view that MLATs, mutual legal assistance treaties, would be the gold standard by which you would use to respond to purposeful requests.

So first we have to establish that purpose and several purposes where we would entertain extralegal requests, extraterritorial requests and then it would

be first of all in the context of MLATs and then other things further down the line.

Steve Metalitz: Thank you (Carlton). David.

David Cake: Yes. The - to echo what sort of what (Carlton) said, we - yes, we have established mechanisms for dealing with these tricky cases. We have MLATs and Interpol. But we do understand that the - we do not have - that there's old mechanisms.

They're very slow in practice. They are not practical for a world in which we have to deal with, you know - well Internet moves a lot faster and a lot - you know, automated quantities. And those mechanisms may not, you know, be useful.

And at the moment we kind of mostly hope to work around that by, as Michele says, you know, registrars don't want to be seen as being involved in serious criminal activity. But there is a, you know, they'd have to make their own judgment when there is a gray area.

We - there is a big problem here. It is possibly solvable. There are people - certainly people trying to solve it. I mean (talk to veteran) (Delisha Powell) and he will talk to you for a long time about the complexities of his problem and how to solve it. And we are not going to solve it in this working group. We are going to have to come up with a compromise for now that we will refine later as people chip away at this very big problem. Thank you.

Steve Metalitz: Thank you David. So we'll have one more comment here and then we'll move on to our remaining one or two slides and further questions.

Man: Thank you very much for giving the opportunity. I've been listening the comments of (final things over the year). Certainly there is a issue being

faced by the law enforcement agency. One solution has come about the mutual legal assistance treaty, MLAT.

But I must say that the mutual legal assistance treaty largely have (incurred), which encompass in the physical issues also. This is a (show) more cyber issues solution need to be come out in a very (good behavior). So we need to look at whether the mutual - this treaty that kind of arrangement will work in these cases.

In India is a little bit more (unintelligible) community serve there. We find the (unintelligible) happen, there's destructions happen to the (lives) as the physical property there. And we face it. We have seen our experience is that most of the domain (to each other) (unintelligible) behind the privacy protection that are abused.

Issues - who decide the abuse if the registrar or the registry decides that there is abuse or thought abuse, are they better than the law enforcement agent to decide that this is not abuse and (unintelligible) or a variance of the law enforcement agency.

We need to find a solution certainly. And the issue becomes much more serious than is (across jurisdictional) issues are there. I agree with my friend there. We need to find a solution particularly in a place from which a side of the country, which I come from, is a serious issue there.

We must make the process for the getting the details as simple as we make for registries to remain under privacy protection. We must make the process simple. Thank you.

Steve Metalitz: Thank you very much for that perspective. So let's turn to the next - let me turn it back to Graeme to walk us through the remaining slides and then we'll have more time for discussion.

Graeme Bunton: Thank you Steve. So this is a fun one that we've spent a considerable amount of time on and is certainly the subject I think of a number of the public comments already. Steve is joking. Okay, fine.

So there's quite a division within the working group on this question. And we talked earlier about use of privacy and proxy services. And we all agreed that there is no need to distinguish between who can use privacy and proxy services.

That means you can be an individual, an organization, a company, a commercial organization doing business or sorry - that's next. So anybody can use it. It doesn't matter who you are.

It does possibly matter what you're doing. And so this text is proposed by some members of the working group and it is domains used for online financial transactions for commercial purpose should be ineligible for privacy and proxy registrations.

And certainly there are many within the working group who disagree. And there are two annexes on the initial report describing both of those positions and I would encourage everyone to read those and provide us with input in the comment period as that would be very helpful to help us tease this question apart.

There's not a whole lot more to say on that other than just to make sure that distinction is clear that anyone can use privacy and proxy services. It's just that you become - you may become ineligible if you are doing commercial - financial - online financial transactions for a commercial purpose.

So that would exclude non-commercial purposes for doing transactions for instance. I think that's relatively straightforward and should be quite clear and it's certainly a topic that we've spent lots of time on. And I would be interested

in seeing if there's anyone we haven't heard from who has thoughts on this matter. I don't see any hands. What?

Woman: You limit it to people you haven't heard from.

Graeme Bunton: I did - Stephanie has put her hand down. Stephanie please.

Stephanie Perrin: I invite anybody else to jump in first because you have heard from me. Okay. Stephanie Perrin for the record. Just for greater clarity, could you describe further what we mean by those words you just said, financial transactions for a commercial purpose?

So in other words, if I'm a charity, donations to my registered charity are not for commercial purpose. Is that correct?

Graeme Bunton: That's a good question. I don't have the - I don't have that answer. I don't know that we've gone too far down the road of really teasing it probably what we meant by commercial transactions. You know, and certainly we've talked about this a bunch about is the donate button...

Stephanie Perrin: Yes.

Graeme Bunton: ...on a journalist blog or, you know, donations especially come up in many contexts. (And those would count).

Stephanie Perrin: Well, perhaps I'd just like to put on the record then that as we as a committee go through the comments, which we receive on this, we need to be sure that the people commenting have it crystal clear in their minds and this is a matter where the legal framework varies considerably from jurisdiction to jurisdiction. Thank you.

Graeme Bunton: I'm seeing lots of hands coming up now. I am shocked and amazed. I've got - we've got a question in the chat. I'm going to go to Mary. We've got about 23 minutes left. Am I right?

Mary Wong: Correct. This is Mary from staff. It's not so much a comment from the chat although there may be. I haven't looked in the last 30 seconds. But more to follow up on Stephanie's question. The working group's initial report does propose not a formulation or definition but some sort of framework for your question.

The intent is not just financial transactions that take place online but financial transactions that take place online that associated with commercial activities. And I believe that is the language used in the initial report by the working group.

Graeme Bunton: That's helpful. Thank you Mary. I've got Volker and then Kirin and then I saw a couple hands on this side if you can - it was Christian. Okay. And Ollie.

Volker Greimann: I (unintelligible) this before but here's the real life example for a company that I've recently used for private financial transaction. This is a service based in the U.K. On their Web site they have their contact details as required under European law for service providers of any kind.

They offer money transmission services to any country in the world. That is in my book - that's as much as financial transaction as you can get. You can send money to other people or to yourself in other countries. They accept cash or transfers and they - you can pick up the money at the location or have it transferred to your bank account.

But they use domains by proxy, which is in my book under my understanding still the privacy proxy service used by GoDaddy. Now I've thought about this and I don't really see anything wrong with this as using this service.

Is there any danger involved in using this service? Is there any danger involved in any other legitimate site using privacy proxy service even if they offer financial transactions? It's a question that I've asked myself. I've done some research on this side. They seem legitimate. Money arrived. So I have no problems with that.

The only question is should we really regulate them out of their privacy service. There might be legitimate reasons why they use it. I don't know why. Maybe they don't own the domain name, only rent it.

There could be a dozen reasons but I don't know if we should take the place of legislators and say they must say also on the Whois even though they say it on the site who they are. Otherwise you won't be able to provide the service or have a domain name.

Graeme Bunton: Thanks Volker. I've got Kirin next.

Kirin Malancharuvil: So I think that one of the things that's really important to note as we kind of frame these discussions and frankly don't get off on tangents - multiple tangents is that the - this is a threshold question and that we haven't really gotten into the issues surrounding implementation.

So for example, my position would - on charitable donations would have to take into account the fact that over $3 billion are diverted from charitable - legitimate charitable organizations every year by very different various criminal hackers that are posing as charities and collecting the donations that would have gone to, you know, like legitimate foundations.

It doesn't all happen online. It is - I certainly have no information or numbers associated with, you know, what percentage of those fraudsters are using privacy proxy services. But there are lots of things to look at with this. And I think that we need to be reminded where we are in the process of discussing this question.

We're only trying to figure out if it's a question we're looking at. And, you know, I think we brought it up in the GNSO session over the weekend some of the language that was out there on the outreach sites on this issue about, you know, which was frankly extremely fear mongering in the community.

Oh, you know, we're going to have - we're going to be monitoring your Web site. We're going to be taking down this Web site and this specific instance is going to result in this person's privacy being - privacy shield being taken down. And we don't know the answers to those questions yet because this group hasn't actually look at how this is going to be applied and how it's going to be implemented.

So I would like to see this discussion become a little bit more measured back into what the report is actually asking of us, which is are there circumstances where this, you know, this distinction of permissible uses should even be considered by this group.

And I think that the fact that there are so many questions out there means that the answer to that is clearly yes and that we should actually move forward to discussing implementation because there are a lot of concerns and there's a lot of misinformation. And we need to - we need to start discussing it. Thanks.

Graeme Bunton: Sorry. Missed my microphone. I've got a couple people ahead of the online queue that I'm going to go to first, which is Christian and then Ollie and then Michele and Stephanie. And then we've got about only 18 minutes from now so let's keep it relatively quick and hopefully we can dip into some of the implementation issues that we're - might be able to hear about. So please.

Christian Dawson: I think it's very fair to at least foreshadow the idea of implementation. I for one am not convinced at all that there is value. In fact I mostly see destructive value in the idea of doing this in the first place.

When you take a look at how implementation would have to work and you realize that there seems to be a great deal of gray area, seems to be a very good - great deal of difficulty in understanding what the criteria are, you realize that there's going to be a very difficult arbitration process that's going to be required for something like this.

There's going to be a very difficult negotiation process of how exactly this is going to work and potentially a great deal of cost. And so I think it's fair to say as you are trying to determine whether there is value in doing this to balance it against the difficulty in doing this.

And so that's where I think that it is very reasonable to talk - to at least foreshadow implementation. And in this case my feeling is that with the extreme difficulty that I expect there is in implementing this and in my mind a very low value or even negative value in doing this. It's a deterrent value. But it should be something that we do not accept moving forward.

Graeme Bunton: Thanks Christian. Ollie.

Ollie Hope: Thanks. Yes. Ollie Hope. Yes. It's a similar point actually to what you just said. I was just sort of looking I think in the difficulty of putting this in, the complexity, the problems that it will cause. And I'm sure there are many arguments for it. We've heard one. There are also many arguments against it.

So it's almost like it's a balanced view it seems. And I think the weight of it ends up being that, yes, it should be discussed but I just don't think it can work. It can't be done.

I also think you have to be very, very clear in the definition because the wording that was out there it said, you know, the domain name is used for financial transactions. Well, how far do we go down that line? I assume it means the content on the Web site the domain points to.

But if that domain then points to a ccTLD that doesn't have any of these restrictions and the content on that Web site, you know, does that apply? Does that not - these are just parts of the reasons why it's so difficult. But I think before you almost get to that, you know, that definition is key and I'll be quiet now. Thank you.

Graeme Bunton: Thanks Ollie. We're back up into the Adobe queue now before Michele. Right. Okay.

Paul McGrady: Paul McGrady. Another topic that I think that needs to be discussed in relationship to this is who will have the burden. Will the provider have the burden to be constantly looking through all the second level registrations to see what they're doing? Or were - or will there be a reporting and then action based upon that reporting by an (aggrieved) party?

I think that those are two very different things with very different burden models. And so was we continue to discuss this issue, I think we need to take a look at that issue. Thank you.

Graeme Bunton: Interesting. Thanks. Now Michele.

Michele Neylon: Thanks Graeme. I think there's one thing that I - I think there's some language people have been using -- sorry, Michele Neylon for the record -- some language that some people have been using that does cause a certain degree of confusion. I don't think it's particularly helpful.

We're talking about the domain name on the Whois - the Whois for the domain name. Mixing that up a lot of the time with the Web site sites (unintelligible) it is confusing. Because it - what we're seeing in some conversations is, you know, Web Site X uses Whois privacy. Well actually it doesn't.

The domain name, which is just part of the Web site, does. That is - you could see there are things (unintelligible) but in many respects it's actually not because we've come across a lot of Web sites where the Web site itself is made up of multiple host names, content served from multiple host names because I can make the entire thing up that constitute the Web site.

I mean the points that a couple people have raised around, you know, the - when this goes to implementation if it goes to implementation. The example I look at is a lot of our clients are more than happy to publish their full contact details on their Web sites, as they're obliged to do under Irish law if they're commercial entities. But they do choose to not publish their details in the Whois on gTLDs because the Whois on gTLDs is not protected.

Now the ccTLD space this is not an issue because the ccTLD space is either minimal Whois output both for commercial, non-commercial business private, whatever. But it's also protected.

You talk to any ccTLD manager and they would quite happily tell you that their Whois servers are (wreak) limited in some way or another whereas with the gTLD space theoretically at least there aren't any limitations and there are a bunch of companies out there that are selling people's data. And that data is being used for spam. It's being used for sending fake renewal notices and a whole load of other things.

Which if we're talking about the Web sites and what they do or don't do and sure it's a matter of work for law enforcement and for the consumer protection people. Why is it a matter for the Whois?

Graeme Bunton: Thanks Michele. We're not going to have time to get into some of the (information) stuff. So we can carry on here and then - and we have a summary slide or two don't we?

Woman: (Unintelligible).

Graeme Bunton: Oh and there's another meeting at 5:00 so we've got a few more minutes. I see Stephanie and then Volker. Is there anybody else in the queue? (Holly). All right. Stephanie.

Stephanie Perrin: Thanks Stephanie Perrin for the record. And oddly enough Michele and I appear to be on the same wavelength here so I can be brief. For some of us there is a deep and abiding concern that ICANN stay within its remit and that being related to the domain name and how that is managed and the information associated with it.

So indeed what happens on the Web site is outside of ICANN's remit except insofar of course as if law enforcement comes to investigate what they consider is a crime and the only data they can get would be through the reveal process or the disclosure process on this, well fine. Then they go through due process and exercise that.

But drawing this bright line is very difficult and determine why somebody purchases a domain name and I'll use an example. I purchased a domain name seven or eight years ago, which sooner or later I may use to sell my book on data protection law. I urge you all to buy a copy.

In the meantime, why can't I have privacy proxy service for that name? How is the privacy proxy service provider going to determine what my intention for using that Web site is until somebody gets, you know, this is a mug's game.

How would a service provider manage that and make the determination. It falls into that category that A, ICANN shouldn't be doing it and B, the cost if they did do it would be prohibitive. Thank you.

Graeme Bunton: Thank you Stephanie. We've got probably about six or so minutes left. We need to hear from Volker, (Holly) and then Steve, you wanted in the queue. (I'm sorry).

Volker Greimann: Thanks Graeme. Volker Greimann speaking again. I'm saying - I'm going to say something heretical that probably would get me stoned in some countries.

I've given the entire idea of an accreditation program a lot of thought and it has come to me that possibly the accreditation of such providers is not the best idea. We might want to look at alternatives such as a more lightweight alternative such as in a certification process.

Just bear in mind that if we create an accreditation program, we are essentially creating a third contract parties group. Very closely affiliated with registrars in some cases. Not at all affiliated with registrars in other cases. It would have to appear that ICANN currently have no voice at ICANN. They would be suddenly here as a contracted party required to come where they have currently not had that cost before.

Also the accreditation program carries very high requirements for - well, it is cost intensive for ICANN and for the providers. It has - it would probably require a fee, which would price the services higher than they currently are. And all this could have been - could be avoided if we do not go the process of an accreditation but rather follow a certification route.

Of course this would require a certain amendment in the RAA and other agreements and other processes. But I think those could be done. And I would like the group to give this just some thought to - for further, yes, discussions.

Graeme Bunton: Thanks Volker. (Holly). (Kabani).

(Holly): I think we're sort of on the same length but come up with different answers. I was asked why are we - why did we decide in the beginning to lump privacy and proxy providers together. Because privacy actually servers generally are

registrars of one kind or another. But proxy can be just a lawyer, actually an agent.

And if you're starting to say we have to now have accredited for lawyers who are - is that what we're saying? I don't think so. So I mean when I was asked about compliance and I suddenly thought is ICANN going to be running after a bunch of lawyers for being an agent. I got a little sort of doubt in my mind.

Graeme Bunton: That's a delightful one to bring up with two minutes left. Thank you (Holly). Much appreciated. I've got two minutes left or so and then we've got Steve and...

Vicky Sheckler: Thanks. It's Vicky Sheckler with the IPC for the record. As I've been listening to the conversation, I am struck by how much there's discussion of I think the answer's X, Y and Z and not so much specifics in terms of how you got to that position or how you support that position.

So as we move forward, as we get public comment I for one would appreciate having more specifics. If it's cost prohibitive, what are the costs? You know, in my world if I make a complaint, you want to know what the evidence is behind that complaint. I am happy to share that with you. I'm happy to share with you how we got to that point. But I think that if we dig a little deeper and have a date driven process, we'll get to better results. Thank you.

Graeme Bunton: Thanks Vicky. That's an excellent suggestion. Steve.

Steve Metalitz: Yes. Thank you. I have found this discussion actually more revelatory than I perhaps I anticipated. And I'm not just talking about the Volker and (Holly)'s revelations that after 18 months of donating every Tuesday to this discussion they think maybe it's not worthwhile.

I'm not going to stone Volker because - I'm not going to stone Volker because I have no stones in hand. But actually what I wanted to say was I think

Christian had raised an important point here on this question, which is we probably should figure, you know, look at the principle and its implementation.

Now I know Christian's view is that the principle is not worth carrying forward. I think I disagree with that. But I think there really are serious implementation issues that would need to be resolved.

So it's - and it's just something to think about as to whether this could be identified as a principle that if we can fashion a way to do so that ought to be incorporated into the accreditation program that Volker is going to boycott now. And then recognize that there are serious implementation issues.

And, you know, the last slide - the last characters on this last slide show that we have a deadline. And so we have to be very mindful of that deadline as well.

So that's - I just thought that was an interesting way of approach this and I want to thank everyone for their contributions. Do we have any further remarks?

Graeme Bunton: No. I think that's just about it. We need to be out of here in a couple of minutes. So comment period is still open for another two weeks or so. Please submit. And to thank you for everyone attending, members of the working group, fellow co-Chair Steve and (Don) who is not with us today and especially staff. Thank you everyone.

END