ICANN Transcription

Privacy and Proxy Services Accreditation Issues PDP WG F2F

Friday 16 October 2015 at 10:00 UTC

Note: The following is the output of transcribing from an audio recording of Privacy and Proxy Services Accreditation Issues PDP WG call on the Tuesday 16 October 2015 at 10:00 UTC. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.

Steve Metalitz: I want to welcome everybody to this meeting. I'm Steve Metalitz. I'm the co-chair of this group, and I know some of us are meeting each other in person for the first time. So the first thing we'll do is go around and introduce ourselves.

But I just want to say that I think we have covered a lot of ground in this process and I feel like we have some momentum. So I'm hoping that we can capitalize on that today and bring this closer to fruition after two years. So I'll stop with that.

I'm Steve Metalitz, and I will pass it along.

Victoria Sheckler: Victoria Sheckler with Recording Industry Association of America.

David Hughes: David Hughes, Recording Industry Association of America.

Christian Dawson: Christian Dawson with the Internet Infrastructure Coalition.

Todd Williams: Todd Williams with Turner Broadcasting.

Kathy Kleiman: Kathy Kleiman with Fletcher, Heald & Hildreth and NCSG. And it's great to meeting people face to face for the first time.

Michele Neylon: Michele Neylon, Blacknight. Also with the ITC, now that I think of it, and lots of other things. And welcome to Ireland.

Chris Pelling: Chris Pelling, (unintelligible).

Volker Greimann: Volker Greimann, Key Systems and GNSO councilor.

Stephanie Perrin: Stephanie Perrin, NCSG and GNSO councilor.

Paul McGrady: Paul McGrady, e-mail enthusiast and I'm here with IPC member (Pat On).

Griffin Barnett: Griffin Barnett from (Mayer Brown), IPC as well.

James Gannon: And James Gannon, security consultant and CSG.

Lindsay Hamilton-Reid: Lindsay Hamilton-Reid from (Fallsace) and 11.

Holly Raiche: Holly Raiche, Internet Society and ALAC.

Amy Bivins: Amy Bivins, ICANN staff.

David Cake: David Cake, Electronic Frontiers Australia, and NCSG GNSO councilor.

Mary Wong: Mary Wong, your friendly neighborhood staffer for this working group for the last two years.

Graeme Bunton: Graeme Bunton, Tucows Registrar, co-chair of the working group. And I don't know if it's official yet but I think I'm vice chair now of the Registrar Constituency too.

Michele Neylon: You're elect.

Graeme Bunton: Elect.

Michele Neylon: Yes you officially get seated on Tuesday.

Graeme Bunton: Oh okay. Not quite yet.

Michele Neylon: Well it's fine. I'm quite happy to delegate pretty much 50% of it to you so, you know.

Graeme Bunton: Thank you. So welcome again everybody. We have a pretty good solid day here of work to get done. And as Steve was saying, we've got some momentum and it would be good to carry that forward.

So the first thing we're going to do is we're going to look at some of the issues we identified when we went through the public comment review tool that we flagged. That document should be on the wiki. It should also be in your e-mail.

We've got about 45 minutes for this session. There's at least one topic in there which will require some discussion. And it's first on that list, but what I'm going to try and do is actually leave that one till last. I want to save about 25 minutes of -- at least -- of this discussion for that. And that is whether lawyers or legal services firms need to be accredited. So we're going to come back to that one.

And I'm hoping that we can move through some of these other issues hopefully very quickly, and by very quickly I mean very quickly. And then we

can come back to that issue. So if everybody's ready to go, and we know who we are, then let's get going.

So you can see there we're going skip that clarify whether the privacy and proxy service definition includes lawyers. I'm going to go right to B, which was the definition of LEA. And we had some discussion about this and we ended up deciding that, or getting to a point where I think there was some agreement, that we could link the definition of law enforcement authorities to the 2013 RAA, and any changes in that would be reflected in privacy and proxy.

So we've discussed that a bit and let's just see if there's any issues on that from around the room and hopefully not, and then we can carry on. Anybody have thoughts on linking the definition of law enforcement to the 2013 RAA? Kathy?

Kathy Kleiman: I just, I wanted to ask a question, which is has there been any issue with, you know, asking registrars in particular? Has there been any issue with the definitions? Is there - is it clear enough? Have any questions arisen that we would want to clarify here, based on the definition in the RAA?

Graeme Bunton: Thanks, Kathy. And actually just a reminder that I'll get smacked from staff if I don't say please make sure that you introduce yourself at the mic when you're speaking. And this is Graeme for the transcript. I see Michele has put his hand up. I'm going to interject myself as a registrar.

For the most part, there are not issues. There were some questions around the -- I don't have the language immediately in front of me -- but I think it was quasi or arm's length, and that has caused some consternation. But my sense is that the inconvenience of not linking these two things overrides the problematic definitions inside of the RAA.

Michele Neylon: Thanks. Michele for the record. I think, you know, I would agree with what Graeme said. I think one of the issues I think would arise on a per jurisdiction basis more than anything else, here in Ireland for example we have one law enforcement agency and one only, whereas in, say, the U.S. you potentially have thousands.

So I think the complication there is more - has potentially more to do with, you know, who is included in law enforcement in jurisdictions where you potentially have hundreds, if not thousands, of agencies. But for me as a registrar, I don't care. I only have to deal with one. We have a consumer protection agency as well. That's clearly defined. It's not an issue for me personally but I think for some - in some jurisdictions that could be a problem.

So I think the issue that Stephanie has raised a couple of times in the past is -- I'm not sure it's so much in this group but definitely in the EWG -- she would always talk about the dog catcher. So the dog - does a dog catcher have standing. That was the thing.

Graeme Bunton: And I think if those problems -- sorry, this is Graeme for the transcript again -- I think if those problems are true then we deal with them at the 2013 RAA level and then they filter through.

Cool. I see lots of nodding heads. Excellent. We have one issue settled.

Next on the list is going to be requirements to label. So there is - we had some discussion, and it's in our final report, that we have a recommendation to label privacy and proxy registrations as such in the Whois. There was some concern raised in the comments about -- and we flagged this for this discussion -- is that labeling as such reduces the benefit or value of such a registration.

And the proposal that the chairs have put forward is that we continue to label privacy and proxy registrations. I have my own thoughts but maybe I'll hold

off and see if there's any concerns with the issue of labeling privacy and proxy sort of aside from implementation issues that we have no idea if that's possible or not. I see Michele's got his hand up. I'm not looking at the queue in the room at the moment. Maybe Mary you can look at that.

Mary Wong: Yes, James Gannon.

Michele Neylon: Michele again. I think in some respects labeling that this is using a privacy proxy service could...

Man: Sorry my fault.

Michele Neylon: Excuse me whilst I wait for my technically challenged registrar colleague to work out how to use his laptop. The - I think in some respects that actually would solve certain types of issues that we face, because if somebody looks at the Whois output on a domain name at the moment and sees an entity that's affiliated with the registrar or whatever, they might think that the registrar is, or its affiliated entity, is doing something specifically with that domain name.

Whereas in fact if it's labeled as a privacy proxy registration, okay sure I'm not saying that the registrar doesn't have anything to do with it but it's pretty clear that the registrar isn't the one actually running the services associated with the domain, if that makes sense. I don't know if I'm being clear or not. No? Maybe perhaps? Okay. Help me out here. Okay, but that's kind of something in my mind.

Because we've had the situation where people have come to us and tried to say that we are doing X and we are doing Y, and (unintelligible) is not us, it's one of our clients. You know, we are not the registrant of that domain names, it's our client.

Graeme Bunton: James?

James Gannon: Thanks. James Gannon. So I know you mentioned possibly not looking at the implementation side of things, but as to whether we label or not, personally I'm slightly ambivalent about it. I don't have a strong opinion either way. But when it comes to implementing a possible decision on that, we have to be aware of the potential workload that we may put in if we're talking about possibly doing new Whois records, new fields.

You know, we need to be careful about how we define that and it can't be interpreted in such a way that might put additional technical restraints onto registrars and how they're going to manage new fields in the Whois. And I think we need to stay away from that if we do go down that road.

Graeme Bunton: Thanks, James. I think that's a concern, and my sense is that is dealt with in implementation.

Any other comments on the issue? We're okay with labeling? Awesome. Moving forward. Two down.

The next one that we'd flagged to talk about is from preliminary recommendation number eight. And this is the option of service terminated in lieu of disclosure or publication. And there was whether the option to have a registration cancellation should be prohibited, and the proposed response is that it shouldn't be prohibited but it should be up to the service provider whether they offer that as an option or not and it should also not be mandatory to offer that.

Michele?

Michele Neylon: I'm enjoying the fact that I'm on the correct time zone. So I'm at a slight advantage to the rest of you. This is awesome.

The one thing I suppose that we should make clear here is that if the domain is subject to a UDRP, cancellation should not be an option. I just think - it just struck me as being an obvious one because that would really drive people nuts that if your people were to cancel domains as soon as they got a UDRP. So I think that's kind of forbidden. But it's something that actually came up in a recent case involving - Volker, what's the name of your favorite competitor again?

Graeme Bunton: Open TLD?

Michele Neylon: Yes, them. Because they cancelled the domains instead of actually letting the UDRP go through, which they're not meant to do. But it'd be the same here. If it is subject to a UDRP, you should be able to cancel it, I think.

Graeme Bunton: Okay thank you. I think that's a good point. We can capture that. Anybody else have thoughts on the issue? I see Stephanie's hand up.

Stephanie Perrin: Stephanie Perrin for the record. Is there not some way to narrow this down to the user cancels the domain, not the provider? Because that was the concept. The concept was you give the user the option: reveal or cancel.

Graeme Bunton: I think they can request that of the registrar, but I don't know the capability for a user to actually cancel their own registration. I don’t think it works that way.

Stephanie Perrin: Why not, said the consumer advocate.

Graeme Bunton: Please, Michele?

Michele Neylon: Did somebody turn off the mic? I'm sorry. Michele speaking again. I'm getting feedback. The issue really is that the ability to cancel or to register a domain name is a contractual arrangement between a registry and a registrar. It's not between a registrant and the registry. So in order for a registrar to offer a facility it's because they're passing through something they're able to get from

the registry. So you can't bypass that completely. I don't know if you fully understand what I'm getting at.

Stephanie Perrin: Stephanie Perrin again. Well I do. It just strikes me as a contractual weakness that the end user has so few rights that's it's really - they're treated like some kind of dumb end user. I should be able to say, "Right, I no longer want the domain. Shut it down. Bang." And you should be obligated to do that for me immediately.

Michele Neylon: It's Michele again. Okay if the domain is subject to a UDRP, you could just not contest it and just say, you know, transfer the domain to them as well. That's an option as the respondent.

Graeme Bunton: I see Kathy had her hand up.

Kathy Kleiman: It might be worth clarifying that we're talking here about the disclosure. This is a reveal of publication request. That's what we're responding to here. So other things like UDRPs might be somebody else. Are we echoing? Hm, okay.

Stephanie, would this solve your problem? At the last line looking up: it would be up to the provider's discretion to offer and apply a cancellation at the request of the customer. And I'll just add, this is very important provision. I'm glad it's there.

Graeme Bunton: I think I saw Amy.

Amy Bivins: Yes, and this - it veers over into implementation a little bit but staff has a question just about your intent regarding the disclosure portion of this related to the accreditation of privacy proxy providers that are not directly affiliated with the registrar, just about how disclosure would even work. So just any insight you guys can provide on that would be great.

Steve Metalitz: This is Steve Metalitz. I think the problem isn't how disclosure would work, the problem is how this kind of provision would work, because that type of provider wouldn't have the ability to do this. So. That's one reason why - that was one argument against making it mandatory.

Let me just say this is in here because some commenter said it shouldn't be allowed, and then other people around this table have said it should be mandatory. And I think where we've come down is kind of in the middle. It's provider's discretion. I think the suggestion to add those few words at the end at the request of the customer makes sense, because I think that addresses Stephanie's point. But it still is a matter of discretion for the provider as we - at least that's where we've come to rest so far.

Graeme Bunton: Stephanie?

Stephanie Perrin: And this may be a matter of implementation as well but I have a cluster of questions about how some of the things we're coming up with will be implemented with the unaffiliated providers of proxy services. It - my understanding, and please correct me if I'm wrong, but my understanding is that these guys will not be accredited and therefore allowed to offer the service unless they agree to these provisions.

So for this particular instance where, yes, they're not operating the switches, they're not the ones with the agreement with the registry, but if they don't provide that option, with the caveat that it's up to the policies - up to the discretion of the registrar, then they won't be accredited. In other words, it's not mandatory but the option is - you have to state what you're going to do so that the customer can make a choice, you know? Not in each instance. I mean generally, you know?

So an unaffiliated privacy proxy service provider might say, "We will never shut your domain down at the request," in which case the consumer has the option to go to another privacy proxy service provider who has a clause that

says, "Under normal circumstances we will terminate a domain at customer request rather than do a reveal." Am I being clear?

Graeme Bunton: I think so. This is Graeme.

Stephanie Perrin: It gets a little convoluted. If we were to make this mandatory, then they would all have to at least consider the requests, right?

Graeme Bunton: Right. And that's not going to be the case. It would be in the sort of terms of service of the privacy proxy provider whether they offer the service not and the consumer could choose a privacy and proxy service provider that said this was something they did or they could pick someone else.

Stephanie Perrin: But the accreditation provisions will dictate that they have to at least enumerate it in their terms of service as how they're going to go. Have I got that right?

Graeme Bunton: If they're going to do it, yes I think that...

Stephanie Perrin: Or if they're not going to do it.

Steve Metalitz: Excuse me, I'm sorry. If I'm not mistaken, and Mary can correct me if I'm wrong, I think in our conclusions we say they have to say whether they have this policy or not.

Graeme Bunton: Cool. I think we're good on that one then. I'm mindful of time, that we want to get through a couple more and then we get to the lawyer issue. So let's keep going forward.

Part two, preliminary recommendations 10 through 15. Recommendation number 11, designated dedicated. Someone flagged this again, but I think we've had a bunch of discussion on this, that a designated contact was just fine rather than dedicated. It doesn't need to be an individual that is specified

by name. It can be a team, as long as they fulfill the operational requirements.

I don't think that's controversial, but if anybody has an issue there, I'm willing to discuss. Any hands? Great. Easy. Designated contact it is.

Number 13 was consider extra territorial issues in determining what is malicious conduct. And I think there is some concern. I see Stephanie's waving her hand. I see James Gannon is waving their hand. Kathy. Great. We have a bunch of people in the room too. I think there are still empty chairs, so if you can find one, please do. There's one beside me. There's one beside Mary. There's two beside Amy, one beside Holly. So please join us at the table.

Mary Wong: And please state your name before speaking.

Graeme Bunton: And always make sure to state your name before speaking.

So where are we at with this guy? The working group's recommendations here are just starting points for further implementation work. Perhaps adding phrases such as in accordance with applicable law when stating the need for flexibility will help clarify this.

So we referenced a number of possible different sources for defining malicious conduct. And I think the sense here is that we want to ensure that we're not forcing people to do things outside of their national law, which I don't think we could do anyway. But I saw Stephanie, then James, then Kathy. We're going to make our points concise, super clear and brief so that we can get through these next two bits and then come back to the lawyer issue. Cool? Great. Stephanie?

Stephanie Perrin: Stephanie Perrin. You're going to hate me because I'm still back at the previous agreed response. Just a brief question. On the dedicated versus

designated contact thing, the next thing says it may be a team or process. Does this include a bot? Like can you - can it be a mechanical or piece of software, or do we care?

Graeme Bunton: That was not the intent of the language. The intent was that it goes through a ticketing system or something like that, but the automated - it's not an automated response process. It has to eventually end up with a person.

Stephanie Perrin: Should we not be clear that there has to be a human involved? Because process is pretty vague.

Graeme Bunton: Sure. We can find some words there that it has to see some sort of human review. That doesn't - I think it would ultimately, wouldn't it?

Michele Neylon: This is Michele for the record. I'm confused what the problem here is, because, okay, just speaking as a - putting my hat on as a hosting provider and a network operator, we have an abuse desk. Not we don't deal with the volumes of abuse reports that, say, a Verizon or even our At Large ISP like (Air Com), who are now called (Air), would have in this country, but we still get enough of them that it landing in people's inboxes would be a bad idea so it goes through a support desk system. It's a ticketing system.

Some people use Kayako. I mean ICANN compliance uses Kayako. We use Zendesk. Other people use a whole variety of different things. But unless we see (unintelligible) machine-generated complaints, then every single complaint that we get is going to be reviewed by a human being.

So it kind of - it has to be. We have an obligation and we have an obligation as a network operator to kind of look and make sure our network is kept clean. So I'm not really sure what the problem is. I mean I would have a much bigger problem if you were to say that every single complaint has to be routed to Michele Neylon, because at which point I would throttle you probably, you

know. But it's going - they have to be reviewed by a human. I mean it has to be processed.

Now there might be some automation in order to help filter them. I mean if you were dealing with, say, oh I don't know, let's say you were dealing with a few thousands complaints per day, you would probably parse those emails for certain keywords so that they would end up in the right place. Because in a larger team I can imagine that, you know, stuff that's flagged as, oh I don't know, malware, you might want to filter through to a security team.

If you see the keyword copyright or trademark, maybe you want to send that to a legal team. I don't know, I'm just thinking. This is off the top of my head. So, you know, using automation is not a bad thing as long as there's a human at the end. But you'd end up with that. I'd be overly - I'd be very, very cautious about getting too far into the weeds on the wording on this because it'll end up biting everybody on our collective asses.

Graeme Bunton: Thanks, Michele. And I think that's a good point that we don't want to wordsmith this too much. Process is meant to be what he's describing there. I don't think we necessary have...

Stephanie Perrin: Please understand it was just a question, not a suggestion. I'm just wondering. As a consumer we all know that it takes you an hour to get a human to talk to you about a problem with certain companies and types of regulated industries.

Michele Neylon: Michele again. Just very briefly. No, I appreciate that, Stephanie. The thing is that you've got to realize that, you know, in the registrar hosting domain Internet space, you know, you have companies that are operating literally out of people's bedrooms with two or three staff and they're perfectly functional. You've got other companies with offices spread across the globe with thousands of staff and a totally different set up.

So what I'd be very, very cautious around is getting too far into this. I mean if your concern is that...

Graeme Bunton: You're going too far into this anyway.

Michele Neylon: Okay sorry.

Graeme Bunton: So I'm going to cut you off there. And we've only got about sort of 15 minutes left in this session, which isn't as much as I would like. Should we park the law enforcement for - or the lawyer thing for now and come back to it this afternoon?

Steve Metalitz: No let's do it.

Graeme Bunton: Let's do it now. All right, so we're going to circle back to the beginning and we'll come back to the remainder of the issues in this sheet hopefully later this afternoon. So we flagged - so we're going back up to the top here to talk about who the privacy and proxy accreditation regime should apply to, and we've got three people pegged to talk about this. I think it's Paul, Stephanie, and Volker. And we're going to hear from each of them for a minute and then we're going to have some more discussion about this.

Steve Metalitz: Can I put it in context for a couple seconds?

Graeme Bunton: Please.

Steve Metalitz: Thank you. Steve Metalitz. So right now there's nothing in our report about whether lawyers and law firms have to be accredited. So the question is should there be an exclusion there. And what we've asked each of these people to talk about is what do they see as the practical problem if there is an exclusion or if there isn't an exclusion from their perspective. So that's really what we've asked each of these three to tee up.

Graeme Bunton: Do we have a volunteer from one of you three to get us going? Volker Greimann, please.

Volker Greimann: Okay I'll pack away my 30-page summary document that I prepared. No, kidding. Going back into the history of why we're all here is that we have an interest in regulating privacy proxy services of all kinds. We have regulation sort of that was agreed between ICANN and the registrars as a temporary measure that is included in the 2013 RAA, but everybody agreed that this was not sufficient as it didn't apply to all providers.

We are here to find a solution that would be applicable to all providers equally. In other words, if we are now creating a subgroup of providers that would be exempt, then we've been wasting our total times here because we are trying to get something that applies to everyone, and creating loopholes for single professions isn't what we're here for. We can just go home and stop all this.

Graeme Bunton: Concise. Thank you. Stephanie, you look read to go.

Stephanie Perrin: I am indeed. Stephanie Perrin for the record. I have a few points. Number one, the whole concept of having lawyers have a separate status and being exempting from this sets up a two-tier status. Those clients with money will be able to hire their lawyer and those without won't. There are - why this is problematic of course is the potential application of solicitor current privilege to protect the identity of the substantive user in the event of a reveal requirement. And this essentially, again, sets up a two-tier kind of regime, where we don't - where we're not operating under some of the rules.

Now we understand that there are differences in how jurisdictions or countries apply the use of solicitor client privilege, but in many countries the lawyers will fight to the death before they reveal their clients, right? There's no fair way to differentiate between a trusted bar and an un-trusted bar, from an international perspective.

We've already got labeling so that we know -- at least we've agreed on the labeling this morning -- so we know that it's a proxy registration, so that's good. We'd like to see that the contract that the client must provide for accommodation of the accreditation requirements of ICANN, because in a way there are very few ways to touch lawyers who are acting for their clients.

So if you don't accredit the lawyers and require them as a condition of offering this service to meet the requirements, you're going to be in trouble. You're not - we're not going to be able to enforce it. So it has to be in the contract with their clients and that has to be passed on through the accreditation agreement.

And in terms of implementation problems, I see it as a similar problem to the problem of enforcing this or making it implementable with the unaffiliated privacy proxy services, except in this case they'd be lawyers. The other this is if we do create an exempt category, it's going to draw out all the bad guys to it. That might be very convenient for our law enforcement buddies, but I don't think it solves the problem at ICANN. So that's my two bits.

Graeme Bunton: Thank you, Stephanie. Next up we'll hear from Paul, and then we'll open the discussion.

Paul McGrady: Paul McGrady for the record. So the bottom line here is do we really think that lawyers and privacy proxy services are the same thing. Are privacy proxy services agents for their clients such that they're responsible for the actions of their clients and/or are they address alternatives with some communication forwarding?

If privacy proxy services are agents of their clients, then that's a different discussion, but that's not the discussion we've been having for the last 18 months. The right to counsel and the right to act - have counsel act for you anonymously has been recognized for hundreds of years.

Those of you who are friends of literature will recall from Great Expectations that Abel the convict used counsel to anonymously act for him in order to provide for Pip so that Pip would take the money and would benefit himself. So this is not a new concept for most cultures.

As I said, attorneys are agents for the clients. They're subject to regulation by bar associations, by state, federal courts. In the event that there is an attorney who decides to use his practice to open up a sub business to make sure that all the bad guys have a place to reside to avoid disclosure of their identities, it won't be long before that attorney finds himself in hot water. And there's already a regulatory scheme in place. It's a regulatory scheme that's far more robust than ICANN could possibly hope to be in any event.

So far harms haven't been identified by - certainly by the providers in the event that ICANN specifically excludes attorneys as not being privacy proxy services, because they're not, they're attorneys. Then there would be no compliance issues if a registrar accepts a registration in the name of a law firm. The exemption needs to be explicit around the table (unintelligible) in the community who do not see the inherent distinction between a privacy proxy service and a law firm. And so in order (unintelligible).

I don't have enough time to tell you a couple of stories but I could share a couple of stories about how this fits into the protection of individuals, if you'd like, maybe over coffee or if I'm granted an extra minute. So - but the biggest concern I have frankly is pushback by law firms who have no intention of letting ICANN regulate them.

We've done a lot of good work here. This seems to me to be a bit of a cul-de-sac to go down, but if that's something that is - we are going to propose as policy, I think you'll expect to hear from law firms. They simply are not going to let ICANN dictate what language goes into their engagement letters with their clients, period. It's not going to happen.

Importantly, no harm has been identified by the providers. From a consumer standpoint, again, I think that there are - there's great concern about the protection of people who are no longer able to access counsel for them to act. And again, I'm happy to share a few examples of that if there were more time. I'm sorry this has been so rambling, and I'm happy to answer any questions that my rambling has caused.

Graeme Bunton: Thanks, Paul. And thank you again, Volker and Stephanie. So we've got some positions laid out. I'm seeing some hands going up. I've got Holly and then Steve and then Volker in the queue, and then Amy. Go ahead, Holly.

Holly Raiche: I don't think we want to revisit it but let me remind people we very, very early in the piece said we were not going to distinguish between privacy and proxy. Now in the Whois report that some of you may have read, the final report made a distinction between actual privacy services and proxy, which was actually an agency and in fact adequately completely described a relationship between a client and a lawyer.

So if we're having this debate and we can't solve it, if we go back to that definition, that was a reasonably clear definition of what we're actually trying to overcome and we decided we're going to push the two categories into one, maybe a solution is to disentangle that. Thanks.

Graeme Bunton: Thanks, Holly. Steve?

Steve Metalitz: Yes thank you. Steve Metalitz. I guess I'd like to ask a question to Volker and I guess since he's next in the queue he can answer it then, but it also may apply to Amy. And that is what I didn't here in what you said is what you think the harm is to you as a registrar. Under this system, the registrar cannot knowingly accept a registration from an unaccredited proxy service, or privacy service.

So if you get a registration from Paul's law firm and you note that Paul's law firm is not on the list of accredited proxy services, are you going to reject that registration or do you fear that if you accept that registration, Amy will come after you, or ICANN compliance will come after you? I'm just trying to understand. I get the theoretical arguments here but I'm trying to understand the practicalities of this. Thanks.

Volker Greimann: Well under the definitions of our current plan, the - Paul's law firm would be an unaccredited provider. And if we were to see that he's providing services as a privacy service provider without being accredited, we would not be able to - or allow to take his registration. So taking his registration knowingly would put us at risk with our own accreditation terms, at least under the current regime.

If we created a carve out, then I see problems with creating loopholes that might be abused down the line and also a problem of equal footing for providers of privacy services, because lawyers would be in a very much better position to provide these services than we as registrars would be. Why should a lawyer be treated differently just because of historical reasons? I don't see that.

Graeme Bunton: Thanks, Volker. I've got Amy and then Paul in the queue, and then Kathy. Did you have a response too, Steve?

Steve Metalitz: No, no.

Graeme Bunton: Okay. So Amy, Paul, Kathy.

Amy Bivins: This is Amy from staff. On the implementation side, just thinking ahead, we just have questions looking at this. You know, if you want these recommendations to cover attorneys or unaffiliated providers as well, we're trying to figure out how to write this into a policy that people are actually going to abide by and that people are going to sign up for accreditation.

And our question is, you know, for unaffiliated providers and attorneys too, how is the registrar going to know that these people are privacy proxy services? You know, if it's John Smith that's a solo practitioner or something like, like how would the registrar know? So those are just things that we're thinking about.

Graeme Bunton: Thanks, Amy. I - from a registrar perspective, if I can speak for a moment, I think we know when we - for an individual registration, we would almost never know. I think when you get into where there's many registrations, then it become possible to find out. And certainly there are people who have a cottage industry of pointing out to registrars where they're in violation of Whois accuracy or accreditation regimes that would certainly point this out and complain to ICANN compliance that we're violating the rules.

I've got Paul, Kathy, and then Stephanie.

Paul McGrady: So the cottage industry you mentioned is perhaps another reason why the exclusion needs to be explicit. The concern of course is that what will happen if it's not explicit is what we've heard around the table, which is that every registration from every law firm, every registrar will feel like they need to go back and ask that law firm is this on your behalf or on your behalf - or behalf of a client for whom you're acting, which again, the distinction between acting to provide an alternative address and acting as counsel is very much a different concept and whether it's rooted in history or reality, or both in this case.

So what we want to do is to provide clarity for the providers that they don't have to do that, that there already is a regulatory scheme in place that is, you know, robust and sufficient to ensure that in the event that law firm is creating a safe haven for bad actors that the bar associations and the courts that govern lawyers are more than capable of handing that through their regular complaint process.

So again, clarity of an exclusion provides clarity for the registrars. It relieves ICANN of the duty to, you know, to deal with the compliance issues with providers around that issue and provides certainty in the marketplace.

Graeme Bunton: Thanks, Paul. I've got Kathy and then Stephanie in the queue.

Kathy Kleiman: The concerns on this issue go back to our very first meetings. I'll never forget Elliot Noss at the microphone talking about this repeatedly, as did others. So, you know, I'm glad we're circling back. Thank you for the time today to talk about this.

I think labeling is important because it tells - it gives a sense of who you're dealing with. Are you dealing with the registrant or are you dealing with an agent or a proxy for the registrant. That seems consistent whether you're talking to a proxy privacy provider and attorney.

Let me raise a question which has to do with bad actors in foreign countries. I happen to think one of the main reasons we're here is that certain proxy privacy providers in certain countries don't respond. It's what we heard on the Whois review team, I think the Expert Working Group heard it. You know, the fact is around the table, these providers response. It's the ones who don't.

So what's to stop, if we create this loophole, what's to stop the creation of exactly the same situation but through the attorneys of the same countries that currently are not disclosing? Instead of going to a proxy privacy provider, they'll go to their attorneys and who will then have the mafia instead of, you know, the organized crime will them find a different front.

And I'm not sure that the lawyers in those countries have the same bar rules and the same enforcement mechanisms. So what's to stop changing the front door, but the front door still doesn't open, it doesn't answer? And that's really what brought us here. Thanks.

Graeme Bunton: Thank you, Kathy. I've got Stephanie and then Volker in the queue.

Stephanie Perrin: Thanks. Stephanie Perrin for the record. I don't see why -- and this has already been answered by Graeme I think -- but I don't see why in the registration form you can't have a little box saying are you acting for another person or company, you know? That makes it easy.

You'd have to, I think, have a familial carve out so that, you know, a kid can registrar for grandma but without having to be an accredited privacy service provider. But it doesn't seem to me that this is that big a threshold from an implementation side.

In terms of the arguments for exclusion, I still don't get it. I don't understand how we're fundamentally harming the solicitor-client relationship and the right to independent counsel by insisting that if counsel are going to perform a technical service, namely registering domains, that they meet the requirements of ICANN with respect to transparency. I don't get it. Why wouldn't they? Maybe I'm being very stupid, but.

Man: It's up to the registration agreement.

Stephanie Perrin: Yes. Yes, I don't get it.

Graeme Bunton: I've got Volker. And Paul, that's an old hand? That's a new hand. Okay.

Volker Greimann: Volker Greimann speaking his name for the record. They also have to accept the registration agreements for the - when they register a domain name in their own name for a client. So that's something that they also have to put into their agreements with their clients, their obligations arising from the registration agreement. That's one thing, the obligation to, for example, accept the UDRP or something like that.

We've heard a lot of concerns about the loopholes that are being created. Maybe the solution is to see what lawyers would be able to accept and make that the groundwork, the structure that we can accept for everyone. If what's the de minis solution that lawyer would be able to accept when he's provides this service, which is essentially a non-legal service, at least in my eyes.

We've employed law firms for our customers that provide a trustee services and moved away from those law firms because we could provide the same service cheaper. And there was no change in the service or quality of service when we provided than when the lawyers provided it. I just don't get what's so special or - about lawyer, and if the lawyer needs special consideration, then why should that service provided be extended to everyone if I'm offering the exact same service?

Because creating two different categories will create an uneven playing field. Competition for existing providers through lawyers that would be in a very much better position and provide a better service to their clients than privacy service providers would be. So granting an exception to lawyers would be saying to privacy proxy service providers, "Hey you can provide a service but not as well as these other guys who have this loophole."

Graeme Bunton: Thanks, Volker. I've got Paul then Michele and then Steve in the queue. This is good discussion. Thank you.

Paul McGrady: So what the lawyer accepts and if you're willing to accept it, this is great but we're going to have to make some changes in our document. What the lawyer accepts is in the event that he creates a safe haven for criminals and hides their identities so they can engage in criminal conduct, he will lose his license to practice, right? So if the privacy proxy services are prepared to lose their right to do business and if it's bad enough, that lawyer can be disbarred permanently.

So if you are prepared to say that you will forever - you are prepared to forever not engage in your business again forever. And if you're prepared, if it's really bad enough to face criminal prosecution for providing your services as the lawyer will in the event he creates that kind of criminal safe haven, then we're talking about the same thing.

But if we're not talking about the same thing, and we're not talking about the same thing, of course we're not talking about the same thing, and anybody who's ever had a lawyer and wanted to tell that lawyer something in private without being disclosed publicly, knows we're not talking about the same thing, then I'm concerned what we're really talking about is a desire to rein in people who you may believe have done you some harm in the past or whatever.

I'm still not hearing any real harm other than this recent comment about competition in the marketplace. The attorneys at their billable hourly rates as a practical matter, this is an ancillary thing that they do that's usually part of a bigger project or it's part of a pro bono project, those sorts of things. This is - historically lawyers have not been in this marketplace now prior to accreditation in any big way. If they were going to be in this space in a big way, they would be in the space now.

My concern is that in our desire to expand ICANN's reach now into the regulation of attorneys, not only are we dramatically overstepping ICANN's remit but we actually will draw a significant amount of attention to this process by law firms, who will not be happy about ICANN attempting to regulate them.

So again, unless somebody can identify a harm, a serious harm, that would -- I hate to use the word trump; it's such a nasty word right now -- but that would trump a universally recognized global right to counsel, I'm just simply not hearing it. I'm hoping that some consumer advocate who believe that people should have right to counsel might speak up as well. Thank you.

Graeme Bunton: Thanks, Paul. There was something in there, if I can editorialize for a second, that from a registrar perspective and a proxy and privacy service provider, there is increasing responsibilities for us in respect to our customers. The general push lately within ICANN has been that registrars are responsible for their customers. And people want to see increased responsibility there for us. If that be the same responsibility as a lawyer, I'm not a lawyer, I couldn't tell you. I don't think so. But that is certainly a push that seems to be happening.

I've got Michele then Steve, Stephanie and Volker in the queue. We've got about seven minutes left on our schedule for this session. So we're going to be brief and succinct and then we'll probably have to cut that off. And then Steve and I will have a discussion about how we can see if we can wrap this issue up. So that brings us to Michele.

Michele Neylon: Thanks, Graeme. Michele. A couple of things. One hundred percent agree with what Graeme's saying about the responsibility. I mean the - what I find rather entertaining that's unintentional, Paul, is you're actually making an argument in our favor around certain points around this, because the overregulation and the kind of emphasis on making registrars responsible for every single thing that their clients ever could possibly do is something we're facing all the time, and it's not getting any better.

But the reason I raised my hand was in respect to the comments from Stephanie. You've got to remember, and people I think tend to forget this, that in the real world, in the real marketplace out there, a lot of domain names are not sold directly by registrars. They're sold by hosting providers, ISPs, marketing companies, IT service companies, and a whole bunch of other people.

So while you might say that it would be relatively easy to get Blacknight or GoDaddy or Register.com, or someone like that who controls the full flow to add a field or something like that to an order form on a website, which, you know, we may have issues with at one level or another, but, you know, we

control it, when you're looking at business - at other business models such as that of companies that specialize in the wholesale market, it's much, much harder to get that there.

I mean, sure, you can mandate it in a contract but whether that's actually going to transpire in reality or not about, you know, who is you're registering a domain name for and all that, it's much, much harder. I mean to Graeme's point around, say, you know, the who is registering the domain name, like I have absolutely no idea who is registering a domain name.

I mean we go on whatever information we're given. So if I see on our system that a domain name has been registered by Stephanie Perrin, as far as I'm concerned it's registered by Stephanie Perrin. I don't know that you actually registered it for the - your friend who runs the hairdresser's down the street. I've no way of knowing that.

The only time I know about that is when you and the hairdresser have a falling out and the hairdresser comes to us, "Why the hell is - won't you give me my domain name?" And we're like, "Who are you?" So, you know, that's when we become aware of it.

I mean maybe sure if you're dealing with very, very large volumes of registrations you might begin to think that okay obviously that person isn't actually registering those domains just for themselves, but the counter argument to that would be have a look at any large domains that are registering thousands and thousands and thousands of domains. So it's not going to be that easy to identify.

So just a couple of thoughts. It's just because I think this thing where people are assuming that because the contract is with registrars and because registrars are expected to do X, Y, and Z, that automatically that's going to happen simply and easily, it's just not reality.

Graeme Bunton: Thanks, Michele. Steve, Stephanie, Volker.

Steve Metalitz: Yes this is Steve Metalitz. I'm hearing a lot of people talking past each other here. One point of view is that these services - the services lawyers provide are the same as the services proxy and privacy services provide. And sometimes that might be true but there are certainly a lot of things that lawyers do that have nothing to do with what proxy and privacy services do.

And this does get into the human rights aspect of this. And it was raised in sub team four as to whether what we're doing has impacts on the right to counsel. So I think we need to be - I mean if we are going to have a carve out, it probably should be about lawyers and law firms acting in the core business of delivering legal services to their clients because, as Paul pointed out, they may do a lot of other things as ancillary that don't really, you know, that don't really amount to legal representation.

The other thing is, again, let's try to keep our focus on the practicalities here. What we - what has driven this whole process is entities that advertise themselves as privacy and proxy services. They don't advertise themselves as lawyers. They're saying come to us because we'll keep your information out of the publicly accessible Whois. And that's the focus of what we've been trying to do here, what are the ground rule, you know, what the, you know, what are the minimum standards that ought to apply to someone that's offering that service.

It strikes me that really is a lot different than what lawyers do in the full range of representation of their clients. And if we can find a way to articulate that, we should do it. But again, I'm not sure on a practical level that some of the examples we're coming up with here are likely to occur if a law firm, which is not acting and advertising itself and holding itself out as a way to keep your name out of the Whois, but if they put in their name, at least for some period of time, often a short period, a registration is made for a client.

Graeme Bunton: Thanks, Steve. I've got Stephanie and Volker. You guys are going to both be very quick, and then we'll wrap this up.

Stephanie Perrin: I don't - I would suggest that I don't think we're going to wrap it up that quickly, Graeme, with a nice, tight little package. I agree with Steve. We are -- Stephanie Perrin for the record, sorry -- we are talking past each other because I think I understand the full range of services, particularly in the human rights area, that a lawyer operates in or offers for our client. That's not what we're talking about.

What we're talking about is why should a lawyer that is acting -- let's take, I'll pick on Time Warner -- outside counsel for Time Warner, because they don't want to use their internal counsel because they don't want Time Warner anywhere near it, if they use their employee, Time Warner's going to show up sooner, why should they basically gain time in an end process advantage in a reveal procedure by using outside counsel that is not listed and accredited as a privacy proxy service provider.

And I think in response to my friend Paul's here argument that we don't have good data about harm, well we haven't regulated yet. Once we start these accreditation procedures, there's a regulatory impact, and we're not doing a regulatory impact assessment. But there are competitive issues, as Volker pointed out. Any of the ones who don't have to be listed are going to have a competitive advantage.

If a lawyer will have a procedural advantage in delaying reveal. When it comes to actual criminal behavior, our law enforcement colleagues will tell us that a week or two makes a different if you're talking about serious crime. I'm not talking about trademark infringement, although I realize you think that's serious crime too, but I'm talking about people and, you know, harm to individuals.

All of these things, including in response to the business about being disbarred, that may be a threat in the United States and hopefully still in Canada, although I do have my doubts, but it's much less of a threat in many other countries. And we're in a global marketplace so, you know. Some unemployed young lawyer in pick a country where there's a high unemployment rate for lawyers could set up and run all kinds of services.

I just don't think there's been a good argument for the exception, and we will have to narrowly craft the language to make sure that nothing in there interferes with the right to counsel. I don't - that's the part I don't get and where we're talking past each other. I don't see that making lawyers that are offering this service indicate that they're offering a proxy service and abide by the same rules as everybody else. I don't see how that's interfering with the rights of counsel.

Graeme Bunton: Thanks, Stephanie. Before I go to Volker and then Paul, and I think we're going to close the queue and move on, though my expectation is not that we'll have come to a conclusion at that point, I do think we're in place that we've been several times before in this working group in that we don't have concrete text here to look at and respond to and so a lot of this is pretty philosophical.

So maybe what we need to do as an idea is actually take a crack, as Paul suggested, a specific carve out, and if we have language that we can look at and think about, maybe that will help us move forward. So that's a suggestion perhaps for the group.

I've got Volker then Paul, and then we'll wrap this up.

Volker Greimann: Yes Volker Greimann speaking his name for the record. To what Steve just said the privacy proxy provider actually provides a service that essentially just keeps the data from the public Whois, actually in my view that's also providing a service that ensuring a basic human right, at least in Europe it is,

which is the right to privacy, privacy of its own data. The ability to keep it its data private is a human right, at least in European countries.

Therefore we are talking about - what we're talking about here when we create rights to reveal and rights to threats to information or rights to disclosure is already affecting human rights. Of course right to counsel is a human right but the right to privacy is as well. And when we're looking at both, then we need to weigh them accordingly.

What Paul just said was very interesting. You mentioned that this was an auxiliary service, and that's just it. That's - the provision of privacy proxy services is not the essential service of what the lawyer is providing to his customer or his client. It's an auxiliary service that touches upon what he does as a lawyer or that he chooses to provide a complete package to his client.

There's no reason why a lawyer cannot go to an accredited privacy proxy service provider to provider that service. Is it just cost savings that makes a lawyer want to do it himself or anything else, I don't know, but as it's just an auxiliary service that doesn't really touch upon his client confidentiality rights, I don't know. Is there a specific reason why he cannot go through a third party for that?

Graeme Bunton: Thanks, Volker. Paul?

Paul McGrady: Thanks. Paul McGrady for the record. Graeme, I appreciate your suggestion that we try to reduce this to writing so that we can haggle over specific language rather than this in theory. I would very much like to be a part of that, as you can imagine.

In the event we ultimately can't reach a conclusion on that language, I guess we should postpone talking about what we do then. But I would like to say for the record, as far as I've seen, 100% of the public comment has been against

the idea of interfering with the attorney-client relationship and having ICANN attempt to regulate the legal profession. And I think that in the event we can't reach an agreement on that and we send this to the GNSO with a note saying that, you know, we didn't reach an agreement, I'd like for the record to reflect that the public comment was against getting involved in this business.

If there are public comments that I missed where people said this was a great idea, we should, you know, we should make lawyers essentially to the same status as privacy proxy services, then I'll retract the statement. And I hope you guys will send me links so that I can see what those other public comments were.

And I also think by way of disclosure, if we are going to come to that conclusion, it might be helpful to give advanced notice to whoever within ICANN is in charge of thorny problems that will be thrown into their lap, because this will be a thorny problem thrown into their lap. Thank you.

Graeme Bunton: Okay thanks, Paul. And thanks everybody for that discussion. I think what we perhaps will take, and we'll take this offline, is maybe look into having a couple people take a crack at that language and then we'll have something concrete to discuss. And it could be we reject it outright, it could be we figure out a compromise there and we're able to move forward, but I think that might be the best way I can come up with immediately to move this discussion forward.

I think that brings the end of that piece of work. There's still a couple issues left on that sheet. We'll try and circle back to those later this afternoon, but we did get through some stuff there and we had some good discussion. So thank you everybody.

I'm going to hand over Steve now, who's going to pick up the mantle.

Steve Metalitz: Thank you, Graeme. This is Steve Metalitz. So our next item is the summary of recommendations from sub team four. And I just want to thank the participants in sub team four who had one of the toughest jobs of going through all these public comments that didn't fit into the categories we had already come up with and didn't necessarily relate to a specific recommendation of our preliminary report, so it was a bit of unchartered territory.

And the document that you have in front of you was, I believe, the staff's effort to, based on the discussion, you know, the preliminary report that sub team four had brought out, which was also sent out in your materials, to try to boil this down into some of the areas the sub team felt that might need discussion based on the public comments that they had reviewed.

So I guess I'd just like to walk through these briskly, if we can. I'm sure some of them are going to be maybe in thorny department but others perhaps not as much so. The first one that you see up there -- and let's start on the first one and of course then we can take a queue of any comments on this -- about law enforcement agencies. And there's no specific recommendation here, but if the working group decides to take up the issue, then we have to look further into these comments.

It strikes me this is the overall question of, you know, what have we said in our report about law enforcement. We've got a definition, basically copying the definition that's in the RAA, and now we've linked to that if ever changes. And we have a few other mentions of law enforcement but we don't have a disclosure framework for law enforcement. And I think frankly it's - we're not going to come up with one on the timeframe that we're talking about, you know, that is within all of our collective lifetimes.

No, I mean if we're going to bring this across the finish line, we're not going to have that. And there's a variety of reasons, and I'll just be very candid about it. I think we've had a - too low a level of participation from law enforcement

groups to really delve into this. So I'm not sure that we can take the law enforcement issues any farther at this point, and it may be that we don't make any change to our recommendations as they stand now dealing with law enforcement.

So I'll - let me just throw that out and I'll ask either the sub team co-conveners, who are both here, or other members of the sub team that have any comments on that. Kathy?

Kathy Kleiman: Kathy Kleiman. Here really I think -- and maybe it's already in the final report, the draft final report -- but the idea that Annex E, which I think has become Annex B, which is how we deal with intellectual property requests is not probably how we're going to deal with law enforcement requests. And I think that's really - at least that's my sense of what this category A is is that we received a lot of comments that says this is apples and oranges, don't treat them the same way.

And so whoever - so that there shouldn't be a sense that the IPR is the template of which we overlay every other type of request, whether it's private security or whether it's law enforcement. And so I think that's what I take away from here, as well as a lot of different comments that will provide insight to whoever has to deal with an LEA template request, if that comes up in implementation, which I hope it doesn't.

Steve Metalitz: Thank you. I don't know if, Paul, if you had anything you wanted to add there. And I see two other hands in the queue. So.

Paul McGrady: Paul McGrady. Just a note of humor. I've already hubristically -- is that a word? -- hubristically, with hubris, spoken for the entire global legal profession today even though they did not send me here, so I won't attempt to speak for law enforcement.

Steve Metalitz: Thank you. Michele and Volker had their hands up. Was that on this topic?

Michele Neylon: Oh sorry, that's old.

Steve Metalitz: It's old, old?

Michele Neylon: Sorry.

Steve Metalitz: So does anybody else have any comments on this law enforcement topic?

Graeme Bunton: I see David Cake.

Steve Metalitz: I'm sorry. David, go ahead.

David Cake: Actually just slightly disagree with Kathy. I think one of the interesting - we actually - it's too late perhaps to really dive into this, but in terms of how we deal with IPR, there is significant issues where there's a gray area where that is law enforcement and where it isn't.

Some of the questions here may be really - a lot of the questions about commercial, you know, regulation of commercial use and so on really come down to the broad definition of law enforcement and trying to draw - I think in general we'd be better taking - saying IP requests where the issue becomes difficult, we can pump that towards it being an LEA request rather than trying to cover every possible IP thing within the definition of that.

And the example I'm really talking about it is a lot of these requests about - there are a lot of the arguments we had about commercial use and so on really come into my mind, come down to the fact that the, you know, national, you know, commerce agencies and so on are in fact law enforcement in a limited way.

And, you know, if you really want to get a - if you really find that you can't a request that you like doesn't fit into the rules we come up with for dealing with

IP requests, then by all means punt it to your local national level agency and get them to try and do it as LEA rather than try and make our IPR request so strong they will catch every possible circumstance. Does that make sense to anybody or am I just jabbering here?

Sorry, Kathy's looking very confused at me.

Steve Metalitz: We will be getting to Annex E, which I - you're right is now Annex B, and I don't quite understand that. But we're so used to calling it Annex E, we'll be getting to that later in the afternoon to talk about whether we've got that nailed down.

So anything else on the law enforcement issue? Kathy?

Kathy Kleiman: Again, just the request that it be codified. Thanks.

Steve Metalitz: Yes. And I think that - I think we've got - we captured that that we should make it clear that the illustrative framework is one area and it isn't supposed to necessarily say how other types of disclosure requests, including law enforcement, ought to be addressed. Was that basically your point?

Kathy Kleiman: And that there are a lot of comments that should be reviewed if implementation looks at them.

Steve Metalitz: Okay. Thank you. Okay. Then let's move onto category B, which has to do basically with what - some recommendations about what happens after this policy is approved and goes into effect. One is a mandatory post-implementation review on a periodic basis. The recommendation here is two years. Every two years, starting after the launch after the program, and every two years thereafter. And then there's also a point about an education program on this.

So I think everyone would agree with the concept that we should build in a post-implementation review. I'm not sure that people have different views on exactly when that should be or whether that should be left the implementation review team to decide or what the perimeters should be. But I think that's what these recommendations coming out of sub team B address.

So again I'll ask if either -- excuse me, sub team four -- I'll ask if either the co-conveners want to add some color here or if others have comments that they wish to make on this subject.

Paul McGrady: Paul McGrady for the record. The reason why we put in the timeframes we did was because everybody is concerned that if something, some unintended consequence, regardless of who it affects, right, the end users, the providers, complaining parties, whomever, that the earlier that's identified and robustly looked after, the better off everybody will be.

And so that's why we didn't just put in there saying we think we should have an early review and it should be robust. Instead we tried to do a timeframe so that we were able to convey the urgency of a need for an early look into this to make sure that what we all did around the table here actually turned out the way we hoped. Thanks.

Kathy Kleiman: Exactly. Agree with Paul completely. This is Kathy Kleiman. Could whoever's holding the document page down to category D, number three? Because I just wanted to read that as well. It actually embodies exactly what Paul was saying in connection -- I'll read off mine -- in connection with the post-implementation period review mechanism suggested above that we're talking about, the metric should enable rapid evaluation of the question whether such unintended consequences arise in a systematic manner and of possible ways of fixing them.

So we don't want to wait 10 years or 15 years for the review of this policy, we want it to be quick, early and, you know, if we do find that there's abuses

going on, if we do find that somehow there's harvesting going on, let's stop it, let's nip it in the bud. Thanks. So I just wanted to show that A and D connect.

Steve Metalitz: Thank you, Kathy, for pointing that out. So is there any other comment on this post-implementation review question? If not, I'd like to look at the second point about education program. And now all we have there is "to be decided by the working group." So maybe the sub team members could let us know, you know, a little more what is the issue here.

I mean, again, I don't think as an implementation matter that anyone would object to educating customers, requesters, and the public, but please let us know what you have in mind here.

Kathy Kleiman: Terrific. Kathy Kleiman again. What we had in mind here, and there was discussion in the working group on this, was, you know, do people understand what's hitting them, what's about to happen. Is it - with the URS for example we educated trademark owners but we didn't educate registrants. ICANN didn't educate registrants.

In this case it's very important that customers, requesters, and providers, know what the obligations are, you know, has implementation translated into posted policies, FAQs that are clear, do people understand what's happening. And there are ways to test it and there are ways to put things out there and ask people if it's clear, if they understand, if the new policies that the PPSAI recommends and that are ultimately, may ultimately be adopted are accessible to everyone.

You know, is it published in different languages. Basis things like that. So that's really what this recommendation is about. And we certainly heard a lot of concerns expressed in comments, so can we just address it and make sure it's clear.

Steve Metalitz: Paul, anything to add on that. Okay. Stephanie? And anybody else want to be in the queue on this? Michele. Stephanie, Michele.

Stephanie Perrin: Stephanie Perrin for the record. I'd just like to point out in addition to what Kathy said that we're not really doing an adequate job as ICANN of educating end users as to how the whole system works right now. One of the downsides of being recognized as a privacy person and having your friends discover that you're in at ICANN is you get, "Oh good, I've got a complaint." This is coming from, I forget, somewhere in Europe, from this guy. "I'll send it to you."

And you have to respond to these poor devils who are intelligent Internet users, who didn't realize that there were harvesters out there that once their address and cell phone went out in Whois, they will never get it back unless they want to pay these dudes 15 bucks a year to get it out of Whowas or whatever they call it.

These are basic facts that the average end user doesn't know. So I would just like to put a plea in that if we're going to educate about this new accreditation process, we let people understand why they should always think of using a privacy proxy service when they register, because once it's out there, they won't get it. Fine if you don't mind changing your cell phone and your address every other year. Thanks.

Steve Metalitz: Okay so a marketing plan for the privacy and proxy service providers. But I'm not sure that's an ICANN role. Michele and Vicky, and who else is in the queue?

Michele Neylon: Thanks. Michele. Somebody still has a mic on somewhere I think. Okay this thing around education, I'm very much in favor it but I think we have a much - when it comes to education, we have a fundamental problem in that 99% of the world doesn't have a clue what the hell ICANN does, doesn't understand

the quote, unquote DNS, doesn't know what the hell a domain name is, doesn't understand any of this.

So while I have no issue with a recommendation around education on this particular work group, don't get me wrong, but I would prefer that we - that if anybody's going to do anything about education that we could actually get ICANN to focus on education at a higher level, better use of plain language, be that English or other languages.

I am sick to my teeth -- and I have said this on multiple occasions at the SO-AC meetings on Friday afternoons --that I'm sick to my teethe of seeing public comment periods opening where even for those of us who are relatively engaged with all the things, we have no clue what the hell it's about, we don't know why anybody would interested, we don't know who is going to be impacted, because nobody takes the time to go, "Okay this PDP, this bit of work stream is of interest to the following user groups and this is why you should give a crap about it."

And that's the thing. I mean the - I'm Irish, as you all know. Yay! Woo! No, no, but hold on, hold on. This - okay, so ICANN 54 is here in Dublin, which something we're very happy about, very proud. The problem is how many Irish tech companies, how many people involved in various parts of the Internet industry are going to bother to get off their asses and make their way here this week?

And the answer I've got so far is depressing. And the reason that so few people are going to both is because nobody understands what the hell's going on. And it's like trying - this is a fundamental communication issue. And until ICANN, from the CEO down, get that through their thick skulls that people don't actually understand what the hell is going on here, we're going to have this problem continually.

And I know it's not specific to this thing but it's just - it's really, really frustrating, because as other's have said, you know, around the Whois in particular, people register a domain name and next thing their winging and whining, like, "What the hell are my contact details doing out there?" Blah, blah, blah, all that kind of thing.

We've had the situation where people have posted a comment on a blog and they're going, "How on Earth are my contact details there?" Well it's like their contact details actually aren't, it's just their name, but it's like it's a public blog. You actually, you know. So people don't understand these things.

So yes, it's just at a high level it's a bigger thing. I mean I think it would help everybody if there was a better understanding of some of this stuff because I'm getting buy in, it would save time, because we all see the public safety people who don't have a clue how the Internet works and then are asked - coming to us, asking to fix things that are completely outside our remit.

Steve Metalitz: Michele, I think you've made your point, one I think everyone around this table probably agrees with heartily. Vicky, go ahead?

Victoria Sheckler: Thank you. I was going to say that for once I actually do agree with Michele on one thing.

Michele Neylon: For the record.

Victoria Sheckler: For once, once.

Michele Neylon: It won't happen ever again.

Victoria Sheckler: And when I try to talk to any of the labels and the artist about ICANN and why they care, it's tough, as an aside.

For this issue in particular, I think the concern that we had -- or that I had -- within the working group was how do you do the education and there was a lot of concerns about measuring it. And as Michele just mentioned, there's a lot of education that has to happen. And so while I think that an education goal here is laudable and that it's something that ICANN should take on, to the extent we're talking about measuring that education, we've got to give it time. Because we're starting from a very low base. Thank you.

Steve Metalitz: Thank you. I think, yes, I think all these comments underscore we have to have realistic expectations about what could be accomplished in the education area. But - and I think it's - I hope that the staff is hearing all this and is making, you know, taking notes, that this is a broader problem than just in this area.

Michele Neylon: (Unintelligible) agree with me.

Steve Metalitz: Yes, that is noted for the record. David and then we'll -- two Davids -- and then we'll wrap this point up.

David Cake: Yes, David Cake. Sincerely, in terms of public education and knowing about the work of this group, if the general - if registrants were made aware of the existence of proxy and privacy services at time of registration, that would be a grand achievement and all I would realistically expect we could actually get done.

The people that want to know the nitty gritty have ways of finding out. But we are so far behind that people don't even know, often do not even know that proxy and privacy services exist at times of registration. And if they knew that, we would be well ahead of where we are now.

David Hughes: This is David Hughes. A point of humor, I hope. So going back to Michele. So people ask about ICANN, and I said, you know, "ICANN needs a slogan." I was talking to somebody. I said like, "They need a slogan like 'We are the

Internet.'" But then immediately - yes I know. So immediately it came back and they said, "Well actually we'd have to change the language a little bit." They came up with, "We are a highly technical operational activity underlying the core functionality of the DNS..." Yes that doesn't fly. That doesn't help anybody.

Steve Metalitz: Thank you. We've touched on some much bigger marketing issues here in several contexts.

I'd like to move on. I think there's general agreement that this implementation has to have an education component. That's very important. Let's move onto category C, which I think is going to be a little more thorny perhaps, new or additional features.

The first one has to do with accepting and investigating notices of breach of accreditation standards, leading to improper disclosures of publication or improper refusal disclose.

So again, I'll invite the - if the sub team members have any color to add here, because I think this sounds like kind of a core implementation issue that if you have these standards and if people don't follow them, and I think you're certainly drawing attention to the fact that it's not so much a question of some technical violation of the standards but something that leads to disclosure when there shouldn't be - or it leads it to refusal to disclose when there should be, that there needs to be a compliance response to that of some kind.

Is that - does that catch the gist of this or is there something else underlying this that you wanted to convey? Okay. So I think we're set on that as an implementation issue but a very important one.

The next one is consider monetary damages or other penalties for repetitive abuses of the disclosure process. And there are a couple of brackets in there.

So I take it that to mean that there was some disagreement within the group about that or there's some thorniness so, so let's talk about that. Do you want to start, Kathy or Paul?

Kathy Kleiman: Sure. Kathy Kleiman and then pass it to Paul, and Vicky may want to add as well.
So the question is what happens, particularly when there's violation of the very strict restrictions on the reveal the data that we talked about. So a third party requests something and then they've agreed to limited use and they go ahead and publish it.

The reason you see brackets around repetitive abuse of the disclosure process is because obviously systemic repetitive abuse is something we agree is a problem and I think there's actually consensus on that, or well I'll leave it to my colleague, that there should be some kind of penalty for repetitive abuse. But a single abuse can lead to lives being lost. We've talked about that here. Battered women shelters having to be relocated, women who are stalked having to move. Single abuse, potential to be a real, real problem.

So the question is what kind of damages. How do we put teeth into the restriction that we've put there, and if we don't put teeth in, is anybody going to follow it. If there's no enforcement mechanism, who's going to really care about ICANN not enforcing anything. So that's what number two is about to me. I'll turn it over to Paul.

Paul McGrady: So my concern about number two is just that I have no idea how this can be done, right? There's not really a contractual relationship between ICANN and the requesters if the requester is abusing the process. I don't know how it would work if ICANN mandated providers to collect monetary - I just don't know how to functions. And I mean I think that's all I had to say.

Steve Metalitz: Vicky. And does anybody else want to - Volker next. Vicky, Volker.

Victoria Sheckler: Along with what Paul was saying that if the idea that there's going to be penalties against the requester, it's not clear how ICANN in its accreditation process can do something meaningful there. I imagine that privacy proxy services very well may tell a requester that they're no longer allowed to send any kind of request if something like that happens. I know that in other contexts, service providers have cut off the ability of an abusive sender request, or whatever you want to call that person.

So if you look at it from that perspective, it's not clear how an ICANN accreditation process can implement this. If you look at it that this is against the privacy proxy service for continually giving out information when it shouldn't have, I mean that's - that is something different.

But if you're thinking about it from that perspective, that's why repetitive matters, in my view, because if there's a one off, that doesn't make a whole lot of sense, but if this is a systematic thing or repetitive thing, is it accreditation, is there more teeth to it for that privacy proxy service. So I think it depends on how we think about it.

Steve Metalitz: Okay. I have Volker in the queue and then Holly, and then I'll put myself in the queue.

Graeme Bunton: Michele I think (unintelligible).

Steve Metalitz: I'm sorry. I'll put you ahead of me, Michele. Volker, you're next.

Volker Greimann: You can speak as much as you like because you're at home here, Michele. Volker Greimann speaking his name for the record. Just maybe we could take some learnings from the UDRP, where the complainant also binds themselves to certain terms by submitting the complaint, as in he agrees that he will be able to be sued in the local jurisdiction of, A, the domain holder, B, the registrar that manages the domain name, and there are certain terms that a complainant agrees to when he submits a UDRP.

It could be the same that the registrar or a privacy service provider has certain terms that the complainant has to agree to. It should be reasonable, should be even be managed by ICANN, a brief draft document that says if you submit a complaint under this policy that may lead to a reveal, then you agree to certain terms that may require you to pay certain damages to the provider if you violated the terms of this agreement or acted in contrast to the policy. It might be a suggestion that we might look at.

Steve Metalitz: Holly, go ahead.

Holly Raiche: I think Vicky's got a better conceptual framework, which is this is really about a breach of accreditation. You said you will do X, you haven't done X. But I would argue that even one breach should be taken seriously, because the reason we're accrediting a privacy proxy service is to recognize people's desire for privacy. So in that case, one breach can be as damaging or more damaging than many.

So - but if we base it on the contractual relationship between ICANN and accredited provider, we've actually got a much better mechanism for enforcement. And then we can say any breach is serious and then think about it that way. I think that may be a better way to go about it. Thanks.

Steve Metalitz: Thank you. Michele, I think you were next.

Michele Neylon: Thanks. I feel so unloved here. Michele for the record. Now just this is again one of those things where I find myself oddly aligned more with the lawyers in the room. The reasonable contractual arrangement here that's going to cover these kind of damages, so I think the concern which I would have is making sure that if we as a proxy privacy provider say right well (Report Rex) is a scumbag and is just wasting our time and is abusing it and whatever, they were able to shut them down and we don't have a situation where (Report

Rex) goes winges and whines to ICANN and gets - and we end up with a compliance issue.

We're able to cut them of and that they're not able to use some kind of runaround to ICANN compliance. So there'd be a clear process for that and not something that's invented like two years later and costs me thousands of euro in legal fees. That would be a very clear reference to the data retention thing, which cost me a bloody fortune.

But it just needs to be something so that we can say okay, company X, requester X, whatever you want to say, we're able to - we are cutting them off for whatever reason, but they can't go to ICANN and get past that, that we're able to say categorically they have abused that. That to me is something that would concern me. Trying to get damages and everything else, I can't see that working because as others have pointed out, there's no - ICANN is not - it doesn't have a contractual relationship with them.

ICANN is not global police. ICANN cannot start collecting money from random third parties. I don't see how that would work. I really don't. I mean it's a nice idea, don't get me wrong, and obviously would work in my favor, I'm just thinking of it terms of it being something that could actually work. But the compliance thing is something I would be very concerned about.

Steve Metalitz: Okay. I will pass on my spot in the queue. I think we had Todd and Kathy, or Kathy and Todd.

Kathy Kleiman: Great. Kathy Kleiman. I think Vicky did a really good thing by bifurcating this. So we're looking at repetitive abuses perhaps for providers but also a cause of action for individuals, organizations, and companies if their information gets out and their docs are swatted based on that.

And that's where the monetary penalties come in is if you go to court and so that ability to create that cause of action, as Volker outlined, so that

customers can take their requester to court. You know, work would have to be done under national law, but the idea that ICANN wouldn't preclude that.

But basically I think we're diving in too deep. Sub team four is kind of presenting you with this out of the blue, and I'd like to recommend that, while I don't want to continue meeting for the next year, that we add this -- there seem to be a lot of good ideas around the table -- that we add this to one of the issues that we work through in one or two meetings on a Tuesday, because it's really a final piece, which is teeth, enforcement, making sure that what we set out to protect people works. Thanks.

Steve Metalitz: Okay thank you. Todd and then Stephanie.

Todd Williams: Todd Williams for the transcript. So I'm going to agree 100% with Michele that what we are doing is drafting accreditation standards for privacy proxy providers. And so when we think about what is our hook to give these teeth, is going to come from that accreditation and it could be well you, privacy proxy provider, will not have you accreditation at risk to compliance if you are ignoring requests from somebody with a history of abuse.

And in fact what I wanted to point out is that that is already enumerated explicitly in Annex E -- and I know we're going to talk about that this afternoon -- but, you know, because it came up here, I mean I can cite it. It's 1b...

Kathy Kleiman: You probably wrote it.

Todd Williams: Four, I think, 1b5, I'm sorry. But basically it says nothing in this prevents providers from implementing measures to manage access to the request submission process, which is what you were outlining. And then it goes on and explicitly says revoking or blocking requesters access to the tool for abuse of the tool or system, including submission of frivolous, vexatious, or harassing requests. So I think that's what you were asking for, and I'm saying we've already done that.

Michele Neylon: Fair enough.

Steve Metalitz: So yes in that area we - I think it has been addressed. Stephanie. And then we'll wrap up on this topic.

Stephanie Perrin: Yes, Stephanie Perrin for the record. I just wanted to point out that in many jurisdictions that have data protection law, an unlawful disclosure would be considered a data breach and there are many remedies that you can do. As part of an education package, you might want to make the user aware of who they could complain to.

So, you know, you have a right to complain to ICANN, not that ICANN's going to do anything about it, you have a right to complain to any relevant data commissioner, you have a right to take a data breach to court. So just - most people wouldn't know that, certainly most registrants, and they wouldn't necessarily know that this was an unlawful data breach. Thanks.

Steve Metalitz: Okay thank you. So, yes, we've had some good discussion of this and I think this goes back to - it was in Mary's comment when she circulated this, which is, you know, in a contractual setting how could that actually be carried out. So. And we have a suggestion that we ought to return to this later. So Graeme and I will, as we go through the output of this meeting, we'll kind of figure out how we can take our next step on this.

Let's move onto C3 about a limited retention period in accordance with applicable laws. It says it's already included or at least addressed in Annex E, which we will get to. But - so I guess the suggestion here is that it should be a more global requirement that whenever there's disclosure it should be retained in accordance with applicable laws, which I think since if those laws are applicable then presumably if someone violates them, there's some remedy of some kind, which would not be provided by ICANN, it would be

provided by the national legal system. But I think that's what - so if I understand what this is driving at.

Let me ask first if there are sub team participants who would like to add any color on this. Kathy, anybody else, Vicky, and then we'll go to Michele.

Kathy Kleiman: Yes, just very briefly -- Kathy Kleiman again -- just very briefly, this is one of the situations where we were taking something out of Annex E, Annex B, and universalizing it to all other types of requests. So here in language that Todd wrote, reading in Annex E, "Requester will comply with all applicable data protection laws while retaining customer's contact details and will use customer's contact details only for" and it lists that. So we've got the language now in Annex whatever. This is an idea of universalizing it. Thanks.

Victoria Sheckler: Kathy is right. It's the idea of expanding what was in Annex E to other areas. I don't think that language is quite what was in Annex E, and I couldn't find my Annex E here quickly, because I don't think it was that direct - sorry, I can't see anything without my glasses.

Steve Metalitz: We'll get to Annex E, but the basic point is that type of approach that is reflected in Annex E, which we will talk about this afternoon, should be applied more broadly or applied more generally.

Victoria Sheckler: Exactly.

Steve Metalitz: Okay. All right. So any other comment - oh Michele, thank you. And let me see anybody else wants to be in the queue.

Michele Neylon: This is Michele even though Steve is trying his best to ignore me. I feel so hurt. No, jokes aside, I mean this thing around the applicable laws and everything else, I mean again while I like it, I can this causing issues for requesters. Because now as of now any of you American law firms who want to send me review requests, I'm going to say to you, "Okay fine I will reveal to

your European office. If you don't have European office, you can shove it where the sun don't shine." There's no safe harbor anymore. I cannot send that data from Ireland to the U.S. I can't do it.

Steve Metalitz: I'm not going to comment on your legal advice there, so the legal advice you might be receiving. But I hear you.

Woman: (Unintelligible)

Steve Metalitz: No I understand. I'm familiar with the decision, Holly. It's also struck me that it actually has almost nothing to do with anything we've been talking about, because no one is relying on the safe harbor in order to access this information. There's plenty of other basis for it.

So let me just ask if there's anything else on C3. I think we have a general agreement that this precept should be applied generally and obviously we have to figure out exact language for that. C4 is on statistics and collecting the number of publications and disclosure requests.

I think this also I assume is not particularly controversial but I suppose there could be implementation issues in how this is done. You know, again if it's an accreditation requirement, you know, would there have to be some type of annual report that each accredited provider would provide or what. So let me ask Kathy or Paul or others on the sub team to comment.

Kathy Kleiman: Me again. Note the wording "provide the statistics in aggregate form to ICANN for periodic publication." There was some concern with individual providers having to list their information individually. I don't know how we get to aggregate, but in general some people want to know the number of publication disclosure requests -- we got comments on this -- those received, those honored.

And in Paul's wonderful wording, he said, "The data should be aggregated" -- I think it was -- "as we do not wish to create a market where nefarious users of the DNS fine proxy privacy service, the service least likely to make disclosures." So the aggregate service providers, I think it serves everybody, kind of this anonymous aggregation.

Steve Metalitz: Okay. Graeme is in the queue. Does anybody else want to speak? Okay.

Graeme Bunton: Darcy.

Steve Metalitz: Darcy. Graeme, go ahead.

Graeme Bunton: Thank you. This is Graeme for the transcript. This causes me some anxiety and maybe it's because I'm a little bit close to it on a practical level. I'm also in the Data Metrics and Policymaking Working Group.

In that, we specified that you cannot compel a contracted party to provide data, and there's a lot of reasons for that. Also, you know, that sentence "Provide the statistics in aggregate form to ICANN," well who's doing that? We don't trust ICANN, contracted parties, do that. ICANN has had repeated breaches of their systems. So it's certainly not ICANN that we would give our unaggregated data to.

There's also competition law and all sorts of reasons why that sort of thing is extremely problematic. We'd have to have a third party that is trusted by contracted parties in order to do that aggregation. And even then, you end up with curious issues where you have different sized registrars that collect data in different ways.

And this sort of request requires ahead of time that all privacy and proxy service providers are capturing these statistics in a very similar way. I think it becomes pretty difficult.

Conceptually I think it's interesting and probably good to do. The particular implementation and how do we get providers to do this en masse in way that's useful, I have to think about a bit more, because it's not going to be easy or straightforward.

Steve Metalitz: Graeme, thank you for that slightly depressing litany of practical issues that may arise here. Darcy, go ahead.

Darcy Southwell: Darcy Southwell for the record. So Graeme touched on a lot of the things that I wanted to say too, but it's - I like this language a lot better than the last version. I'm much more comfortable with this, but I'm very concerned about the aggregation.

And it's going to, for our registrars and many others that have multiple registrars and multiple platforms, it's going to be very difficult to track. Because even internally we don't track it the same, let alone how maybe Tucows tracks versus how I track. So it can be very difficult for anyone to aggregate any of this information consistently to give us any flavor for what we're talking about.

Steve Metalitz: Okay. Further caveats here. Holly, go ahead.

Holly Raiche: It's really a question. If we're going to have an early review, which I think we've all agreed we need, we're going to have to have some data. But I think we're going to have to here from the registrars as to the ease of collecting the data and the various ways it's collected so that we can come up with some words that actually don't completely defeat the purpose.

Graeme Bunton: Graeme for the transcript. You know, varying sizes of registrars collect data on this sort of thing in very different ways. You know, some registrars are literally -- and I've had meetings with a kid in his parents' house in his bedroom where he runs his hosting company that's a reseller of ours -- and so their statistics for this, you know, like maybe they're accredited, are literally

just an e-mail address. They don't have an actual ticketing system that you can tag and filter and number.

And, you know, that's going to be an awful lot of people. And then compelling them, this one-person shop, to take time out of their day to provide statistics is a problematic request.

I had another point on this, which is escaping me at this exact moment, and if I remember it I'll come back to it.

Steve Metalitz: Thank you, Graeme. I think we'll wrap up the queue on this point. But I think Holly made a very important comparison here, which is we glibly said 15 minutes ago, "Oh yes, definitely there should be a two-year review here" but it doesn't sound as though it's going to be quite as easy to get some of the data that we need for this two-year review. So we either have to figure out how to do that or figure out whether that two-year review is really what we're looking for.

Stephanie, very briefly, and then we need to move on.

Stephanie Perrin: Stephanie Perrin. I think if the public relations education campaign is successful, you can at least get stats on complaints, because people will know enough to complain. I think that might be a very attainable goal. You'll know if you don't get any complaints that it can't be running too badly. But the idea of getting comprehensive stats, I think that's a heck of a leap.

Graeme Bunton: I remember what I was going to say. Very briefly, and I see Paul's hand up. He's got something very brief. I was just saying this point is coming very close to sort of mandating transparency reporting from privacy and proxy providers, and I'm not sure we can do that.

Steve Metalitz: Okay. Paul, Michele, and then we will move on.

Paul McGrady: I think we may be over thinking this a little bit. All this is saying is that we keep track of the number of requests and the number of disclosures, and that can be done on a chalkboard. Got a request, disclosed it. Got a request, if you didn't disclosure, then you don't put a mark on the other side.

What - we're not talking about providing all the information related to that request, because then we would have a super scary entity that had all the super scary information that we're trying to keep from being disclosed in the first place, right? And so we're talking about a very simple dataset. Got a complaint, disclosed. Got a complaint, didn't disclose.

And I - from my point of view, there reason why this is important is because if after one of these cycles, we collect that data and we see that 98% of the time where there was a request, there was a disclosure, and that means at least from the privacy proxy services point of view, those were healthy requests. If we see that 70% of the time there was a request, there was a disclosure, then that means there's an illness in the system, right? Because we shouldn't be getting 30% bad requests, right?

And so that's what I'm - you see, that's why that stat matters, because if the privacy proxy service gets requests, and 30% of them are junk and should not have been made in the first place, then that's a problem we need to address. That goes back to request for abuse, I suppose.

If 95% of the time, or 98% of the time, the provider says, "Yes that's a bad actor, I should turn over that information in accordance with scheme," then that says that the requests coming in are healthy, I suppose. That's one way to interpret the data. But what we don't need is a bunch of other data, we just need to know how many we got and how many we acted on.

Steve Metalitz: Okay, Michele and then we'll move on.

Michele Neylon: Yes thanks. Michele. Okay, agreeing with Graeme. I mean there is - I think what we need to be careful of is -- how can I put this? -- I think this is a little bit too specific in what it's requesting, because as Graeme pointed out, I mean a lot, you know, registrars and other providers vary a lot.

I mean it might, to you Paul, seem very, very simple to go yes, no, I'll keep track of it, I know - look, speaking from personal experience of growing a company from 1.5 people to now over 40 and how much it cost me in various other thing because of record keeping and everything else, I mean when you are literally juggling 10 jobs as one person, doing something extra like that is very, very hard and it's very easy for it to slip through.

Now if you're looking at it in terms of, you know, we need to have some level of statistics, something beyond anecdote or whatever in order to be able to conduct a review, I totally agree. Because I think any policy, it doesn't matter what it is, it needs to be reviewed on a fairly regular basis in order to make sure that the policies reflect reality, that it does what it's mean - what it was set out to do, and that it isn't either too broad, too narrow, or whatever, that it's kept up to date. Because, you know, out of date policies cause us all headaches at all sides.

I just think we need to be careful in getting too specific around the statistics here, just because, you know, if you're saying specifically the number of requests or something like that, that's suggesting you're getting very, very granular, which I know will be fantastic and might be feasible for a larger provider, but for a smaller provider, that could be a problem. I mean it could become a major problem. As I say, they're juggling a million and one things.

Steve Metalitz: Okay I'm going to cut this off here and we're going to go on to the next section, which fortunately the next - fortunately for everyone who wants to have lunch, which we will have in about nine minutes. But if you would scroll on there, Mary, we've actually dealt with number five. Michele gave a very elegant presentation on this about an hour ago.

D1 is the same question that we just had about another aspect of Annex E, about retention period. This is another question of whether something that's in Annex E should be provided more generally. I'm going to defer that to the Annex E discussion. So let's flag that when we talk about that, as well as, you know, about the retention, whether those should be made more general.

D2 is the right to counsel. I think we've had that discussion. I don't think we've reached a resolution but I think we've had that discussion. D3, we've also discussed, and Kathy thanks for calling our attention to this when we talked about the - this great two-year review that we're going to do, only I'm not sure we'll have any data for it. But we're on record as we want that two-year review.

E1, this is the sub team had to look at a lot of comments that came in that said there should be no accreditation system. ICANN should set no rules in this area and their - I'll ask them to kind of walk through what they concluded here, but I think it - they did attempt to take into account all of these comments that were in a sense out of scope for our work here, but which were reflected some very strongly held views in some parts of the community.

So Paul or Kathy or Vicky. I'll ask Vicky because she had her hand up, but Paul or Kathy feel free to add.

Victoria Sheckler: I just wanted to give kudos to Stephanie because she came up with the idea of thinking about these comments in connection with the two-year review and that that might be a good time to think if it's successful or not.

Steve Metalitz: Okay. We're loading something else on the two-year review here, but I hear you. I think that's right, and that is the second sentence here, I think, or the first two sentences. So Kathy or Paul, anything to add here?

Kathy Kleiman: Kathy. Just a note that in the final report we should acknowledge that we received these comments and that, again, that we're bumping it to a later time for evaluation, given that our mandate is to create the accreditation system.

Steve Metalitz: Yes thank you. Or recommend. Okay. Unless there's other comments on E, let's move on to F, in which the type - the color of the font seems to have changed, but I'm not sure that that is a significant point here.

The working group should also consider which law (unintelligible) should apply to the request, and there are several options given. This strikes me as a kind of a huge, slightly submerged issue but one that, you know, like use things that slightly submerged could become quite a hazard to navigation. So maybe I would ask the sub team members if they can provide a little more background on what they are thinking the working group should do in this area.

We'll start - well let's start with Holly, then Vicky, then Paul. Did you want to be recognized? No. Okay. Holly and Vicky. Holly, go ahead.

Holly Raiche: I guess, speaking as a lawyer, I'm asking what law, and I think up there either you say applicable law, which means the national law, or you start to say regulation or something else, but I read that and found it a little bit puzzling.

Victoria Sheckler: I thought where we had left this is slightly different than what's written here, so I apologize for that. I thought it was that we should consider whether to suggest a choice of law or not. And I think Mary reminded me that we may have had this discussion already in this group and come to at least -- or there was some discussion -- that it may not be possible to specify a law through this type of accreditation because of the national laws that apply.

Holly Raiche: Well either it's an applicable law because there's no universal law on the issue, so you can't say law. You've got to say applicable law or something - another word.

Steve Metalitz: I'm going to ask Mary to respond on this and then Kathy.

Mary Wong: Go ahead, Kathy.

Kathy Kleiman: Steve, I think the larger issue here is actually when we were going down the sheet originally, the open recommendation, we stopped at preliminary recommendation number 13: consider extra territorial issues and determining what is malicious conduct.

So I think here the call is more generally to point out in the final report that we had discussions on the problems of law and on the problems that requests may come to a provider on issues that are illegal in the requester's county, be the requester a third party like a lawyer or law enforcement, but legal in the country of the provider or of the customer.

So I think here part of it it's linked to preliminary recommendation number 13. So let's bind it. That's my sense. And at least whatever our decision is or lack of decision that we should raise this as we've discussed at great length noncommercial and commercial, we should discuss that we've talked about this and it's really a difficult issue, but we want to flag it. Thanks.

Steve Metalitz: Thank you that's helpful. Mary, did you want to add something on this?

Mary Wong: Actually it was just to remind folks that going on Vicky's point that this was the point at which the full working group had stopped in the discussion of the first report from the sub team. I think this - in the last sub team call this was also where the discussion was taken to, and so that's why we brought it back today.

Kathy Kleiman: Right, because we had hit our two-hour mark and had to go.

Steve Metalitz: Now we're hitting our own two-hour mark here. Okay so Kathy's last comment that this is an issue that should be - it should be pointed out in the final report that this is an issue that would have to be considered as this whole accreditation scheme goes forward. So I'm not sure that we can do more than that at this point, but Michele did you have something to offer on this?

Michele Neylon: Yes I'm just - thanks, Michele again for the record and all that. I just think in some ways we're getting a bit down into the weeds on this one because it's, you know, no matter what recommendation comes out at the far end of this, the reality is that anybody who wants to litigate something is going to litigate it anyway. Anybody who wants to interpret a contract is going to interpret the way they want to interpret to it.

So I would just say we're actually going to cause ourselves more headaches and get more twisted round on this by trying to be over specific. I mean I can understand. I mean from my perspective I would love to see it worded in a particular fashion, and I'm sure from your perspective you'd love to see it worded in quite a different fashion for obvious reasons, because we're not in the same jurisdiction. But that's not going to happen and it's not going help either of us.

So I think, you know, the applicable laws thing you - that you were saying, that kind of solves it by not solving it. And I think that's actually probably the only sane way to approach it, because otherwise we could be spinning around this for the next six month.

Steve Metalitz: Yes I think you make a very good point that ICANN is not a law-making body. So. And there are entities set up to do that, so, including courts to resolve disputes. Stephanie, last point on this.

Stephanie Perrin: I don't want to make this -- Stephanie Perrin for the record -- more complex again. I'm just concerned about not dropping to the lowest level where there is no applicable law. So for instance, if I am coming from a country where there's no constitutional protection that provides due process and I register with, say, Tucows because I think Canada has due process and I'm blissfully unaware that that is provided for in the charter and you won't get it if you're in, I don't know, pick an African country.

I'd had to think that Tucows would not follow best practice, and I'm sure they would. But - and I'm not sure that we want to start defining best practice for due process either because I hear what Holly's saying. So I'm still in a quandary about this one as to have I feel. I want to set a bar that we don't fall below, you know? Because I think we have a responsibility under the ICANN's duty to operate in the public interest that we not allow a free fall where there is no applicable law.

Steve Metalitz: Okay. All right. I think the time has come to recess for our lunch break. Thank you everybody for helping us move through the sub team four, the huge landscape that sub team four covered. I think we've made some progress. Obviously a few things deferred to this afternoon, so we will return to those. And, Mary, could you tell us what are the logistics for lunch.

Kathy Kleiman: Thanks from sub team four for the time.

Steve Metalitz: That's outside? Okay, so - and what does our schedule say about when we'll reconvene? Two o'clock. So unless they're famous last words, we will recess until two o'clock. Thank you.

END