ICANN Transcription

Privacy and Proxy Services Accreditation Issues PDP WG F2F

Friday 16 October 2015 at 13:00 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 13:00 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.

Coordinator: Meeting room 2 at 2 o'clock. This is the PPSAI face-to-face part 2 October 16, 2015.

Man: It's an open session.

Graeme Bunton: Yes it's an open session.

Woman: The one on Tuesday.

Graeme Bunton: If you want to make registrars angry I mean that's a great title to start with. We're going to get going I think in another minute or two so people should return to their seats and regain their laser like focus and...

All right ladies and gentlemen let's take our seats and get started again. Do we have to restart the recording? We're good the recording has started.

((Crosstalk))

Graeme Bunton: (Makaley) and (Glen) are going to stop talking and take their seats.
((Crosstalk))

Graeme Bunton: So thanks everyone. I think that was good work this morning we had some good discussion and we made some progress on some issues which is excellent.

We have a couple of new people around the table who weren't here for introductions this morning. So if you didn't introduce yourself already maybe now is the right time to do that. So we'll start down there please.

(Aspalda Noa): Hello I'm (Aspalda Noa) from (Eurway). I'm in the ISPCB constituency.

Rudi Vansnick: I'm Rudi Vansnick I'm the chair of (ENPUC).

Philip Corwin: Philip Corwin I'm interim chair of the business consistency and also I'm counsel.

(Sara Bocque): (Sara Bocque) with GoDaddy.

Darcy Southwell: Darcy Southwell, (Endurance).

Susan Kawaguchi: Susan Kawaguchi I'm on the BC and a counselor.

Frank Mishlick: Frank Mishlick I'm an independent consultant to registrars.

Graeme Bunton: Great I think that's everybody. So where we're at now on the schedule is we've returned from a very nice lunch thank you for the people who made that happen.

(Glen), (Glen) made that happen.

(Glen): Thank you.

Graeme Bunton: Thank you (Glen). I'll refrain from telling her not to talk anymore. So Section 3 we're going to dive back into the illustrative disclosure framework and we've got from now until 1 - no wait 3:30 for that so we've got an hour and a half.

Man: If we need it.

Graeme Bunton: If we need it. Hopefully we don't need it and then we can carry on to some of the remaining issues that we've got. So we've identified a few issues in earlier discussions this morning that we'll try and come back to in this.

But the sense I got was we haven't had a lot of discussion about the latest version of this document. So there was a brief overview on our call two or three calls ago and this document has been out for a little while.

But we should probably hear from Todd and I think (Kathy) about the - where we're at with this current version and then we can see if we can identify some of the remaining issues we've got to sort out as well as

some of the issues we came up with this morning that are affected by this.

So I'll perhaps hand off to Todd and again thank you for your work on this and everybody else who worked on this and let's get going.

Todd Williams: Great thanks Graeme. Todd Williams for the transcript. So what you're seeing here, Graeme is right this is a document that we circulated before I think the previous call.

And we went over it very quickly at the end of that call but I think just to kind of help set the stage it might be good to just go through what it is that we're looking at and then we can go from there.

So the first some of the changes to the policy purpose I guess kind of preamble, those are all just for readability. I mean we've heard a lot today and previously about trying to make these easy to understand and so that's what this is for.

Same for the next paragraph as you scroll down to the extent that you see changes there it's only for readability.

The first kind of substantive change actually comes in 1B3 which is going to be at the top of - there you go yes. And this is a clause that we've had in and had out and it is now back in minus the word standardized per a suggestion that (Kathy) had made on the last call.

So this is about nominal fee recovery and again I'm happy to talk about any of these as we go through but I think it's probably easier to just do kind of an overview and then we'll come back.

The next substantive point actually appears three times. I'll just talk about it the first time but understand that it comes in in the next two sections as well and that's about the state of retention issues that we've been discussing.

We had changed some of the language and the concern was that it was overly complicated and it made reference back to previous sections et cetera. And so to address that point what we did was we went back to the language that had been included previously again about what a requestor has to do once it has this data.
But then we included this clause in the beginning stating that the requestor will comply with data protection laws and will use the contact details only in that it enumerates what it is that they're allowed to do with it.

And again you see that repeated in the next two sections and I think one of the open issues from this morning was how universal we want to make that beyond this particular illustrative disclosure framework.

So all of the other issues are going to come in Section 3. When we did this quick review on our last call Volker raised an issue and I want to talk about that and we'll come back to that kind of at the end and that's in this Section 3.

But of the ones that you will see in the document because that won't be reflected in the document there are change to 3B1 which talks about secure communication channels.

We've had some discussion about how feasible that is and then what exactly is disclosed and per a suggestion from James Bladel we went back to what the original formulation was which is basically just what would appear in the Whois absent the proxy service.

We didn't go to C we changed the language in C2 and 3, this was per a suggestion that (Kathy) had made from a reasonable basis to a basis for reasonably.

And the reason that we did that is that these sections are meant to mirror what it is that the requestor is providing up in Section 2. And so the idea is just that a provider if a provider thinks or if a customer has shown if we're looking at 2 that the requestor hasn't done that then that's what the basis for non-disclosing would be and so that's just again to make clear that it's a mirror of what came previously.

C4 gets to the point that we talked this morning about whether this surrender in lieu of disclosure should be mandatory or optional. I think we have two alternative formulations right now.

Be allowed to allow or if the provider offers this meaning optional which I'm not sure that substantively there is a difference between those but I think this is consistent with kind of where we came out this morning in terms of whether this should be optional, mandatory et cetera.

And the only point on this would be whatever we decide on the first question to be reflected here as well.

Six, let's see six which you'll scroll down just a little bit to get to has been added back. Again this is one section that's been in and out and

it's now back in and this gets to the point about disclosure endangering the safety of the customer.

And then one of the big issues that is still to be resolved and we touched on it a little bit this morning but it's this question of what happens when there is misuse of the data once it has been disclosed.

We've got two options. One is an arbitration option and one is a jurisdictional option. But again this tracks very closely the conversation we were having this morning and so earlier we decided on one ought to be consistent throughout.

So that's just a general overview. Real quick the issue that I had flagged that Volker had raised when we went over this in the call last time was on whether this provides a discretion for a provider to basically say to a requestor I am not going to disclose because you have not met what you needed to provide, what was enumerated in Section 2.

And so the way that it's drafted now the very first sentence of Section 3 the very first before we get to any of the kind of sub-clauses. It says upon receipt of the verifiable evidence of wrongdoing set forth above in writing.

And so, you know, the point was that that is meant to capture exactly that concern. If you providers think that any of the eight or nine things that we've enumerated above that a requestor has to provide you haven't been given then none of what follows is triggered.

You know, that said to the extent that we want to make that more explicit and basically just enumerate it as another subsection under C I guess it would be C7 at this point that just says the requestor failed to provide the provider with the verifiable evidence of wrongdoing, you know, set forth in Section 2 above I mean that's fine too. But that's it in terms of an overview.

Graeme Bunton: Thank you that's helpful. So maybe we'll tackle that last point first. I saw (Kathy) nodding her head there that adding that to was it C?

Todd Williams: Three it will be three.

Graeme Bunton: Three, seems reasonable to me. Is there - I see other nodding heads. So that is good I think we can do that and we've covered that base. Excuse me, right so we've looked at this a few times.

We can probably talk about some of the specific issues we covered this morning and/or any other issues that people have currently. And I see Steve has got his hand up first so Steve please.

Steve Metalitz: Yes thank you Steve Metalitz. Just to clarify one point back on it's on 3C4 so I guess it's the next page. There were these alternative language about surrendering the domain name registration in lieu of disclosure.

I'm not sure what all providers must either allow or be allowed to allow and there's just one too many allows in there because I'm not sure what - if it is that this should be an option and that the provider can make available to its customers.

And I think we've already said that if it does so it's supposed to disclose that fully, you know, in its terminating conditions. Is that what both of those are aiming at or is there some substitute difference between those two?

(Kathy): Remember everybody is dealing - this is (Kathy) for the record. We're dealing with kind of the same issues in different places. So I'm glad we had the discussion I guess this morning and whatever we decided should really be reflected in this language.

That this option has that one of the reasons for not revealing is that the option has been disclosed. This option to surrender has been chosen by the customer.

Steve Metalitz: If the provider offers that option.

(Kathy): Perfect language there you go.

Steve Metalitz: Okay thanks, thank you.

Graeme Bunton: So we've got language on that one now that we're - and I think it's the second one. Great, I see Volker's got his hand up, Volker and then (Kathy).

Volker Greimann: Yes just to the introductionary language that we just talked about with the provision of the evidence being sufficient. A question in my mind remains of who makes the determination of whether the information that has been provided is sufficient or not.

It can very well be that the provider thinks rightly or wrongly that the information that was provided was not sufficient and then it would be up to compliance to figure out if the information was sufficient or not.

There has to be something that the provider must also be able to rely on a certain - must have a certain security operating to be able to make that determination because if he's forced into a position where when in doubt I will be faced with compliance he will be maybe more intending to more leaning towards accepting any information as sufficient as opposed to when the determination is in the hands of the provider as to whether the information is sufficient or not.

Graeme Bunton: I think I saw Steve looking to respond to that.

Steve Metalitz: Yes I get - this is Steve Metalitz. I guess I would respond with a question of what you - if there is some specific language you would be looking for there. Remember the way this is structured now.

These are various reasons that can be used by the provider to refuse disclosure even if all the points have been met. Now this is the point of saying that all those points have not been met.

So one of those eight or nine points is missing or defective in some way. Also I think over time this disclosure framework has eliminated appeal so there isn't any basis for a requestor to appeal this decision.

I think we still have - he can ask for reconsideration and say well you didn't give enough weight to something I said here but he can't - there is no appeal to an independent third party at this point.

So I just want to put it in that context that I'm not sure we will ever come up with a framework that totally eliminates any uncertainty about the ultimate outcome but I think if we can - this is already quite specific and granular I think but if you have a suggestion about what should be put in there to deal with a level of uncertainty that you're still uncomfortable with I'd be interested to know what that is.

Volker Greimann: Yes could we please move to the language at the beginning of 6 and 3. I think the only way that we can resolve it is by rephrasing and I will think about that.

I'll make a copy of that in the proposed language on the end of the (chat).

Graeme Bunton: Thanks Volker. (Kathy).

(Kathy): Just a quick note. Reading it you can have receipt of verifiable evidence of wrongdoing but inaccurate disclosure of who the requestor is or who they represent.

There are other fields involved so, you know, let's say it's blank on everything else. So that idea of having - and for the purpose of our mandatory review in two years which the idea that a rejection if there is, if we do have (Paul's) chalkboard and we're keeping track of that which I don't think we will.

But the idea that something was thrown back because it was incomplete versus rejected may wind up being a difference that means something later on. So just I think there was something...

Graeme Bunton: Okay thank you and Volker you'll take a crack and that and send that back? Awesome, anything else on that particular topic? No, good. Do we have any other - Stephanie and then (Kathy), Stephanie.

Stephanie Perrin: Stephanie Perrin for the record. I hate to slow things down but I'm ruminating over the last line and authorized the provider to communicate such reasons to the requestor.

Now that appears to be mandatory at the moment. If this is a fishing request from I don't mean it in the PH sense from an ex-spouse or an ex-religious group and they don't know for sure and they're casting a wide net then providing the reasons i.e. I fled this group two years ago and they're after me solves the fishing request.

So it would be nice if that was discretionary.

Graeme Bunton: Thanks Stephanie.

Stephanie Perrin: You don't really mean that I could tell from your tone.

Graeme Bunton: I don't know what you're talking about. I wonder if there is discretion in there where the service provider can respond in a way without explicitly phrase - like forwarding that response but say...

Stephanie Perrin: It needs to be working though because that discretion is not there right now I would suggest.

Graeme Bunton: Do we have other...

Darcy Southwell: Are we on C3?

Graeme Bunton: No we're back on A here a bit.

Darcy Southwell: I know but C3 kind of gives providers...

Graeme Bunton: Into the microphone if you would please.

Darcy Southwell: Sorry this is Darcy Southwell. C3 gives us some unless I'm totally not following this right but that gives us that basis for reasonably refusing based on our position.

So if we were given information about a customer to indicate let's say it is a fishing expedition as you referred to Stephanie that that would be our - we could say that we're not going to disclose because we have reason, you know, we have our own reasonable beliefs here.

Graeme Bunton: That sounds like it covers it to me and I see Todd and then Steve I think.

Todd Williams: Well I was going to ask the question what is the concern? So if the response that the requestor gets in that scenario is I am now disclosing because - and you can even use the language from C6 here.

The customer has provided or I have found, you know, a basis for believing that somebody's safety is in danger. What's the concern, what's the risk? There is no information in terms of contact ability that's being disclosed in that case?

Graeme Bunton: I think what Stephanie is saying was that acknowledgement that someone's safety is at risk is acknowledging that they own that domain name.

(Kathy): Right, if part of the fishing expedition is to find out more about how is behind that domain name because you're actually after them for stalking purposes or harassment purposes.

Getting back that confirmation that you can't disclose because they're stalking me is that it's exactly the confirmation the requestor was looking for in this harassing situation.

So it sounds there is something to what Stephanie is saying. I think Darcy is right that now with that clearly added new section that Todd and I talked about and kept broken out about safety I think there is a cover for not providing the details if there is some safety risk.

Graeme Bunton: Just to confirm we have that in there already? Okay, so that's covered. Steve.

Steve Metalitz: Yes I agree with (Kathy) on that. We need to look at all of the different, you know, some of the reasons for non-disclosure are based on things that the provider knows or decides based on looking at the request.

Other things are based on what the customer tells a provider and in that situation which I think again is a, you know, particular factual situation the provider has a way of dealing with that which I think would minimize the risk which is C6.

(Kathy): Would it be possible - this is (Kathy), to add a comment or clarification because I see what Stephanie is talking about in 3A that we're authorizing the provider to communicate such reason.

We're actually in some ways if you take this direct language authorizing the provider to pass along the exact or maybe requiring them to pass along the exact communication of the customer whereas really we're saying that's not necessarily the case particularly when safety is involved.

So maybe we could just think about some re-wording. I don't know if you want that to go back to Todd or stay with the co-chairs.

Graeme Bunton: I think that's reasonable that we can put up that language. I don't have a strong opinion and maybe that's for you guys to see if you can put that language in together.

Stephanie hopefully last comment on this point.

Stephanie Perrin: I think we do need the cross reference and I've got it in my head because at the moment it is shall advise must disclose and authorize. So there is no discretion there.

We need the cross reference to the danger section where we talk about this. So it's going to be something like subject to the safety concerns provided for in Section (unintelligible).

Graeme Bunton: Okay thank you. All right I think we've got that base reasonably covered. (Kathy) did you just put your hand up again?

(Kathy): The next issue (unintelligible).

Graeme Bunton: Yes so I'm not sure what exactly the next issue is going to be so if you have one that you'd like to raise please go ahead.

(Kathy): Sure, if we could page all the way down to the bottom. Option number 2 jurisdiction and I just wanted to show Todd would have the sub-team memory more than I would but this seems to go back a long time.

This has been there for as long as I remember and I just wanted to read it because it may help address something we were talking about in our first session our opening session.

So jurisdiction. In making a submission to request disclosure of a customer's contact information requestor appears to be bound by jurisdiction at the seat of the service provider for disputes arising from alleged improper disclosures caused by knowingly false statements made by the requestor or from the requestors knowing this use of information disclosed to it in response to its request.

Presumably that these include violating the terms that is agreed to for the revealed data. So like blogging it suddenly or posting it publicly, harvesting it.

So this language has been around for a while. This may be one of the answers that we were looking for in another area of our discussion.

Graeme Bunton: Yes thanks (Kathy) I think that's helpful that gets back to the teeth argument how are we going to put teeth on the false request or misuse and that seems reasonable to me. I see Steve has got his hand.

Steve Metalitz: Yes I think (Kathy) is right to flag this but remember this is I think the main issue in this annex is still unresolved which is whether it would be this or whether it would be the arbitration that's above.

And the first sentence of this annex to the annex if you scroll up a little bit it says neither option below is intended to preclude any party from seeking other available remedies at law.

So this is, you know, obviously there may be other things that people can do if there is misuse. But I don't think there has been agreement on - between these two.

I think the concern from the perspective or requestors is that I think I don't think it comes as a surprise that sometimes providers are corporate alter egos that are located in jurisdictions where it's really not viable to accept jurisdiction to be sued in that jurisdiction because you've made a request because you're not going to, you know, there is no due process in those jurisdictions.

So and this is something that's, you know, obviously under the control of the provider as to where, whether it's incorporated in the Cayman Islands or (unintelligible) or wherever.

So I think that's the hesitation for accepting option two because it may have nothing I mean it's totally a jurisdictional convenience. The registrar is located there.

Again looking at the situation where the registrar is the parent or the owner of the provider. The requestor isn't there, the customer of course we don't know where the customer is that's why we're asking for this information but the customer is not there either.

We can be pretty confident that very few of the registrants who use these services are necessarily located in these jurisdictions of

convenience. So that's the hesitation there to accepting option two on a blanket basis.

I think there could be plenty of circumstances where it would be un-objectionable but to say that in every case where you ask for a disclosure and you, you know, meet all of the - try to meet all of the requirements you're also subjecting yourself to litigation in a jurisdiction of convenience is difficult.

Graeme Bunton: Thanks Steve. Yes I'm not sure what the solution to that would be like whether you could specify a jurisdiction that's more convenient to you. I saw (Makaley) has got his hand up and (Kathy) has got her hand up so (Makaley).

(Makaley): Yes thanks, (Makaley) for the record. I can appreciate from Steve and other people's perspective that you may have issues in certain jurisdictions. My problem with some of this could be that, you know, where is the line.

You know, for us for example again I'm being completely self-interested which, you know, why the hell wouldn't I be? As an Irish company operating in Ireland we try to do everything under Irish law under the Irish jurisdiction.

Now okay I know for a while that okay if you're working for a large law firm that's not going to be an issue for you because you probably either have an office in Ireland or you have a friendly whatever that you can work with or, you know, that's fine.

So you're probably not going to have an issue with us. But if we're not careful how this - sorry how this ends I mean you could be putting a position in where because you're having issues in certain jurisdictions that now you're trying to force everybody into kind of do back flips to fit around that.

Is there a way and I'm not saying that there is because again I'm not a lawyer and I don't know but is there a way to specify some kind of recognition of some legal standard that would help with this?

I mean for example I don't know are the jurisdictions which do not recognize the Madrid trademark stuff or whatever the hell it's called. I'm just throwing that out there.

I honestly don't know I'm just trying to see is there some way to fix this without breaking things for those of us who are in kind of normal sane jurisdictions who I don't think you're going after. At least I hope you're not.

Steve Metalitz: Right, can I respond?

Graeme Bunton: Please.

Steve Metalitz: Yes I'm not sure I have a solution. I mean one solution is option one. You have arbitration instead. Now that has problems too because the system does not currently exist although it could easily be modeled on the systems that do exist.

We obviously have arbitrators who arbitrate issues related to domain names all the time. So I think it's doable and it helps to deal with this

problem but I think I'm just explaining to you why I think option two isn't acceptable as the sole option in this circumstance.

Graeme Bunton: I see (Kathy) in the queue and then Volker.

(Kathy): I wanted to go up to the line at the very top that neither option below is intended to preclude any party from seeking other available remedies at law. And that's what we're trying to achieve is that ability to seek that remedy at law, that ability to go to court in which case jurisdiction is an issue.

When we talk about arbitration and I'm not going to start my rant on that one right now but there is no arbitration form for this right now. There are no teeth for this right now.

We've talked about difficulties and ICANN enforcing penalties and the whole idea of setting up having survived the UDRP just, you know, set up process. The idea that at the end of our process we're going to begin the beginning of a new kind of UDRP type creation of an arbitration system and the procedures and the protocols.

Sorry I actually delve into that. So option one I think is really hard. Option two jurisdiction I think was modeled somewhat on the UDRP. Isn't there, doesn't the provider, doesn't the complainant agree to be bound where the registrar is located in a UDRP for purposes of challenging the UDRP the UDRP decision or halting it?

Mary Wong: I don't have the specific language but it is two options. I believe it's either the registrar or something designated by the registrants or something like that.

Steve Metalitz: Again in that one you know where the registrant at least in theory you know where the registrant is. You've gotten, you know, you have the Whois data or whatever you know where the registrant is.

So when you bring the case you could take into account that, you know, I might get sued in that jurisdiction.

(Kathy): Right but so it's the or where the provider - well where the registrar is located or where the registrant is located. If he were eliminating the or where the provider or the registrar is located.

Steve Metalitz: But this is just where the provider is located.

(Kathy): But it seems pretty parallel.

Steve Metalitz: I'll just say by the way and (Kathy) - I mean (Kathy) when we were first working on the UDRP and we got the UDRP up and running in a third of the time that this working group has been gone.

So it can be done and obviously it was their kinks needed to be worked out but we know something about arbitration. It's not a panacea I'm not suggesting it is but I think there are kind of precedents we can go by.

(Kathy): But WIPO had been working on it for a long time before too and yes we go way back.

Graeme Bunton: This is the...

(Kathy): That wasn't a comment on you Steve that was a comment on me in this process.

Graeme Bunton: I've got Volker and then Paul in the queue. But the language for jurisdiction on UDRP is the domain holder's address as shown for the registration of the domain name in registrar's Whois database at the time the complaint is submitted to the provider. Yes okay.

Mary Wong: Either or the registrar or the provider.

Graeme Bunton: So it's either the registrar or that one is the point there so it's an or for jurisdiction there. Volker and then Paul.

Volker Greimann: To (Makaley's) comment where he referred to jurisdictions where certain laws are commonly accepted practices do not apply the same as they would in other countries.

I think if a registrant is based in a country where a trademark doesn't account for anything or copyright doesn't account for anything and he distributes works that would seem as infringing as most countries of the world that distribution.

Even though we hate it is his right under the laws of the country. And we cannot force this registrant into a - to sue in a jurisdiction where his home base legal concepts don't apply the same way.

So that is something that we also have to keep in mind. On the other hand I fully accept and understand the problems that a complainant may have of (Monte Hall's) type situation where he opens the doors and finds he has just lost everything because the registrant is in the jurisdiction where he would never think of suing him in the first place.

We I think we need to figure out how to make this work in a way that is both acceptable to registrants that need to see their rights protected under their home jurisdiction but also the complainants who would very much like to avoid certain jurisdictions just because they are ridiculous for registrants or for complainants to work in.

Graeme Bunton: Yes thanks Volker, Paul.

Paul McGrady: Paul McGrady for the record. Just a clarification on the choice of law provision in the UDRP. It's the complainants choice between those two options either the location of the registrar or the jurisdiction of the registrant issue and the Whois record.

So there is a complainant's choice option. What's that?

(Makaley): If you're dealing with Whois privacy proxy protected registration that is going to be the providers address in Whois.

Paul McGrady: Presumably because we don't know where the customer is. So that was just a clarification on the UDRUP issue. And it's not - those choices are always based upon who has good courts and who doesn't.

So for example if the registrant and the UDRP context were New Zealand and the registrar was in Ireland I'd pick Ireland because I don't want to fly 18 hours if I have to go to court with my local counsel I want to fly 6 right.

And so I mean it really is, you know, there really are lots of reasons why you would select one or the other. It doesn't really have to do with

due process concerns necessarily and so that's the background on the UDRP.

Graeme Bunton: Thanks Paul. So it feels a bit like we're getting around to the language in the UDRP and maybe that's acceptable for the jurisdiction or at least something to ponder as we move forward. Paul has got his hand up.

Paul McGrady: It can't mirror the UDRP because we don't know where the - we don't know where the end user is located right. So you would be choosing between the location of the registrar versus a grab bag who knows what's going to happen outcome.

And so that's de factor choosing the location of the registrar because nobody is going to pick wild card.

Graeme Bunton: Right, well I don't have a solution for that at the moment but that is clearly something we need to spend a bit more time on. So maybe let's move on to some other issues within this document unless people want to speak to that some more. No.

Man: (Unintelligible).

Graeme Bunton: Well those two. Before we get to - Volker you've got one more on that guy, little guy?

Volker Greimann: Yes just a small comment which is a situation that we've seen at least as registrar in which also is probably of great annoyance to any complainants in the UDRP is that when you are raising a UDRP against a registration that is currently under privacy proxy protection or if not and you send in that complaint in English and then the response from the registrar comes back.

Yes but the registration agreement was in Chinese or Japanese or Kiswahili or whatever then you have to translate that and you have no choice about that. Your complaint is either forfeit or you translate.

And that situation could also apply in a certain sense into with the jurisdiction of the contestational or the whatever you call it, arbitration afterwards. You have a similar situation already which is not favorable to the complaints and I agree with that. It's a design to protect the registrant's interest.

Graeme Bunton: Thanks Volker. So we have two other issues that we've flagged this morning, retention periods and something I'm calling asylum. Do we have any other text choices we need to make in the document that we can think of?

All right so maybe we go - Darcy.

Darcy Southwell: This is Darcy Southwell. Just for implementation purposes on 3B. I can scroll to it. We see just that providers have to within one calendar day after the time for customers responses pass that we have to take action.

I'm just wondering from an implementation perspective if we're setting up a standard that might now work. Not all providers would respond like do a followup on a routine abuse complaint within a day if there is a holiday or if they're not a 24 by 7 team for those routine followup things. Am I - so the first line.

Todd Williams: So I think James Bladel raised that point in a call a little while ago and we had changed the initial time to five calendar days. So that one calendar day after, it's coming after the five so it would be basically six after the request has come in.

Darcy Southwell: Well it's one calendar after the time has passed and there is no response. I have - I raise it because I have teams that they're not there on Sunday night or Sunday or a holiday.

And so I worry that other providers would have a similar challenge and we're setting up a policy that's going to dictate an implementation that's going to be challenging.

Graeme Bunton: I saw a whole bunch of hands go up very quickly. I'm going to go in order this way so it's going to be Steve, Todd and then Volker.

Steve Metalitz: Yes just again I think this is what Todd was saying. This is one calendar day after the time has passed and the time is 15 days. So it's a known date. When you send out, you know, when you pass the complaint for the request - I got to make sure I have my terminology right here, onto your customer you could set your clock that on the 16th day if you haven't heard back then you have to respond to the customer.

If you have heard back then you have 5 calendar days after you hear back. So in other words it's a known date. I get the point that it might potentially be, you know, everyone could send in their complaints on December 9 and for countries that celebrate Christmas that would be the day. So I hear that but it is a known date.

Graeme Bunton: Thanks, could we get around that by first business day after? So I see Chris. Todd did you have a comment there too? No, I see Volker and then Chris.

Chris Pelling: Chris Pelling for the transcript. Why are we using that (unintelligible) business days as per the (RAA)? Because obviously business days is then a far simpler task for the registrar and more importantly for holidays in Thailand for instance I've never known a country to have so many holidays.

There is only one registrar in Thailand so - but they have like 74 days a year in holiday. They've only got one week (unintelligible) make this holiday but 74 days they're off.

So, you know, I'm just wondering why we've opted not for business days like the (RAA).

Steve Metalitz: That's a good question but the downside of going that way is that if there are 74 holidays I have no idea how many business days it might take to get to three or five.

How many calendar days it might get to get that many business days. But I'm not, you know, I'm not wedded to this of course but I think that's the other side of the coin there.

Graeme Bunton: Volker and then (Kathy).

Volker Greimann: Yes Volker Greimann speaking his name for the transcript. I think we need to adjust this to business realities and business day changing that to business days is I think the first step.

We've danced this dance in the locking of domain name PDP just a couple of months ago. So I think having that discussion again is just needless because we already agreed to another PDP how to do this best.

And I think one day is just too short. I mean we are a smallish registrar compared to some of the big ones and I am happy to say that I have a team of two people helping me.

One part-time and one full-time but we have other things to do as well. We have deadlines, we have things that we really, really need to deliver in a certain time period.

And when there is sickness, illness, holidays then a time period of one day that might seem reasonable to an outsider or someone working for a big company is very unreasonable for a small company.

And there are companies that are a lot smaller than we are and having to look at all these deadlines is simply too much. So I'd rather propose a turnaround of three business days than this one calendar day that's in there right now.

Graeme Bunton: I'm not hearing a lot in defense of calendar days. Is there anybody who feels really strongly about calendar days? (Vicki).

(Vicki): (Vicki). I don't feel strongly about calendar days but I do feel strongly about the timeline. So that if we're going to go I think it's 14 days now if we're going to switch or 15 days if we're going to switch it to business

days I assume it will be 10 business days or whatever the traditional equivalent is.

Graeme Bunton: That doesn't offend me. I see Todd, (Kathy) you had a response in there too I think. Could you...

(Kathy): Just to the timeline then I'll respond after Todd. But so promptly notify the customer about the complainant disclosure, request that the customer respond to provider within 15 calendar days and I know we had talked about that extensively.

So then going down to B within 5 calendar days after receiving the customers response or one calendar day. So that's the whole timeframe that we're looking at.

Todd did you want to say something and then I'll...

Todd Williams: Well no it was just related to that whether the change from calendar to business was also in this section as well for uniformity. I don't necessarily mind doing that I just think then that is extending the overall time period by a pretty significant amount if we're then adding time on the back end as well.

Graeme Bunton: I think (Kathy) wants to respond and then I've got Holly and then (Makaley). I'm not sure how much we need to labor this though. The calendar days is on the registrant end of things and they're not necessarily operating as a business.

In my head if I'm territorialized I'm okay with calendar days for customers but the business that is responding should be on business

days. So maybe we don't need to adjust this particular piece we just need to adjust the next piece.

(Kathy): This is (Kathy). I would agree with that and I like switching to business days. I can understand why one or two, why two or three business days would be necessary because there may actually be emergencies that have arisen or other types of problems, you know, big flags that are flying.

Just noting that in some countries there are double holidays. So in Israel if the Jewish New Year falls - when the Jewish New Year falls it's two days that the whole country is shut down.

So I'm glad we're moving to business days that will keep in mind that will help with some of these holidays.

Graeme Bunton: Okay good.

Man: Can we just turn it back to Todd?

Graeme Bunton: Yes, no I think what we can do is you're right we can pass that back to Todd and (Kathy) to make that change and we can carry on. Do we - are you guys more or less clear on where we're at?

(Kathy): Could we ask the provider I mean I just ran this past Todd and what's realistic, you know, two days, three business days. Not what's easiest but what's doable.

Darcy Southwell: This is Darcy Southwell. I mean one to two business days as a provider I'm happy with. We can make that work. I think I do like too to somebody's point earlier about if you have emergencies.

Our teams are going to mess around with taking child porn down before they mess around with this. So if I've got 20 of those that showed up today that's where my team needs to be focused.

So two business days would probably be preferable but would not be the practice necessarily.

Graeme Bunton: Cool I think we're good. So let's move on then I think to retention periods in Annex E was a topic that we flagged earlier this morning. I'm not exactly sure what section that is. Does anybody know off the top of their head?

Steve Metalitz: Well it's the one that's in there three times. I think the first one is in 2A6.

Graeme Bunton: Two A 6 is I think where we're at.

Steve Metalitz: Yes right there. See where it says the requestor will comply with all - would comply with all applicable data protection laws while - I think that's the - I'm sorry.

This is Steve, I think the issue was whether that was raised was whether a provision like this which says that requestor has to comply with all applicable data protection laws after or while retaining customers contact details and will use customers contact details only to determine whether further action is warranted or resolve the issue.

Should that be generalized even into areas where we don't currently have a disclosure framework but we're saying in advance that

whatever disclosure framework ultimately emerges should have that feature I think that's the issue that was on the table.

Graeme Bunton: So that seems like a reasonable request to me that in general disclosure should operate under those constraints. Do we have people who disagree with that notion?

Man: Do you disagree with me?

Graeme Bunton: No, sorry I'm not at all used to sort of broad agreement.

(Makaley): If you want us to disagree just say would some please disagree with me and don't worry one of us will do it.

Graeme Bunton: No, no Stephanie rises to the occasion. Stephanie I see your hand.

Stephanie Perrin: Thanks Graeme I'm here for you. Stephanie Perrin for the record. I just wanted to tack on my usual caveat that in jurisdictions where there isn't any data protection law best practice should apply.

That doesn't mean it's open season on the data. So once again we need some kind of best practice there.

Steve Metalitz: We have a partial best practice because it says to comply with all applicable data protection laws and only use of details for the specified purpose. And I understand that that's not the same thing as a comprehensive data protection law but it is a best - not a best practice it's a minimum standard I guess is what we are saying.

Stephanie Perrin: I would argue, Stephanie again. I would argue that by saying only use it and only use it for this purpose you haven't restricted those in a non-data protection bearing jurisdiction from disclosure, selling, marketing blah, blah, you know.

Steve Metalitz: I don't understand that point because it says the requestor will only use the customers contact details to determine whether further action is required and it goes on in legal proceeding.

That applies whether there is a data protection law or not. So again I'm not saying it's the same thing as having a full data protection law it isn't but it is a minimum standard that would apply even where there is no applicable law.

Graeme Bunton: Did you have your hand up there (Makaley)?

(Makaley): Yes I think Stephanie - it's (Makaley) for the record. I think Stephanie you did a wonderful job of arguing with us which is great but I'm not sure that you need to because I think it is covered.

So I think it's one of these things I mean what you are saying is okay if there is no data protection law then best practices need to be followed and that's fine. But I think we have (unintelligible).

I mean unless there is something in what we've outlined there that is missing a best practice which I don't think is the case because I mean it's saying that you can't abuse the data which is essentially the issue isn't it or am I missing something?

Stephanie Perrin: I don't want to take up our time. Supposing I just send an email with all the pieces of data protection law that aren't listed here how about that? Because basically disclosure like okay all right you're shrugging so I'll walk it through this may be painful.

Graeme Bunton: I don't know that that's strictly necessary.

Stephanie Perrin: No.

Steve Metalitz: We're agreeing with you.

Stephanie Perrin: Yes but we're missing bits, we're missing bits. So...

Steve Metalitz: Stephanie I'll just say yes. As the transcript would show when we have one. I'm not saying this is a substitute for having a data protection law but it is a minimum standard.

It applies even when there is no data protection law. That's all I'm not - it is not a substitute for it.

Graeme Bunton: And you people thought I was weird for being surprised by the general agreement. All right I feel like that one now we have covered. Stephanie is leaning in and raising her eyebrows like it's not but feel free to bring that up on the list and by all means bring clarity there where you think we've missed it.

The next - that was retention periods and there would seem general agreement that we're going to bring that into the rest of the report and not just leave that in Annex E.

So great. Also known as Annex B I was meant to ask Mary why it changed.

Mary Wong: We dropped some annexes.

Graeme Bunton: All right. Mary said we dropped some annexes so it's been what I'm calling (bemoted). Thank you good night try to land. Levity aside we have a piece on asylum which is 3C6.

And I'm not sure who brought this piece up although I suspect if I had to guess it was (Kathy).

Mary Wong: It's in the sub-team four.

(Kathy): Actually it wasn't but I supported it.

Graeme Bunton: So 3C6 that the customer is provided or the provider has found specific information, facts and/or circumstances showing that disclosure to the requestor will endanger the safety of the customer.

And there was another piece or another interpretation of this. Steve do you have a...

Steve Metalitz: No I think the question was whether something like this not necessarily verbatim this should be a feature in those areas where there currently isn't a disclosure framework but this should be a reason for non-disclosure.

Graeme Bunton: And that also seems like a reasonable thing to do. Volker has got his hand up, Volker.

Volker Greimann: Yes similar to this I'm not sure if it has to be the safety i.e. personal physical safety. It might also be a legitimate interest or reasonable legitimate interest that may be at risk by disclosure not just the physical safety.

I mean there is other ways of harming people, unduly harming people that they have a right to be protected from. And I'm not talking about not being subjected to a lawsuit for infringing on someone's rights of course. That's why reasonable should be in there.

Graeme Bunton: I'm a little bit concerned about making that super broad because, you know, then that applies to everything and we want to keep that I think reasonably narrow.

I'm not sure if you just picked up some homework for trying to phrase that in a way that is broad enough to cover the issue you're speaking to. I see Steve's got his hand up so maybe Steven has a wonderful formulation.

Steve Metalitz: Well I don't know that I do but I think this was intended and again the people on the sub-team can correct me if I'm wrong. I think it was intended to deal with an exceptional situation, a real situation but an exceptional one.

Where, you know, you've got the requestor has checked all the boxes and actually has made the case that, you know, they need this information and yet there is some extraordinary piece of information that reflects on the safety issues.

I mean in our part of the world the question there was very real concern that this could be misused to say well anybody who is committing criminal offenses and is using a proxy service could say well, you know, if they find out who I am I'm going to jail and that's endangering my safety.

I know that's not what's intended here and I just think if you open it up to, you know, reasonable interest or something like that you transform it from an extraordinary situation to something that's going to come up, you know, that could be the basis for almost any rejection. So I don't really think that's what's intended here.

Graeme Bunton: (Makaley) please.

(Makaley): Thanks, (Makaley) for the ever growing transcript. Just to Steve's point I mean so is there a way then to word that so that it's, you know, physical harm or something?

I don't know I'm just trying to see is there a way to kind of narrow that down because what you are saying makes perfect sense. I mean if it's worded too vaguely or too broadly or whatever way you were comfortable with describing it then saying that I don't want to go to prison because I don't like prison.
It's very different but I'm still a criminal scumbag, it's very different to reveal my contact details and I will be shot or seriously harmed. I mean I'm just wondering is there something that we can do there.

Graeme Bunton: Thanks (Makaley). To me that's covered by how it's phrased currently which is will endanger the safety of the customer. I see (Kathy) and then is it Rudi?

(Kathy): Yes let me just check Steve will you - advocating for changes of wording or are you okay with where it is?

(Makaley): I'm okay with where it is. I'm concerned about it growing. I'm relating to you concerns that were raised to me, but I think this is a reasonable way to strike the balance. And it was appreciated. It did seem weird you guys were agreeing. Rudi?

Rudi Vansnick: Well, being not a native English speaker, safety is also giving me another impression then. And I'm following Michele at the point. I would rather use the word "security" that defines a bit more. To me, safety means I will be protected from jail. Yeah, I feel safe. I feel safe means...

(Kathy): No, no.

Rudi Vansnick: If they review my information I will go to jail. That's also for me a definition of safe. I'm sorry. What if you got to translate this stuff into other languages?

Graeme Bunton: That's true.

Rudi Vansnick: Don't forget.

Michele Neylon: I understand the problem linguistically. I do and I appreciate that. I think - I know exactly what you're saying. But if you'd say security in English, it's very, very different to safety. I feel safe in my home. But I'm probably not as secure in my home as I might be in my office

because my office has got biometric sensors to get in and out the door and it has doors that are like that thick.

And that's not an issue. I mean, others could speak to this greater but saying security is very different. And I don't offer services via what goes into WHOIS for security. I don't know what else I can say really. Sorry.

Graeme Bunton: Thank you. Did anyone else have their hand up on that? I see Phil's got his hand up. Phil?

Philip Corwin: It may be a valid point that for non-English speakers' safety is somewhat ambiguous. Should we consider some defining modification like physical safety, something like that, that makes specific the type of safety we're referring to?

Graeme Bunton: So people seem to be nodding about physical safety, and that seems to have that broad agreement I enjoy so much. So maybe...

((Crosstalk))

Graeme Bunton: Holly.

Man: (Unintelligible). Come on.

Holly Raiche: Holly Raiche for the transcript. If physical safety in people's understanding would mean jeopardy for their safety - for example, we're worried about women and refugees. We're worried about stalking.

Now do people have in mind all those sorts of things that are encompassed by the term physical safety? I mean I think that arguably it does but - (Kathy) has a problem).

(Kathy): Yes if we're worried about burning down battered women's shelters. I know that's a stretch but that's really the outlying area where we are. Is that physical safety? Is that all...?

Man: I mean...

((Laughter/Crosstalk))

(Kathy): I'll have questions too. I'm going to pick on Paul.

Paul McGrady: Paul McGrady for the record. (Kathy) and I turned out to be the hippies of this group. I don't how that happened but it worked out. I mean, but what about intimidation? I mean that's...

(Kathy): No, no.

Paul McGrady: No, no, let me, let me...

Graeme Bunton: Yes it should include a death threat that includes your physical address basically is what we're - yes.

Paul McGrady: Would physical safety and company, would that be...?

(Kathy): Intimidation, yes, stalking.

Paul McGrady: Would that - or just, you know...

Graeme Bunton: If it's a threat to your physical safety I think that would be covered under this. I see Volker's got his hand up.

Volker Greimann: I'm not quite comfortable with physical safety. There's ways of mentally harming people, breaking them by ways that have nothing to do with physical violence. I would be very hesitant to limit it that way.

Graeme Bunton: (David) has his hand.

(David): I mean it is a - it's a bit of a - I mean this is an issue that is the subject of some sort of Internet debate, not just here. The idea of where - what exactly constitutes violence. Some people would say that like, you know, a credible threat of safety or just like ongoing harassment as Volker suggested is not - you know, there may be no credible threat of actual, you know, physical attack but there's definite attempt at sort of psychological intimidation.

I don't - it's one of these things where where there is a big ongoing physical - ongoing debate in the broader Internet, we should probably not try and solve it within this working group rather than debate about what it is or is not included within the definition of violence.

Let's just say or - you know, let's just put in extra wording to include harassment or something to make it clear rather than speculating too much whether or not it is included. Other people will assume that wording.

Graeme Bunton: Thanks (David). So I think the options as we have it is to leave it at safety and encompass that word broadly, which I think most of us do.

Or we can add some ellipses in there and say “including such things as intimidation and threats of violence.” I don’t feel particularly strongly about either.

Man: I think we’ve brought ourselves to a standstill.

Steve Metalitz: Yes I think we’ve heard arguments both to make this narrower and to make it broader and possibly the best pragmatic solution is to leave it as it is, which was what the subteam came up with.

And as I said on the issue of - if you will - globalization of this, if this is to be part of other disclosure frameworks, it wouldn’t necessarily have to be verbatim. I mean, you know, because we’re kind of putting little pieces into a disclosure framework that doesn’t exist and that won’t exist in our final report that is one outside of the intellectual property area.

And I have to say one thing that concerns me a little bit is the only pieces we’re putting into this are reasons why information should not be disclosed or limitations on the use of the information. I support both of those but it’s kind of incomplete and one-sided.

And if we could come up with a formulation of what we think these disclosure frameworks should say on why information should be disclosed or the circumstances under which this information should be disclosed, that would be more balanced.

I don’t think we can do that and keep on our time frame here, but I just want to point that out, that we’re putting a couple of bricks in a wall

here that doesn't exist and they're only in one part of the wall so - or whatever the right structure is for us to be talking about.

So I just want to encourage us not to get too carried away with this. The fact that we don't have these disclosure frameworks for law enforcement and for security malware type things is I think somewhat disappointing but hopefully we at least are kind of charting the way for those to be developed as soon as possible.

Graeme Bunton: Thanks Steve. So I think where we got to is there's sort of general agreement that we're going to probably leave it as is and that also we should pull that into the final report more broadly. And I think - of course Stephanie's got her hand up. Just a moment.

We might - we're pretty close, aside from Stephanie's comment here, to move on from the framework unless there are any other issues in here that we feel we need to tackle.

(Kathy): Repetitive abuse language?

Graeme Bunton: Oh, oh...

(Kathy): Repetitive abuse.

Graeme Bunton: Maybe you can find that while we hear from Stephanie.

(Kathy): That's not here.

Man: Oh that's not?

(Kathy): (Unintelligible) to add this.

Man: Oh no, we need to come back to some other issues. But in this (unintelligible) formerly (unintelligible).

Graeme Bunton: Sorry, one sec. Actually, why don't we hear from Stephanie and we'll sort that out. Please.

Stephanie Perrin: Thanks very much. Just a question. Stephanie Perrin for the record. How did we - what language is going to ensure that access for those two particular groups actually gets developed? We're not including it here but how do we make sure it happens?

Graeme Bunton: Access for which group, sorry?

Man: Law enforcement.

Stephanie Perrin: Law enforcement and private sector security firms.

Graeme Bunton: That's a good question. Maybe we need to put something in this report that - I think it's kind of in there now but we maybe should be more explicit and clear language to say we've come up with this illustrative framework for one area but the system really needs more.

And one thing that - you know, ICANN - we should be encouraging people who are experts in those areas to come forward and work on disclosure frameworks that are appropriate for those topics.

Stephanie Perrin: Far be it from me to be argumentative. This is Stephanie again for the record. But I would go stronger than that. The intellectual property

constituency has participated and come up with a model which we have duly debated for two years. We've got something we can live with. Law enforcement and the security guys have not.

I would say they must, must have a framework that has the same discipline as the other guys, allowing that of course law enforcement has much more power and authority, but they still need a framework for due process. And why on earth should we have it only for the intellectual property guys and not everybody else?

So they can pony up to the bar and give us a draft. And half the work's done for them because we have this framework already. Thanks.

Graeme Bunton: Thanks Stephanie. And I think we should be encouraging those groups to do that. I see Steve and then (Kathy).

Steve Metalitz: I was just going to say that later today when we go through the draft final report I think there are places where we could insert that. I would agree with you. We're a little bit too gentle.

Stephanie Perrin: Deferential is the word.

Steve Metalitz: I was going to say gentle, but you know, about the lack of participation from this group.

(Kathy): But what I worry about - this is (Kathy) - is by the time these groups come together and come back to us, we won't exist. This working group will have phased itself out. So the how to - what we've seen is that it's the debate among the stakeholders that create - that shows the different sides of this, that shows the concerns of those requesting, the

concerns of the providers who are revealing and the customer data that's being revealed.

How do we ensure that that type of review - that type of robust multi-stakeholder review - takes place as these - you know, a year or two or three from now when these other frameworks come in?

Graeme Bunton: Thanks (Kathy). I haven't the foggiest notion how we do that. I don't know if that kicks off a PDP process for each one of those where we - you know, reconvene in some fashion or other. People are convening to go through this process in a more narrow way. I'm not sure what the solution to that is.

(Kathy): I think it should be part of our recommendation that it not be mere implementation, that someone kind of sitting at a desk doesn't say, "Well it looks enough like that other template," that we do think these are different types of scenarios. And they have to go through some kind of robust review process.

Graeme Bunton: I think that's reasonable. Stephanie?

Stephanie Perrin: This is Stephanie Perrin. I think it would be really great if we develop them for them and attach them as appendixes whatever and whatever. That would certainly get the attention.

Graeme Bunton: That might be considered trolling.

Stephanie Perrin: Possibly.

Graeme Bunton: And would take a considerable amount of time, but thank you. I think for real that brings us to the end of our Annex E/B discussion. So thank you. Oh, Todd?

Todd Williams: Sorry. Just real quick, I mean, because (Kathy) and I have been taking notes as this is going about drafting changes, you know, calendar versus business, things like that. And I guess the one area that we were just discussing that we weren't sure where the working group had kind of left us in terms of a charge go back was on this question of the annex, specifically of the two options.

I guess we just weren't sure where it is that we're going with those. Everything else I think we're actually basically done. And it may be that we don't want to decide that right now, and that's fine. I just - we were - wanted clarification.

Graeme Bunton: I don't think we got to a decision on that particular piece.

Steve Metalitz: I don't think so either. I think we had a couple of suggestions of possible sources to look to. But I don't think we reached a consensus on that yet. That's not the right word. We didn't come to closure on that.

Graeme Bunton: All right, thanks everybody. That was good.

Woman: Thank you Todd and (Kathy).

Graeme Bunton: Yes especially thank you Todd and (Kathy). You guys did a whole lot of work on that one.

Man: Should we go back to the Section 1 issues that we didn't get to?

Man: Sure.

Woman: (Unintelligible)

Graeme Bunton: Did we? Sorry, one second while we just figure out what's next. So what I think we just got to is we're going to take a...

Man: As long as we don't take a break right now.

((Laughter))

Graeme Bunton: Boo. We're going to take a 15-minute break and then we're going to come back and look at some of the remaining issues from this morning and any other issues we need to discuss. So you have 15 minutes. We'll be back here at 3:30 quite promptly. Thank you.

END