ICANN Transcription
Privacy and Proxy Services Accreditation Issues PDP WG F2F meeting – Part 4
Friday 10 October 2014

Note: The following is the output of transcribing from an audio recording of Privacy and Proxy Services Accreditation Issues PDP WG F2F meeting on the Friday 10 October 2014. 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/calendar/#oct

Don Blumenthal: All right, let's take our seats; get to the home stretch here, almost home stretch. Next to last lap I guess.

((Crosstalk))

Don Blumenthal: We've got some cats out there too to herd?

((Crosstalk))

James Bladel: (Unintelligible).

((Crosstalk))

Thomas Rickert: I think we should just...

((Crosstalk))

Don Blumenthal: Just wondering - yeah, okay why don't we get started here. Anybody who wants to come in late that's their loss, his loss, her loss, whatever. I hate mixing singular and plural.

Any event, we heard a bit about - from the Implementation Group earlier in our work and some time has passed so we thought it'd be worthwhile since we would be in the same place to see where that work stands now. So we've got Mike Zupke, Amy Bivins, who we've spoke with the last time, and Danielle Andela with us for the first time I think. So I'll turn it over.

Amy Bivins: Sorry, technical difficulties. Okay so this presentation is just following up on the presentation that Mike gave you to guys about a month ago now. And we just wanted to go through some different contracting models that were familiar with the staff and that we're using to kind of frame our thinking about privacy proxy accreditation implementation and how it might work.

And so basically today I'm just going to talk about three different contracting models that ICANN uses right now. And talk about some of the issues that we've thought about that could come up in implementation of a privacy proxy accreditation program and questions that we would have and things that would be good to think about.

So the three different contracting models are the registrar accreditation model, which everyone is pretty familiar with, the reseller model and also the escrow agent model that's being used a lot now by the Registry Services Team.

So the registrar contracting model, as most of you know, is that, you know, when someone wants to become a registrar they fill out an application to ICANN and pay the application fee. And then staff review the application, approve the application, you know, that the people do a background check and screen the answers to the questions.

And then eventually if and when staff is satisfied with the application eventually the registrar and ICANN enter into the RAA. So it's a contract between the registrar and ICANN.

And the reseller contracting model, which is another one that you guys are probably familiar with is instead of a reseller going to ICANN they go to a registrar. And so like the registrar or multiple registrars that they wish to work with and follow the registrar's processes for entering into a reseller agreement.

And the reseller agreement has some terms that are mandated under the Registrar Accreditation Agreement, but the remainder of the terms are set by the registrar so the registrar has control over the various terms of the agreement beyond what's required under the RAA.

So the escrow agent contracting model is in some ways kind of a hybrid between the two. And the escrow agent identifies a sponsoring entity. In this case it would probably be a registrar but in practice right now it's a registry for the most part.

And finds the registry or registrar that they want to work with and then once they found once they submit an application to ICANN and then ICANN reviews the application and then sends it back to the registrar and the escrow agent to negotiate a contract, decide on the terms of the agreement and then ICANN ultimately has to approve the contract. And ICANN isn't a party to the contract but it's a beneficiary to the contract so it has some rights under the contract.

So because these contracts are among different parties - sure...

Kathy Kleiman: The escrow agent, is that for backing up data or what is - okay, thanks.

Amy Bivins: It's becoming more common now it's pretty popular with the new gTLDs program with the agreements between new registries and escrow agents.

Kathy Kleiman: So it's solely for the purpose of backing up data because escrow agent can mean a lot of things .

Amy Bivins: Yes.

Mike Zupke: So this is Mike. You know, just as a little bit further kind of clarification on this so registrars have an option to use the agent that ICANN has designated and pays for which is currently Iron Mountain, or they have the option to select what we call a third party providers.

Registries really only have the one option and that's to find their own provider and have that approved by ICANN. So most of what you'll see in the slides is referring to what we do in the registrar model. And the reason is that in the registrar model it's - ICANN has an agreement with the registrar and the escrow agent so it's a little bit cleaner in some regards for at least discussion purposes about how enforcement works and that sort of thing.

David Cake: My understanding of the escrow model is that the - I mean, it's essentially that registrars can choose any escrow provider they want but they have the - because the Iron Mountain has already been certified by ICANN they have a financial incentive to - it's easier basically so there's some incentive and that's...

Amy Bivins: Right.

Kathy Kleiman: Someone go back to that slide again because the purpose of the slide was to show us that ICANN was a party to the escrow agent agreement is that - okay, I think I get it.

((Crosstalk))

Mike Zupke: So that was kind of the - this is Mike again - that was sort of the point I was making was that in the registrar arrangement ICANN is a party to the agreement; in the registry arrangement ICANN is a beneficiary to the agreement. And, you know, the distinction between the two is a little bit, you know, beyond my comprehension but, you know, and that's why I say for discussion here we're really talking about the registrar model for the most part.

Amy Bivins: Thanks, Mike. Oh sorry. Okay so with respect to these different models one of the big differences between some of them is just how they're enforced. When, you know, something comes up and like if a service is not following the terms of the agreement how enforcement works and so in the registrar model only ICANN can enforce the terms of the contract and the enforcement mechanism is - it's a legal enforcement, not necessarily a specific performance type enforcement.

Whereas with the reseller model ICANN, through the registrar, and also the registrar have enforcement capabilities. The way that ICANN has enforcement power through the reseller model is through the RAA and a registrar could also be required potentially in the privacy proxy contact if it were applied ultimately here a registrar could be required to act on privacy proxy service complaints like they do for abuse complaints now in the reseller model.

And in the escrow agent model, like the reseller model, both ICANN and the registrar have enforcement capabilities.

Mike Zupke: So this is Mike again. I just thought we can also offer in between these slides if there are questions we're happy to...

Amy Bivins: Yes, please.

Mike Zupke: ...you know, to be interrupted. Yeah, please go ahead.

Holly Raiche: I think what you're saying - I think - is the enforcement is through a contract and what you're saying is the contract is the RAA and the enforcement is that the - ICANN has the ability to say to the registrar we have a contract with you and you are not complying with it. Now that can be the only way that this is enforced because third party beneficiaries can't enforce something so it has - I'm understanding that's the way the enforcement happens?

Amy Bivins: Yes.

Holly Raiche: Thank you.

Mike Zupke: Right and so, you know, the distinction here - can you go back a slide? Thank you. So Mike again. You know, the distinction here is in the registrar model ICANN can directly enforce it's agreement against a registrar and if you replace the word "registrar" with "proxy service" it's the same thing; ICANN can say that proxy service, you're in breach, you know, and there could be potentially, you know, penalties for failure to comply or ICANN could terminate the agreement.

In the reseller model, and when, you know, in the proxy or privacy service could operate the same way. ICANN goes to the registrar and says, in your registrar accreditation agreement it says that you will require, you know, your reseller or your proxy service to do the following things. If your privacy or proxy service fails to do the things that are in there we can hold you, registrar, responsible for failing to enforce your agreement.

In the escrow agent model, and this is why - you know, we can sort of set aside the third party thing because what we're really talking about is a three party agreement in this instance. And so either ICANN or the registrar could enforce compliance at least, you know, from a legal perspective against the - what would be the proxy service if there were an issue of breach.

Holly Raiche: I wouldn't say so much a three party agreement as it says an agreement that's enforceable but really against one of the two parties based on another contract really.

Amy Bivins: So do you have a question, James or a comment?

James Bladel: Question or comment or however you want to phrase. Also, welcome, Volker, if anybody didn't see him - I didn't see him sneak in. I just want to point out that from the registrar perspective the pull through model of enforcing contractual obligations by proxy on proxy service providers through a separate agreement is problematic particularly when they're delivering different services.

It's bad enough when a reseller is delivering the exactly same service that the registrar is and just making it up and targeting a different market. This is a different service mode all together. And as a registrar million of customers to have all of them, really all of them, at risk of what our worst reseller could possibly do is not an acceptable framework.

So I would say - and we had this conversation a month ago and I think you guys heard this feedback from us. This mechanism of we're going to build this privacy proxy accreditation framework under the RAA and punt that enforcement responsibility to registrars and just hit them with our RAA stick when they fail, that's not acceptable to us; that's not what the EWG said; that's not what the Whois Review Team said and that's not what the community said.

So I don't understand why this is still on the table as a model here. If it's maybe just for academic reasons but I really think that we should not be going down that path. Thanks.

Mike Zupke: Thanks, James. Mike again. So, you know, we took what you said to heart last time, you know, and we went through the record for the Whois Review Team and went through, you know, their recommendations and what was said about this.

And so, you know, our read of that was that there was sort of a presumption that there is a certain way that accreditation works but I don't think that it necessarily said, you know, you're confined to one path to doing it.

So when we present this what we're trying to do is we're trying to show you sort of the range of possible options that, you know, that we could proceed down. And so, you know, we're not really of the opinion that that was necessarily for close. And while we're not saying that we're, you know, set on doing it that way, you know, this session is to give everybody kind of the full sense of options and also the information about that.

And I think that as you'll see as Amy goes on some of the considerations in this might sort of favor some - might favor that model over others and in particular not to, you know, sort of jump the gun but when we talk about how we do transitions of a terminated entity, a terminated proxy service, you know, there's scenarios where there could be more friction in the process which, you know, we sort of equate to more risk, more potentially - I don't want to say lost registrations but more, you know, lost privacy or so to speak or, you know, there could indeed actually be lost registrations in the process and that they exist but who the underlying customer is might be unknown.

But so, you know, we're still kind of in this state of trying to, you know, figure out how to do the balance and it's not a matter of a decision having been made, this is really about trying to present all of the considerations to you.

And I don't know if people have had a chance to look at that chart, I think, you know, it was probably a couple pages and it's in the middle of a lot of other stuff going on. But, you know, that's kind of - if you want the sneak peek, the

chart that Mary sent around about, I don't know what was that about a week ago, week and a half ago. That's really, you know, where this is coming so there's a little bit more detail in that than what you see on the slides just if it's helpful to anybody.

Amy Bivins: Wendy.

Wendy Seltzer: Thanks. Wendy Seltzer here. And just one notable feature of this whole contractual enforcement structure is sort of the lack of the party who is ultimately affected by registering domains under it. And, you know, we could address that by putting third party beneficiary rights into these agreements. And in the past ICANN has tended sort of explicitly to try to deny that.

But since we are regulating the rights available to end user registrants it would be good to address where they could stake stronger claims to enforce their interests.

Mike Zupke: Sorry, thanks Wendy. I mean, that's a good point. And I think that may even be an issue for this group in that it's really what you're talking about is the customer of the proxy or privacy service, what is their recourse. So, you know, I don't necessarily see that as - exclusively as an implementation issue.

Amy Bivins: All right. Any other questions before we move on? Okay, so one of the other considerations that we wanted to compare these different models for was termination. And under the registrar model terminations require a lot of coordination among all the parties. And as Mike said, they could potentially involve the greatest risk.

In the registrar context when an RAA is terminated all registrations are bulk transferred to another registrar via the registries. And in the event that a privacy proxy service would be terminated it could be more complicated because ICANN would need exceedingly current registration data which

sometimes is hard to get. And the registrar of record would need to be the one to do the change of the registered name holder which could require changes to the registration agreements themselves.

And if ICANN chooses or recommends a new gaining privacy proxy service in some cases this might force a registrar to do business with a privacy proxy service or registrant that they don't necessarily want to do business with. And that's just one of the issues that we thought about that we wanted to point out.

And in the reseller model ICANN could potentially create some sort of standardized termination procedure that a registrar could follow in the event that a privacy proxy service is terminated or allow some flexibility for registrars to decide how they want to handle that situation.

And in the escrow model as with the reseller model ICANN could create some sort of standardized procedure or allow flexibility or ICANN could effect the termination itself. Okay.

Mike Zupke: So this is Mike again. I feel like, you know, we kind of - despite the, you know, the good explanation I feel like we went through the slide kind of quickly. And so I don't know if this group has thought through a lot about termination, I'm sorry that I don't follow as actively as I - as Amy and others do.

But, you know, if would be helpful we could talk more about sort of how we think that process would work. But if everybody's got it then I don't mean to belabor the point either.

Yeah, go ahead, Steve.

Steve Metalitz: This is Steve Metalitz. I had a separate - a question about another dimension of this, which I was trying to figure out how these different models would work in the situation in which first, you have a situation which the proxy service is

essentially a subsidiary of the registrar. That's - seems to be the case with all those that are participating in this working group, it's not the case of every proxy service.

But how would this work in a situation when it's an independent proxy service provider? In other words, or would it work differently for these different models in that case? Because you mentioned one might lead to a situation in which a registrar would be doing business with a proxy service provider that it didn't want to do business with.

The RAA says you can only do - once an accreditation program is in place - I think this is what it says - once an accreditation program is in place you can only do business with an accredited proxy service provider but it doesn't speak to whether you have to do business with all accredited proxy service providers. Do any of these models make any difference on that question?

Mike Zupke: So this is Mike again. We - for the sake of the analysis, you know, we sort of were thinking in terms of exposing where is the most potential either divergence between the models or where is the most potential risk in any of these models, we assumed that there is not a relationship between the registrar and the privacy or proxy service.

So as we go through these, you know, that might be a little more evident as we get kind of into like the impact on registrar slide and the impact on customers. But, you know, that does create some real challenges. So, you know, in the instance where the registrar and the proxy service is accredited, I mean, in the instance where the registrar and the proxy service is accredited, I mean, are affiliated in the event that there's any sort of an issue, you know, the registrar is sort of a de facto backstop.

You know, you don't have that when there's no affiliation and, you know, as we'll get to in this registrar model, you know, that's one of the risks that we see is potentially, you know, there's one entity that kind of controls the ability

to relay or reveal data if they're the only one who has it. And the same in the event of termination they're the only one who can tell you exactly who their customers are or, you know, what data has been escrowed.

So, I mean, it is one of the reasons why, you know, I think, you know, the second or third models that we've described have a little bit more appeal in some ways is that they seem to deal better with the potential transaction that, you know, isn't - that isn't between affiliated parties, the registrar and the proxy service.

Go ahead, James.

James Bladel: Are you saying me? Okay. A question I was wondering about is - and maybe this touches on it is how are registrars going to include the underlying customer data for an unaffiliated privacy service in their escrow deposits because they are required to do so.

Mike Zupke: So I think there are probably a couple ways of dealing with that. You know, and we're getting into really I think part of the, you know, one of, I think, the more complicated areas in implementation but, you know, one possibility would be, you know, we just impose a requirement that says everybody who is a proxy service has to give the data to the registrar.

And I know, you know, Volker, I think has raised, you know, some issues with that in that, you know, in some jurisdictions that may offend, you know, their privacy laws.

So, you know, there might either be an alternative to that or maybe, you know, maybe we just throw that option out; we say there's got to be another way of escrowing data either, you know, that service escrows it with, you know, a similar arrangement that we have right now with Iron Mountain or other escrow agents or maybe we come up with an independent escrow sort of service. And obviously there's, you know, cost involved in doing that.

James Bladel: But - and the reason I ask in the context of this is that depending on the model that we choose we may need to go back and amend that requirement in the RAA because if the privacy proxy service is escrowing it separately then the registrar would only be obligated to escrow that data if they were - as affiliated service.

Mike Zupke: Yeah, I'll have to think more about what the specific requirement is in the RAA because I'm not sure, you know, which part of it comes from the specification that's being replaced and which part of it comes from 3.6 and 3.4 which deal with the data escrow requirements. So I think we'll have to probably take that one back and get back to you and put some more thought into it.

Holly Raiche: Just a question, I suppose a follow on in terms of compliance you would be using the RAA with a registrar to enforce requirements about the privacy proxy service provider. What are you going to do with the privacy proxy service provider is to closely affiliated with the registrar? Surely the registrar is in breach of the contract and surely you'd be taking action against the registrar, not the privacy proxy service. That's all you can do.

Mike Zupke: Right and I think that's - it's almost by design.

Holly Raiche: James is taking note.

Phil Corwin: Excuse me, Phil Corwin for the record. Do we have data on the current breakdown? I mean, my sense up to this moment has been that the majority of domains under privacy proxy protection are using a service that's affiliated that's a subsidiary of a registrar. Maybe I'm wrong on that but the only representation of privacy proxy service providers in this group is from registrars.

It's certainly easier for the registrant to choose to add that service at the time of registration rather than to seek out a third party provider. So the fact that you haven't factored that in I think that may be the majority of providers.

Also, we're envisioning - I assume whether the provider is or is not - is affiliated with the registrar or is a third party provider that my assumption has been that ICANN will be the one accrediting them therefore ICANN would be the one de-accrediting them if they run afoul of their - if they're not compliant with the requirements that they've agreed to comply with to be accredited.

So are we all on the same page and do we have that data about what the current breakdown is? Is that data out there?

Mike Zupke: So this is Mike again. I'm not - you know, I'm not aware that the data is out there and I would think if anybody's got it this working group would, I would think that's relevant to, you know, the work that you're doing and it's probably not, you know, readily obtainable.

But, you know, you know, your point is well taken about, you know, most registrants are probably buying the service, the proxy service, the privacy service, at the time of registration whether that's from their registrar or their reseller. That, you know, intuitively that makes sense that that's probably the normal scenario.

We are aware though of proxy services that seem to be sort of independently run where a person can, you know, discover there's a proxy service out there and sometimes they're even offered free; all they have to do is change their, you know, their Whois data what this is and, you know, just register.

And so, you know, those services do exist. And, you know, to my mind those are probably the ones that have the most risk associated with them. They probably involve the least amount of, you know, sort of safeguards at the registrar or reseller level and also, you know, I think that there's a risk

involved that people are probably unaware of who are using them and that's that, you know, if they're a proxy service who they have really no strong connection to disappears their domain name could disappear with it.

So I think, you know, I mean, I think it's an interesting point. I don't know if it necessarily changes the analysis because we know that those services are out there though. And the second question was - I already forgot what the second question was, sorry.

Phil Corwin: Phil again for the transcript. Just two quick comments. One, I think if we don't have the total data we probably could survey some aggregate representative sample of Whois data just to see how many are under, you know, where the registrant is listed as one of the well known proxy providers.

But I'd be suspicious of anyone offering this for free. It reminds me of back in 2007 when I had just recently got involved with ICANN the registrar situation where the company was offering free privacy proxy protection and in fact the CEO was registering all those domains in his own personal name and it became a huge mess.

So - and I'd be suspicious of any third party provider doing anything for free, you know, why would they be doing that for free because it involves some work and some responsibility, you know, and it's normal for companies offering a service to want to make money doing it. So how are they making their money if they're not charging the registrant? But I'll stop there.

Paul McGrady: So three things. One, I do have that entire data set. I've also figured out how to solve the fresh water problem of Southern California and I'm going to share none of it with any of you. But, no, yeah, right. I don't have that data set.

I wanted to ask a really stupid question, which you've already partially answered which is how would it work? I mean, how would an unaffiliated privacy service work? We don't envision a world where I can go to Go Daddy

and - maybe we do envision this world, I don't know, where I can go to Go Daddy and because other people have qualified as an accredited privacy proxy service then Go Daddy has to list them and I check which one I want.

I don't understand how we would - how that would even - how an independent accredited - not scary people that we're talking about - an accredited business, how would that even work? How would the registrant be able to access that and how would the accredited privacy service actually know that that's happened short of, you know, watching new registration lists and pulling out from that new registration list.

And then thirdly, just to give you guys a pep talk, if you think that we're reacting sort of unexcitedly we apologize but you guys are talking about like how to get off at the station and we're still the committee of trying to buy the ticket, right. And so we're way behind this so it's not you, it's us.

Mike Zupke: Thanks, Paul. I think James is going to answer the question about how it works but I want to say I'm happy to, you know, depart my terminal here and wait for you guys to get to the station.

James Bladel: See I thought we were the committee on how to build a train. You're way ahead of me.

((Crosstalk))

Paul McGrady: ...piece of track.

James Bladel: Yeah. The short answer is - and this is just shooting from the hip here is that a privacy service would be reseller of multiple registrars and that the transaction would start with the privacy service instead of added on at the end of a transaction it would start there and then the domain registration would be the add-on.

Sorry, did I just invent something on the public record? Damn it.

Paul McGrady: I told you it was a stupid question so thank you.

James Bladel: Well right now the path and the way it has traditionally been done, and I will acknowledge that I think the industry has just kind of gravitated around this standard, which is that the registration begins, pick your domain name, search for it, we send it to you, you add it to your cart and, by the way, would you like this to be private and that's added on at the end.

Presumably an independent service would say something like start the transaction with the privacy service, tell us what name you want, we will go - because we are a reseller of multiple registrars we will go and find you a, you know, the most appropriate registrar or the best deal, whatever, and then the registration comes after the enrollment in the privacy service. So it's - just turns the transaction upside down.

Kathy Kleiman: (Unintelligible) that proxy privacy.

James Bladel: Right, and that's where you manage it.

Phil Corwin: Yeah, just to further confuse the situation - do we need to create a definition of a privacy - if we just have a general definition it's a company who is standing between the ultimate registrant and the Whois database and inserting their name instead of the actual registrant.

How do we differentiate between Domains by Proxy doing it for individual registrants and companies like Mark Monitor and CSC which acquire domains for corporate customers who don't want their possession of that domain to be known at that time for a certain reason? Do we need to create a definition of who's going to have to be accredited?

Holly Raiche: I've got a more fun question. James, if we turn things on their head and you start off with a privacy proxy server and then they go shopping for a registrar your enforcement model means you're going to have to take an awful lot of registrars to court for one problem because one privacy proxy server has got all those RAAs and you're working through the RAA. That'll be fun.

James Bladel: Well I think generally that's why we don't favor that model because it doesn't allow for the independent - yeah. Another option would be, for example, for one, oh I don't know, large, well respected and mature privacy service to offer its services to other registrars so that they can be added in its cart for registrars who really don't want to develop the service on their own.

Holly Raiche: Do they sign...

James Bladel: It also becomes...

Holly Raiche: ...the contract with ICANN?

Steve Metalitz: They're accredited by ICANN.

((Crosstalk))

Holly Raiche: Because the enforcement we're talking about is through a contract, is through the RAA.

James Bladel: Again, that's why we're not in favor of that model. One of the 3700 reasons why.

Man: (Unintelligible).

Volker Greimann: Hello, everyone. Yes, my plane snuck in this afternoon so I'm a little bit late and I apologize for that. There's a lot of questions that I would like to give a few words to. First, yes I do believe that law firms that give privacy service in

some form would have to be accredited as a privacy service to be able to offer that service, that has been part of our discussions all along. It's not yet consensus but I think that there is sizeable support for that idea.

Another just brief comment is that in our experience we deal with a lot of resellers because a large percentage of our registrar business is done through resellers. So if they offer their privacy services as a reseller they would be accredited for the privacy service and then could offer that through their registrar that knows that this privacy service is accredited.

For example, we also have resellers that operate through multiple registrars and have a privacy service in place. That would then be accredited and they could go through multiple registrars if they wanted to. That model is already in place in the reseller world, there's just no accreditation model for the privacy service that that reseller is offering. And that has been in demand and we are looking at how to answer that demand in this working group.

And finally, there's similar model already in place which is the accreditation of registrars for the new gTLD registries where every registrar has to be TMCH accredited or certified to be able to offer registration services in the new gTLDs as - during the claims - at least during the claims phase.

And I think that can be compared in some way to the model that the very - that the privacy service then would be facing because it's - the certification is not - not an accreditation but it's a requirement by ICANN and it's something that ICANN enforces as well so maybe that's an alternative model that we also should look at.

Amy Bivins: Does anybody else have any other questions, comments? Okay. So thank you for your comments, by the way, Volker and we will definitely...

Volker Greimann: Just one more comment.

Amy Bivins: Sure.

Volker Greimann: Sorry. If I'm not making any sense that's a lack of sleep, 48 hours.

James Bladel: No, you were surprisingly clear today.

Amy Bivins: Thank you. Okay so one of the other issues that we wanted to - that we've been thinking about is how these models would impact privacy proxy customers. And with respect to the registrar model one of the points that's sort of obvious is that customers would digitally have more service provider options because a provider wouldn't necessarily have to be affiliated with the registrar so anyone could get accreditation.

And the vetting of these services could potentially be more robust if ICANN's doing the screening and it's a full application process and everything. But on the flip side the accreditation process could potentially cost more if there's a really extensive screening process and these costs could be passed down to customers ultimately. So just one issue that we thought about.

And also there's a risk of service disruption in the event that the privacy proxy service is de accredited. And we've already talked a little bit about that and our thoughts about that. But with the reseller model one of the customer impacts that we've thought about or see is that if they have a problem with the service they have more places to go; they could go to a registrar or to ICANN with a complaint.

And in the event that the service is terminated or they want to transfer services there would be less friction or risk in transferring. And the escrow model is sort of a mix of both of those. There would be more screening by ICANN and more oversight on ICANN's part. But there would also be more - or it could potentially ease the transition process. So, Wendy.

Wendy Seltzer: Wendy Seltzer. A question, so it's certainly possible that there would be more screening by ICANN, it's also possible that ICANN could choose not to enforce a contract and other than sort of ICANN's interest in enforcing that contract I'm not sure why the sort of end user should be relying on that.

Amy Bivins: Thanks, Wendy. Phil.

Phil Corwin: Phil Corwin for the transcript. How does - I'm thinking about when a registrar is de-accredited. I don't know how ICANN chooses which registrar to do the bulk transfer to but I know there's obviously some procedure.

But it seems to me if we're going to have an accreditation model and the - for privacy proxy services with the possibility of de-accreditation you have to create a similar system where if a provider is suddenly de-accredited there's got to be a way to transfer all the domains to another accredited provider. You can't just leave all the registrants without anyone to communicate with or reveal all their data suddenly. So I think we got to - we have to build that into whatever we're discussing as well.

Mike Zupke: Thanks, Phil. This is Mike again. And I'll just, you know, I'll confess that's one of the things that drives a lot of our considerations in this if not the primary thing is, you know, how do we make sure that registrants will be okay in the event of termination or failure.

You know, so in the case of registrar termination we have one thing working for us and that's that registries know every domain name that every registrar has.

But in the case of a registrar with a proxy or privacy service which isn't affiliated with it that registrar might not know if this is a proxy or privacy customer unless there's some mechanism by which that proxy or privacy service has had to identify to the registrar, you know, hey, I'm registering this as a proxy or privacy service.

Which, you know, when we look at the three models, you know, one way that we've sort of thought about is the registrar model is sort of the everybody can come, everybody can apply and the registrars are, you know, potentially sort of stuck with this world of potential proxy services, some of whom they might not wish to deal with.

Where in the reseller model we think it's almost like the registrars are choosing who they want to partner with in terms of the proxy or privacy services and the same with the escrow model which allows a little bit more of a streamlined implementation. So registrars can have, you know, for example, they may have some API that they develop based on their reseller API or they may even just say to the proxy or privacy services, great, you're in our reseller program, this is how it works.

But, you know, just so, you know, so you know and so we're on the record that is, you know, our first concern is what happens to customers in the event something happens to the proxy or privacy service.

Amy Bivins: Steve.

Steve Metalitz: Yeah, Steve Metalitz. Mike, just picking up on one thing you mentioned, we have discussed that in this - we have discussed in this working group how to identify whether it's a proxy registration. We've said our preliminary conclusion was domain name registrations involving privacy proxy service providers should be clearly labeled as such in Whois. There may be various ways to implement this recommendation and it goes on from there.

So it should be possible for the registrar to know that this is a privacy proxy registration and therefore to know whether it's dealing with an accredited service provider and therefore know whether it is in compliance with its RAA obligations.

You're right though that they don't know the whole universe, unlike what a registry knows about a registrar, the registrar would not know the whole universe of registrations that that party was engaged in.

Mike Zupke: Thanks, Steve. Mike again. And, you know, that's a good point. You know, the concern is what about the people who don't do what they're supposed to?

You know, and that's - having, you know, having lived through registrar (flight), you know, I'm always sort of thinking about what's the worse bad actor going to do to us because that's probably going to be the big embarrassing one. So, you know, we're kind of - we're always sort of thinking about that as, you know, I don't want to say the worst case scenario but, you know, what might be the most challenging scenario for us to try and clean up.

Amy Bivins: All right you can move on to the next slide. Okay so and most of the issues actually on the next couple of slides we've already touched on so I can go through those relatively quickly.

With respect to impacts on other stakeholders, and we've already touched on this, with respect to the registrar model, the RAA model, parties with complaints about privacy proxy services, compliance or lack thereof with the requirements for being a service, would have to go to ICANN whereas with the reseller in the escrow models parties would potentially have more than one place to go; they could go to the registrar as well.

And then with respect to enforcement powers ICANN's enforcement powers generally, you know, I mean, the way it works with the RAA is that they can terminate a registrar but they can't necessarily force or require specific performance, a relay or a reveal, it would be more about terminating the contract. So a person with a concern might necessarily - might not necessarily get the relief that they would really want coming to ICANN so that's just one thought that we had about it.

Okay. And with respect to the impact on registrars, we see - or in just talking about these different models with the registrar model we see for registrars less flexibility in the terms that they could have for privacy proxy services just because the contract will be with ICANN and, you know, all the terms will be in there.

And with the reseller model there will be more flexibility and potentially more discretion about which services they want to work with. In the escrow model, again, the terms could be limited by the ICANN approval process but the relationships part of it could be more on the registrar's terms.

And with respect to the impact on ICANN, with the registrar model, on ICANN's side there would be costs associated with coming up with an application and a process and also the ongoing account management and compliance enforcement piece.

And with the reseller model there would also be the compliance costs but those start up costs would be a little lower because there wouldn't be the whole application screening process that there would be for the RAA type model.

And the escrow model it would be similar to the registrar model, the contracting and application and screening costs and also the compliance costs. So and that's it for our slides so if you guys have questions, comments.

Mike Zupke: So this is Mike. I have a comment. So we've had, I don't know, three or four policy - or sets of policy recommendations come through implementation since the sort of - the advent of the implementation review team. And there doesn't seem to be particularly strong interest in being on implementation review teams, at least not relative to the policy making working groups.

And I just sort of want to flag that this is all implementation stuff that is, you know, is really, you know, I think near to a lot of peoples' hearts and so when

the call goes out to join the implementation review team, you know, please keep in mind the interest in these things, you know, is probably still going to be there.

But, you know, if you moved on to the next thing and you're not participating in that you sort of lose some opportunities to have a voice in that. And I - hopefully I said that diplomatically. I don't mean it as a criticism at all, it's really - it's not always as glamorous but it is important and that was my point.

Don Blumenthal: I will take the opportunity to make one final comment. As a member of an implementation team, let's talk about that offline, because there may be a chicken/egg deal going on here.

Any event, I really appreciate the presentation very helpful in both understanding what you're looking at and it, at least in my case, prompted some thoughts about some ways we might approach some of the issues we've been looking at and will look at. So thanks also for ending right about on time. And see you on some of the calls.

Mike Zupke: Thank you.

Amy Bivins: Thank you.

Man: Thank you very much. Have a nice weekend.
Man: (Unintelligible).

Don Blumenthal: Let's...

((Crosstalk))

Don Blumenthal: ...(unintelligible) these guys.

Volker Greimann: Say that again?

Don Blumenthal: Do the latecomer introduction, I forgot to do it before introducing these folks.

Volker Greimann: Shall we do that now?

((Crosstalk))

Thomas Rickert: Sure. Okay so before we move to the next agenda item can I please ask those that have not been here from the very beginning to briefly introduce themselves to the group? Volker, can I ask you kick this off?

Volker Greimann: Yes of course. My name is Volker Greimann. I am a member of the GNSO Council and member of this working group. And in severe need of sleep.

Don Blumenthal: Two more.

((Crosstalk))

Kiran Malancharuvil: Hi, I'm Kiran Malancharuvil. I am here representing Mark Monitor. Under this nursing cover is Lilly Malancharuvil representing babies. Yeah, the future of ICANN, the youngest stakeholder. Anything else you need from me about me?

Thomas Rickert: That's okay.

Kiran Malancharuvil: Yeah, member of the working group.

Phil Marano: Hi, my name is Phil Marano. I work with Katen Muchin Rosenman and I'm with the IPC.

Thomas Rickert: Who else do we have? I think Wendy...

Wendy Seltzer: Wendy Seltzer here from the - with the Non Commercial Stakeholders Group and participant in the working group who unfortunately has a standing call that conflicts with the working group's phone calls. But try to stay up to date.

Thomas Rickert: Thanks, Wendy. Now we have on the agenda now a discussion of other questions identified during the day that require further discussion. I would like to take the liberty of prescribing what the open questions are. If I may, I'd like to suggest that we spend the first half of this session to discuss the language that Mary has put into the Adobe and circulated by email since.

That has to do with the relay issue, it's only like four or five lines. So if you could please take a look at that briefly? So I'll pause for one minute or two for you to go through this. But I think it would be excellent if we could take away language that everybody is more or less comfortable with.

((Crosstalk))

Wendy Seltzer: Sorry, what language are we looking at?

Thomas Rickert: Mary has sent an email to the list at seven past one, subject, summary of working group 10-October morning session.

((Crosstalk))

Thomas Rickert: So you've got permission now to look at the email which is also on the screen.

Wendy Seltzer: Thanks. My Adobe was being slow to update.

Thomas Rickert: Steve.

Steve Metalitz: Yeah, Steve Metalitz. I think this draft approaches this from a different angle than I would approach this point. Because it talks about what the service

provider - it talks about the service providers, you know, forwarding hard cop and so forth.

I think the first point is that the service provider should notify the complainant when there has been a certain undeliverable because there's been a certain minimum number of hard bounces within a certain specified timeframe. hat's point one.

Now maybe that's not necessary because, as I mentioned, there's this whole point about having a contact. We've already agreed that there should be a contact for escalation and questions. But I think it's helpful to have this as an explicit requirement.

And, second, this kind of puts it all on the service provider. And I thought that we were talking about that if the complainant is informed that the message hasn't gotten through then it's on the complainant to say to the service provider, we want you to do something additional.

I'm not saying a service provider can't do something additional but in terms of a minimum standard I think it's - tell the complainant or the requestor and the requestor can then ask the service provider to do something extra and then we get into these issues of the cost and the fee.

But that I think is - it might be a better way to approach this rather than saying the service provider has to do something and take alternative means, whether or not the requestor asked them to do it. Thanks.

David Hughes: David Hughes. So maybe just for 30 seconds let's take a scenario of this escalation so the first thing that would happen from our side is if there was contact information that we could use, obfuscated email or however it works through the proxy service, we could send that. Let's assume that nothing happens so then we contact abuse desk or a webpage or however we go through and we send it again.

And in each step here I think what we need to do is we need to get feedback because if we don't know whether the message was relayed or not, if it bounced back or was ignored, how do we know to, you know, how can we make an informed decision about asking them to escalate?

If we got information back that said, yeah, we sent the email, it bounced but we have other information, we say well if you have other information if there's a fax number for the PDF to their fax number or, you know, send them something through physical mail and sort of escalate it back up. But with each step if there's no feedback look of information then from our side how do we request the next step? We wouldn't know to.

And as Steve said, I don't think it's reasonable to assume that the service provider is going to escalate on their side, why would they if it's not coming as a request from us. Does that make sense?

Thomas Rickert: And I think Mary is - or Marika is revisiting the draft as we move on. Any further comments?

David Hughes: I suppose that I was thinking is if you do it in chronological order, I don't know, if that makes it easier for people to understand that when this happens then this is what we expect to get back from the service provider. And depending on that then we could request escalation to the next level or something like that.

Steve Metalitz: I'm just looking at the chat here and maybe I misspoke, from what Todd has said in there, that yeah, I'll be notifying the complainant or the requestor, whatever we're calling that person, and then if the requestor wants it then this - some alternative means of trying to reach the customer.

Thomas Rickert: Holly.

Holly Raiche: I should finally identify myself. Holly Raiche. In the fourth line provided there's been a certain minimum of hard bounces, well we actually haven't put that in there. We've used, in the first sentence, probably a more accurate term simply that it was undeliverable.

Now we're not saying how or why, we're basically saying it wasn't - well for some reason it was undeliverable. And I think we ought to continue that language. Or alternative language is if the service provider becomes aware that the message was not delivered, something that picks that up. James has got a comment.

James Bladel: So I prefer the phrase delivery failure or delivery has failed rather than undeliverable. I think - and I'm struggling to think why I feel that way or articulate that. I think it 's because undeliverable seems to be just kind of a capitulation to something as impossible versus an acknowledgement that it could be a temporary situation, it could be an error somewhere in the, you know, in the pipes, but basically the delivery attempts had failed is more specific.

And I do agree that definition of that maybe doesn't belong in the second sentence but I do think that the concept is something that everyone seemed to be, you know, it wasn't one strike you're out, that there was some threshold that had to be established.

Thomas Rickert: Any further comments on the language as it stands? David.

David Cake: So again, speaking as - I don't know if I'm the only member of the mailing - or the working group that's actually tried to - actually run an email server. Speaking again, the idea that there will always be a hard bounce is not necessarily true. There's plenty of reasons why something could fail to be delivered for technical reasons that do not result in a hard bounce, I mean, there are a lot of poorly configured mail servers out there.

And some of them, for example, may be so poorly configured that they are incapable of properly sending the hard bounce back out. And in that - so I think we would be unwise to rely on that which then leads us into the problem of an email that is not delivered and does not send a bounce back is from the point of view of the outside world, indistinguishable from one that has been delivered and not acted on in any way.

So we may be, you know, it maybe we really have to sort of - when it comes down to it ignore - well not ignore but realize that we cannot 100% distinguish between undelivered and unacted upon mail and put some way in here that we can, you know, it may be just for after, you know, no responses being given for some number of days or something may have to be in there as a sort of catch for the case when no bounce or undeliverable notice has ever been put out.

Thomas Rickert: But I think, David, we've limited it to the service provider becoming aware of that. So if, you know, but I have James, Kathy and Don.

James Bladel: So I just want to put this on the table because it's something we were chatting about over lunch which is that this approach, I think the way we've discussed it thus far, centralizes all of those relay requests with the service provider and then expects them to be able to detect delivery failures, which as we discussed, could be problematic.

Whereas by providing a unique - there's another approach would be to - for a service provider to provide a unique relay email address for each domain name and have that be a one-way channel and then that would immediately deliver any bounce back or delivery failures if they were received, to David's point, back to the complaining person.

I think that would satisfy the notification requirement and the bounce simultaneously and leave the service provider out of the loop as far as detecting which bounce went with which relay request.

((Crosstalk))

James Bladel: So that would be check the box, we're done. Okay.

Thomas Rickert: Kathy.

Kathy Kleiman: Agree with James, that makes sense. I don't think we can mandate implementation but it sounds like a good implementation model that some proxy privacy providers are already providing which is that link to an email that then forwards on to the customer's actual email, that...

((Crosstalk))

James Bladel: But it's a two-way so the bounce doesn't go to the provider it just...

Kathy Kleiman: It goes back.

James Bladel: ...right back to the...

Kathy Kleiman: Which is perfect.

James Bladel: Yeah.

Kathy Kleiman: And to David's point, I don't think we can boil the ocean completely.

David Cake: Yeah.

Kathy Kleiman: I think we have to kind of deal with what we've got in light of the fact that we also have this seeming consensus that lack of a response is something that someone's entitled to as well.

Thomas Rickert: So it looks like we have a solution that everybody might be happy with only that this solution is impacting implementation. The question now is how brave is this group? The GNSO community has, at times, has complained that ICANN staff has stepped over the line with its toe by doing policy in the implementation process so do you want to return the favor with this and prescribing implementation?

I mean, you can always phrase things in a way that's technology neutral. But I think that what we have here combined with what James just said might do the trick, right? So that technical means shall be deployed that provide for a request or a notification in case notification fails. I mean, you don't have to talk about hard bounces or prescribe how things should be implemented.

James.

James Bladel: I think Steve was in the queue but I was just wondering, can we add something about explicitly say either relay the bounce notification or otherwise notify, you know, I just want to allow for the possibility that notification might be just passing that back.

Thomas Rickert: Steve.

Steve Metalitz: Yeah, this is Steve Metalitz. Thomas, I think your formulation may be a very good one which is that it should be set up in a way so that the requestor because aware when - of delivery failures. And when that happens the requestor should be able to ask the provider to make an attempt through another means to deliver the message.

So that's technology-neutral in the sense that it could either be set up the way James is talking about or if it's set up differently, you know, through a - through something in which you wouldn't automatically - the requestor wouldn't automatically be aware of a delivery failure, then it's on the service

provider to tell the requestor about that. But I think your formulation was right. Thank you.

Thomas Rickert: Kathy, I saw that you had raised your hand?

Kathy Kleiman: (Unintelligible).

Thomas Rickert: Wendy.

Wendy Seltzer: Wendy Seltzer. Wondering if we are talking about relaying notice of delivery failure that we be careful that that not turn into a reveal by relaying the actual bounce message that includes details of underlying server configurations and other details of the registrant.

David Hughes: Right. I mean, that's the responsibility of the proxy service, to provide a proxy for their customers to protect their customers' identity. So if they're a good proxy service they won't reveal.

Volker Greimann: The automated bonds, of course, assumes that each and every domain registration gets an individual email. I've seen a lot of proxy services or law firms acting as proxy service, that use the general purpose email address and then do it manually. I just don't want to hard code something into the language that takes out certain business models that make sense or...

Thomas Rickert: But we could leave the original language as alternative language to this so that the service provider can either do it, you know, upon getting aware of delivery failure...

David Hughes: It makes no difference to us if it's an automated process which makes sense for James's big company or doesn't make sense for, you know, somebody's small law firm. It doesn't matter to us as long as the result is the same.

Volker Greimann: And one more comment from my side. I would really like to see the hard copy disappear from this draft and just have alternative methods of communications, i.e. because if we leave the hard copy as a - in the draft it might sneak into the implementation in a way that is not foreseen by this group.

So it would be included in the alternative form of communication but, yeah, I'd rather not see it here because a lot of privacy service explicitly exclude forwarding of hard copy and with good reason.

Don Blumenthal: Let me just explain, Volker. This came up earlier today in the sense of forwarding a hard copy of an electronic community, not necessarily forwarding a request that came in via paper.

James Bladel: I'm sorry, I misunderstood; didn't we also talk about returning a hard copy of a delivery failure?

Man: No.

Don Blumenthal: I don't believe, not today.

David Hughes: This is David. But that's a great idea. No, no I'm just kidding.

James Bladel: I'm not clear - okay.

David Hughes: So this is David. Volker, so what we said was if we sent a notice in a PDF, for example, then you could electronically transmit it to a fax machine or you could print it out and put it in an envelope and mail it. In most cases - now there may be some jurisdictions where an actual signed or notarized physical copy has to be sent or something. But I mean, in those cases people are going to do that anyway so.

Volker Greimann: Well speaking for the privacy service that we operate we will certainly not forward any hard copy, that's an additional cost that is certainly not part of our calculation and we will not have - even if you were offering to pay for that that's not something that our business model currently allows that we except payments from other parties directly for the privacy service provider. So it's a bit problematic to have hard copy in there if there's other means of communications available.

David Hughes: So this is David again. So the conversation we had this morning was if your customers maintain their contact information correctly it will not get escalated to this level. So you could consider passing those charges onto your customer.

James Bladel: And so this is I think something that Thomas and I were discussing at lunch is we have to be very wary of any mechanism that has an asymmetrical cost structure to where the cost burdens are absorbed by a party that's not benefiting from the mechanism. And I think that goes both for the customer and for the complainant.

So I think that we have to be careful, you know, I mean, economically whenever something is free it's going to be abused. You know, and so it - even if it's a negligible cost recovery I think that will help to ensure that these types of relay requests are valid and legitimate.

But I'm curious as to why this escalation to a hard copy relay of physical or postal or whatever we want to call it, why that's part of this - I mean, isn't that two separate, I mean, you could start there if the privacy service offered that. You wouldn't be required to send it electronically. I don't know, let me just noodle on that one for a little bit. I was thinking of them as two atomic processes, not that one was the escalation of another.

David Hughes: And this is David again. And the other thing, James, is that I can't speak for all of the IPC group but I think - I personally think that it would be reasonable

for us to - and we discussed this morning that, you know, law firms have standard ways of calculating pages per copy and all that other stuff and those are the kind of fees that we would consider absorbing if - I suppose the quid pro quo here is that if we're getting feedback on the electronic notifications so that we are in a position to decide okay in this case it's worth it for us to spend money to reimburse you to send a physical delivery, does that make sense?

Thomas Rickert: James, I guess the question was for you.

James Bladel: Yeah, that makes sense. You know, we'll have to think about this one a little bit - particularly the fee structure. Because here's what I'm thinking is if you have attempted - if I have made a good faith effort to relay something and the email address is not functional, now I have to question whether the postal address is valid. And before I start - anyway.

Thomas Rickert: Kiran.

Kiran Malancharuvil: So I think I was on maternity leave when most of this discussion happened because it's not familiar to me. So this is more like a question to the group. The - in the Registrar Accreditation Agreement I was under the impression that if there is, you know, reasonable evidence that an email address is nonfunctional or the Whois contact information in general is thought to be inaccurate that, you know, the registrar then has to make a reasonable effort to verify that information. Was there any discussion about...

Thomas Rickert: Yeah.

Kiran Malancharuvil: ...that being the standard for providers? And if so why aren't we using that standard? And why are we reinventing the wheel here?

Thomas Rickert: Steve, do you want to answer that?

Steve Metalitz: Yeah, both in the - those earlier conversations and then again we talked about it this morning, yes, that requirement is passed through to the - we've recommended that that requirement be passed through to the service providers.

But in this situation I don't think we want to rely solely on that because, again, under the RAA that's a protracted process, it could easily take several weeks for that verification process to happen. So if there's another way that we can try to get the information to the customer or relay the message to the customer let's do it. But it's not an either/or, it's a both/and.

Thomas Rickert: Okay so I understand that James and others will need to think more about the language. I think we're very close to reaching agreement on that. You know, certainly this is not a consensus call but I think that we should leave it here for everybody to further think about it and discuss with your respective groups and then you will pick it up during one of your next meetings. Is that okay or does anyone of you want to make final remarks on that? No

Which is why I would then like to use the remainder of the time to get back to the reveal discussion. I need to check with Marika, how much time will you need to do the overall assessment thing? Okay so let's take like 15 minutes to maybe sketch out the next steps on how to approach reveal. And, Kathy, you wanted to...

Kathy Kleiman: The comment doesn't have to do with the - I just thought I'd let everyone know since we've all been in this room for a while, that there's alcohol being set up out there. And I don't know if it's for us but I was glad to see it.

((Crosstalk))

Don Blumenthal: Can I - you know, can I suggest applause for Glen at this point?

Thomas Rickert: But you will only get access to the booze if we reach agreement on reveal.

Kathy Kleiman: Oh well.

((Crosstalk))

Thomas Rickert: No seriously I...

David Hughes: You're going to get a couple of burnt wood messages.

((Crosstalk))

Thomas Rickert: Where do we go with reveal? I was joking when I said that time flew when we had the session, you know, some of your wanted to dive into some very specific scenarios and, you know, the session was over before we even had talked about the fundamental principles that would be applicable to all the scenarios.

I think that we've made progress on eliminating some of the stuff that we want to keep out of the conversation like law enforcement requests that were sometimes mixed with other types of requests.

But then the - I think for this group to make good progress we mustn't get lost in detail because everybody around the table has their specific agendas and requests, wishes, for the reveal situation. So I think for the initial report the best you can do is maybe to come up with some very high level approaches to things. And I think these high level approaches can be some that we've discussed earlier, and I'm not going to repeat them now.

But as far as trademark copyright and other reveal requests are concerned maybe they should be as superficial as saying a request must be sufficiently detailed to allow for the - to give the opportunity to the privacy and proxy service provider to establish whether an infringement is present or not. And then to give opportunity to the beneficiary owner to respond to that request,

set a certain time span for the response. And we heard somebody suggesting seven days response.

And then based on the response or the lack of response, you know, I would maybe use the word - should there be no sufficient response from the beneficiary owner then the privacy and proxy service provider would be entitled to reveal to the requesting party which would be a disclosure and not a publication.

Which I think improves the situation opposed to the status quo significantly. And I'd like to emphasize what James was saying earlier that at present in most such cases when a complaint is coming in the only thing that would happen is termination of the agreement, and publication. So if you reduce this to - disclosure to the requesting party I think that would be a significant step forward wouldn't it?

And then maybe another basic clause or recommendation whereby you say that this is not withstanding any termination rights that the service provider might have. So if the service provider might face liability by keeping up a side or not revealing then these termination rights that might be in the terms and conditions should remain unaltered from this.

So what I'm trying to say is I think you can't find entirely specified approaches for all types of infringements that are workable in all jurisdictions around the world. I think the best you can do in this group, at least for the initial report, is to spell out such basic principles and maybe get some community feedback on that.

James.

James Bladel: So the one thing that we were missing was the discussion about having an account - or, you know, use-based system for reveal requests so that - authentication of requestors for reveal requests. And then the concern that I

have about allow for the customer to respond to whom, to the provider or to the requestor?

I actually would say something like for the customer to take action, to remedy, to cancel, to - I mean, do we want to list the potential actions, I think, you know, I'm concerned about respond because it begs other questions like respond with what and respond to whom that - maybe we're going too far into detail for the high level principles but otherwise I would say for the customer to take action.

Thomas Rickert: So, James, I thought (unintelligible) - I thought that we had agreed on the need for authentication mechanism for requesting parties. I haven't repeated that but...

((Crosstalk))

Thomas Rickert: ...yeah. And I thought that was common sense and I've just not repeated...

((Crosstalk))

James Bladel: Oh I'm sorry, but it wasn't in your list so I...

David Hughes: James just wanted it on the record.

Thomas Rickert: Oh, I haven't looked at that list, sorry.

James Bladel: Fine, sorry. And then maybe someone can help me with we're giving them a window to do what?

Thomas Rickert: I think that's up for the group to decide. I think sufficient response would be an appropriate thing but that's certainly...

James Bladel: To respond appropriately or respond or take appropriate action, something like that.

Thomas Rickert: You can even establish a back channel for the beneficiary owner to respond to the, you know, without disclosing to respond to the requesting party. So maybe...

James Bladel: So the reveal process falls back to the relay process.

Thomas Rickert: Yeah, but if that fails then you could reveal. I'm not trying to suggest a solution here but just, you know, I think I had Kathy first wasn't it? Kathy, had you raised your hand? And then I get Paul.

Kathy Kleiman: As long as we're listing off points...

James Bladel: Wendy.

Kathy Kleiman: As long as we're listing off points and we - this is actually pulling something in from another - from a Tuesday discussion and also from Steve's draft probably a last bullet point would be or an additional bullet point would be subject to limitations on the use of the disclosed information so you can't put it on your blog.

Thomas Rickert: So, Wendy was first and then Paul.

Wendy Seltzer: Wendy Seltzer. You know, I think leaving a broad category of potential actions under that responsive action is useful. It could be a customer taking action to take down the website and clear up the reason for complaint; it could be filing a motion to quash a relevant jurisdiction and giving notice of that to the provider; and there might well be other things that would satisfy the provider and/or the requestor.

Thomas Rickert: Thanks, Wendy. Paul.

Paul McGrady: So after complaining that we never got down the track I feel like you all got on the train and - and I was still in the gift shop and trying to catch up. I just - I hate to say this but this would have been a great conversation like three hours ago. I don't know, for example, we have a word like provider may proceed to disclose, what does that mean? Must - may isn't must. You know, I just don't think we're going to be able to accomplish several hours worth of work in 11 minutes.

So, I mean, I think it's fine that we're having this conversation but this is definitely one that we're going to - whatever comes out of this 12 minute sprint so that we can appear to, you know, accomplish good stuff in this space today, we're going to have to - we're going to have to take it back and think about it. So I just don't want to - everybody to walk away from this thinking, yay, we're done because I think that this is a - this is important and it has to be thought through. Thank you, bye.

Thomas Rickert: And this goes back to the opening remarks when we said that, you know, everything that we're going to do here needs to be taken back by all working group members to their respective groups. But the intention was just to try to capture the interim results and certainly you have to take it forward from this.

Steve, was - no Volker first and then Steve I think you wanted to speak? Volker.

Volker Greimann: Yeah, having not been present at the earlier discussion I might have missed the salient points where you were also together in saying (com vaya). But I would be very cautious in having an automated process where you put an X at the top and after clunking down the chain of events then why or that comes out at the end.

First of all, the provider, in 90% of the cases, is not qualified neither legally nor competently to determine the facts of the matter and to determine the

quality or accuracy of the complaint. We receive dozens of complaints, he has stole my picture, he has stolen my text from my Webpage. How are we to quantify that? How are we to verify that?

It's - there's a lot of complaints that we as a provider simply cannot make a judgment on. And then we would be still be forced to disclose if he doesn't respond to the complainant the response to go to the complainant would mean that either we would have to forward something or he would reveal his email address to the complainant directly if we say he has to respond to that.

I think if the other party contacts us to say this is harassment, they should go away, I have nothing to do with this; this is okay what I'm doing, and this is believable then that might be a result as well. I just want to be cautious here that we don't want to have a fixed result just because there is a complaint because the merits of the complaint cannot be seen on the face of it in most cases.

Thomas Rickert: I think we had Steve next and then Kiran.

Steve Metalitz: Well this is Steve Metalitz. I was going to second what Paul said that let's not let the train get ahead of itself but I think Volker has now made that comment kind of unnecessary. But I think this is useful as a - as kind of a template for maybe the level of detail we should be striving for. The stuff that comes before this, which is what are the requisites of a complaint that would meet this threshold, this is what we tried to provide as an example for intellectual property issues. So we still have to kind of decide that.

And then obviously there's a lot of bracketed things in here as well. But I think this is useful, Thomas, as far as kind of a general framework for how - where we might want to end up in terms of detail.

I am leaving aside the question of whether we also want to give illustrative examples or work on some use cases and see how this works and maybe,

you know, incorporate that in some way. But I think it's helpful to have this. And I think there are obviously a number of issues that still need to be worked out.

Thomas Rickert: Thanks Steve. Kathy.

Kathy Kleiman: Given that we were talking about all these different categories, law enforcement, abuse, defamation, it seems to me the intro to this section might be - and correct me if I'm wrong - would be for an intellectual-property complaint stated with great specificity including - and here I'm just trying to summarize what you had, Steve - including the identification of the intellectual property owner, the intellectual property, the infringement and I would add and the representative who's making the complaint because it may be a lawyer.

So that's the introduction to this category because we did agree that these points don't apply to everything and they certainly don't apply to law enforcement and we haven't really gotten into abuse and the special cases involving abuse. So happy to read that back. Did that sound right or wrong to people, for the broad brush that we are doing.

Thomas Rickert: I think that's helpful, Kathy. Kiran.

Kiran Malancharuvil: So, yeah, I guess being at the end of a long day this might come across as a little confused by it I agree with Volker - shocker - that it's...

((Crosstalk))

Kiran Malancharuvil: Is this transcribed? I'm screwed. But the - asking the provider are really anybody, and I think I've said this before, to make a decision on the face of a complaint is just a really bad idea, whether as a result of that is that the provider has to force a disclosure which is not ideal for their customer or

whether, you know, they're going to deny relay or whatnot as a result of making a determination on the face of a legal complaint.

So I think it's really important when we put high level standards in place that we're not saying that a determination should be made by the provider but rather that, you know, maybe there is a prima facie case that's made by the complainant.

But I think then that raises the question about - that the registrant needs to respond. And there's been a lot of discussion about well they have the right not to. And, you know, certainly they do have the right not to, you know, people have the right to ignore whatever they want to ignore to a point, right.

And maybe in the terms of the services for the use of these kind of services we say, you know, you have to respond because if you're not responding to the request then we are going to, you know, say that a prima facie case has been made because if they just have the right not to respond then we are at a loss on our end what do we do next? There's no next step for us.

If there's no response and they have the right to do that and then there's no due process for us on our side of it. So there's a lot of really complicated factors with this. So boiling it down to these bullet points is making me really uncomfortable I guess. So I guess in all circles back to Paul's comments. Thanks.

Thomas Rickert: Thanks, Kiran. Don.

Don Blumenthal: Just real briefly just another situation where the model we're focusing on may be different in the abuse area. It's relatively, you know, obviously if you have somebody who knows what to look at it's really relatively simple to verify whether there's any merit to an abuse complaint. I can do it in about five minutes or less.

So again we've got a situation where our models may be different and then the question is how much we have to account for the different ones or just come up with a high level description - high-level principles.

Thomas Rickert: Thanks Don. I have Volker and then Steve and then we have to call it a day.

Volker Greimann: Well, Kiran, that must be cause of both of us being young parents now so...

((Crosstalk))

Volker Greimann: That may be behind it. But I agree that there must be due process in some form and that's something that I tried to address in the draft I sent around last week - this week - where I said that maybe a good faith belief might not be enough but a sworn statement that we could take to court that the complainant is willing to stand by in court if it comes to that and be sued about and sued for damages might be sufficient for a cause of action that the provider can rely on.

Thomas Rickert: Steve.

Steve Metalitz: Yeah, this is Steve. So, Volker, since your plane was delayed so we have some discussion about my proposal or the proposal I put forward and we're going to get into responses to yours so we didn't really get a chance to do that.

Let me just say very briefly that I think there is a lot of overlap. I think that your last point, we can address that with a statement under penalty of perjury; that may not mean exactly the same thing as what you're talking about but it's I think somewhere in the same - on the same terrain.

I think the main concern that we had - that I had with your edits was kind of in the general policy paragraph where you really just kind of flipped everything we said on its head. I think we can get beyond that because I think that, as I

said, I think there really is a fair amount of commonality and with some additional elements that have been brought in here.

I think that - I appreciate you giving us such a quick response on that, number one. And number two I think it was constructive so let's keep moving from there. Thank you.

Thomas Rickert: Thanks, Steve. And with that I think our conversation for today is more or less over or we continue the conversation over wine and beer. I have promised to reserve the last 10, 15 minutes for Marika to do the evaluation part because, as you know, this pilot is to be examined, assessed.

I think you shouldn't be frightened by the level of simplicity of these bullet points. I mean, this was clearly meant to condense down to the very complex discussion to some points that you could work on and she can put all the detail in it that you want to if you can comment if you reach agreement on them.

But I think that with this exercise maybe we've achieved to narrow this down to some principles that you can further work on. With that, I think my facilitation role for today is over. It's been very interesting and informative day. I thank you all for your valuable contributions. So I hand back over the mic to Marika, Don, whoever. Thanks.

Marika Konings: So this is Marika.

((Crosstalk))

Marika Konings: Oh you want to go first.

Don Blumenthal: Just a couple comments and then people do evals and go drink. Just real quickly, this has been an excellent experience I think. I just wanted to make a couple of suggestions for moving forward. Obviously what we've come up

with today there's a lot of people who weren't here so we want to comment you know, you get feedback from them.

There were a couple comments toward the end here about their points we didn't touch. And I'd really appreciate if there's things you think we need to follow up, you know, let us know, send an email to the list, to the chair group whatever, so that we know what we need to follow up on here because that's going to - that's what's going to make this exercise complete.

We're still working on a timetable for moving forward. There's going to be a lot. Fortunately there's no call next week so we won't have to worry about templates by then. But I'd like to impress that we're not done here, we're not done with today's work and we probably won't be for at least a couple of weeks.

So to the extent you're going to be discussing what we talked about I would hope that, you know, I probably will be but I think it would be best to discuss what we talked about, the topics that came up in trying to avoid characterizing the discussions and certainly avoid characterizing any conclusions because fundamentally we don't have any yet. Just a request.

And now for the paperwork.

Marika Konings: Yeah, so this is Marika. So indeed before you get to the booze there's a little bit of homework to do. So first of all I want to all thank you for, you know, taking part in the day and, you know, spending your day here inside even with a little bit of light outside.

But for us it's really important to get some feedback on what your experience was not only from the perspective of, you know, meeting today and how that can be improved but also in the overall context of how this may help PDP working groups. Because I think as most of you know this is part of a pilot

project so we'll the writing similar meetings at the next meeting and the meeting thereafter.

And at the end of that year basically we'll do an evaluation and have a discussion around whether this is something we should be continuing, you know, changing, modifying, stopping altogether. So we really would appreciate if you can just, you know, take a couple of minutes to fill this in.

And then maybe we can still do a little brief round where just people, you know, state what they thought was useful, what they thought was less useful, what should we be improving and, you know, is this something worth considering, you know, implementing as a more kind of standard feature for PDP working groups when needed.

So I'll just hand out the forms and then you get 5 minutes and then maybe we can do a quick round if people just want to throw out some things and then you can get drinks.

I just sent the same form on the mailing list as well for those that were participating remotely or had to leave early. So it's the same form so people prefer to fill it in electronically. But the main reason why we are handing it out here we often get a better response rate if we ask people to do it before they get drinks, it seems to work very well.

(Chris): Have a wonderful weekend all.

Don Blumenthal: Thanks, (Chris).

((Crosstalk))

Marika Konings: So if people are finished with their homework and wrapping up maybe some people want to just, you know, share with us what they thought we should do

more of, less of, what should we keep the same, any general comments people would like to share with the group.

James Bladel: Where'd the facilitator go?

((Crosstalk))

Marika Konings: Thomas is here. The thought this group was such a disaster that he just...

((Crosstalk))

James Bladel: I indicated that, you know, how can I give feedback? He made his introduction and then he was...

((Crosstalk))

Marika Konings: Yeah, no unfortunately he was unwell and basically went back to bed.

((Crosstalk))

Marika Konings: And he was really sorry about that.

James Bladel: I thought we were so well behaved he's like, my work here is done.

((Crosstalk))

Marika Konings: Exactly, he gave up; he gave up. Any other...

Thomas Rickert: Everybody to the...

((Crosstalk))

Marika Konings: ...comments people would like to share or...

Kiran Malancharuvil: I'd like to give thanks to Mary and to Thomas. I thought she did excellent job facilitating.

Marika Konings: All right well I think it's time for drinks with that during thanks everyone.

END