ICANN Transcription
Privacy and Proxy Services Accreditation Issues PDP WG
Tuesday 15 September 2015 at 1400 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 15 September 2015 at 14:00 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.

The audio is also available at: http://audio.icann.org/gnso/gnso-ppsa-15sep15-en.mp3

Attendees:

Todd Williams IPC
Sara Bockey RrSG
Roger Carney - RrSG
Frank Michlick Individual
Steve Metalitz – IPC
James Bladel RrSG
David Hughes - IPC
James Gannon NCUC
Alex Deacon - IPC
Luc Seufer RrSG
David Cake- NCSG
Carlton Samuels - At–Large
Graeme Bunton RrSG
Griffin Barnett - IPC
Osvaldo Novoa – ISPCP
Val Sherman IPC
Vicky Schlecker – IPC
Terri Stumme BC
Holly Raiche ALAC
Kathy Kleiman - NCSG
Lindsay Hamilton-Reid RrSG
Susan Kawaguchi – BC
Iranga Kahangama -

Apologies :
Kiran Malancharuvil - IPC
Don Blumenthal – RySG
Michele Neylon - RrSG

Susan Prosser RrSG
Darcy Southwell – RrSG
Stephanie Perrin NCSG
Phil Corwin – BC
Sarah Wyld – RrSG

ICANN staff:
Mary Wong
Marika Konings
Amy Bivins
Terri Agnew
Nathalie Peregrine

Coordinator: Recording has started. Participants, you may proceed.

Terri Agnew: Thank you. Good morning, good afternoon and good evening. This is the PPSAI Working Group on the 15th of September, 2015. On the call today we have Graeme Bunton, Iranga Kahangama, Holly Raiche, Val Sherman, Steve Metalitz, David Cake, Sara Bockey, James Bladel, Frank Michlick, Alex Deacon, Lindsay Hamilton-Reid, Terri Stumme, Susan Kawaguchi, Todd Williams and Roger Carney. We have apologies from Darcy Southwell, Stephanie Perrin, Susan Prosser, Phil Corwin, Don Blumenthal, Michele Neylon, Sarah Wyld, Kathy Kleiman and Paul McGrady. From staff we have Mary Wong, Marika Konings, Amy Bivins, Nathalie Peregrine and myself, Terri Agnew

I would like to remind all participants to please state your name before speaking for transcription purposes. Thank you very much and back over to (Graeme).

Graeme Bunton: Thank you kindly. So this is (Graeme). I'll be sharing the call today. That certainly sounded like a good number of regrets for today's call. Even though it still looks like we've got a reasonable number of people in the room. So we should be able to make some forward progress. Before we get that far, any updates to (SOI's) we should be made aware of. And your weekly reminder to keep those up to date. Seeing no hands, on the agenda for today is that

we're going to hear from Sub Team Three, talking about the possible revisions to the (NXE) (unintelligible) Disclosure Framework. And the work that they've been doing. And then, if we get so far, we'll talk about any issues arising from Part Three of the Working Group Public Comment Review Tools.

Unless there are issues with that agenda, I'm going to suggest that we dig right into it. And I'll call on someone from Sub Team Three which I suspect is going to be (Todd). But I should probably comment that that team has done a lot of good work. And it's really appreciated. And we should make sure to recognize that. I see (Todd) has his hand up. So (Todd).

Todd Williams: Thanks (Graeme). (Todd Williams) for the transcript. So I think the easiest thing to do would be to just walk through this document. One point though, that I would note. The document that we are looking at in the Adobe Room is -- I think -- a little bit different from what we circulated on the broader group. In that I'm not seeing the kind of comment boxes off to the side that we'd include to note which public comment that we reviewed these proposed changes were coming from.

I mean, I can flag those as we go through them. But I would certainly encourage everybody in the working group to look at that. And again, just too kind of stress -- from the outset -- that I made in introducing this last week. You know, this is - our intention is that this more of an (illicited) tool to kind of illustrate or point out if we -- as a working group -- decide that the public comments, the substantive changes that they recommended or called for -- you know -- have merit. Or something that we would want to accept. This is where those might go. And this is where they might fit.

The document is not -- you know -- some sort of consensus that we, as a sub team, came to and are recommending this is what it should look like. It's more -- you know I think -- when you looked at the summaries that we had kind of circulated three or four weeks ago. We thought this would help to kind of envision where those changes might go. So that's why we've -- you know --

we've included those bubbles to point out this is where those changes are coming from.

But -- in any event -- unless anybody has any objection, I'll just kind of walk through and explain kind of how these work. And where they came from.

Graeme Bunton: (Todd), (Mary's) mentioning in the chat that they can't show where doc comments in the (PDF) in the Adobe Connect Room. So if you could - I think you can see this text highlighted in white. Maybe you can - people can follow along at home with the documents that were sent out. And if you could mention those comments that are put in place. Having said that, please go ahead. And walk us through what you guys have been working on please.

Todd Williams: Perfect. Will do. Thank you. And thanks (Mary). So the first is this inclusion by not requiring that disclosures automatically follow any given request. This was based on multiple comments that we reviewed. (Black) (Unintelligible) Systems, Google, (Access Now) and various individuals, (Ralph Herring), (Simon Kasain), et cetera. Who basically argued that there should not be any kind of automatic requirement? But rather it should be some sort of discretion, et cetera. So we included this language in the preamble to kind of make that explicit. If you look at the structure of -- especially Section Three that we'll get to -- the only reason it's really required is that if a providers deciding not to disclose, they have to provide their reasons for doing so. But just to address the points that these comments raise. And to kind of make that explicit right up front. That's where that language comes from.

The next proposed change came from a comment from (CBT Open Technology) which basically just called for a review after a certain number of months or a certain amount of time had passed. Adds to the (efficacy) to balance that this framework is trying to strike. So that's where that comes from.

And then -- as you scroll down -- when we get to (1 - B - 3), we have this language about standard nominal cost recovery. As we pointed in the comment box -- and what we circulated -- we reviewed six comments that were opposed to that language. And three in support. And so, we've excluded it here. But -- again you know -- some of what this document reflects is -- you know obviously -- not final. And so to the extent that the working group as a whole decides to give more merit to the three - the arguments included in the three comments as opposed to six. That's why that's...

We added the work (vexatious) to Sub Section Five. Just for a comment from an individual (Nick Odell). We've highlighted (1D) and just raised the question does the working group need to revisit this per the (11,000) comments from the "Respect Our Privacy" campaign which argued that everyone deserves the right to privacy and no one's personal information should be revealed without a court order. So there's no substantive change there. It's just more a flag for further discussion.

All right. (2A) we've added this verifiable evidence of wrongdoing including and then kind of enumerated -- you know -- further down. You know this was a big point of contention -- both in our sub team and then in our last working group call -- on this particular topic. Whatever that was four weeks ago, now. Again, the document that we're reviewing now is not a final version. And so I would encourage if anybody thinks that the standard of verifiable evidence requires something more than what's enumerated here, to raise that point. But this is the place where it makes the most sense to include it. And so it's (2A, 2B and 2C) includes that new language taken directly from the Save Domain Privacy Petition. And then enumerates kind of what that might be.

I see (James) hand up. I don't - should I just go through the whole document and then come back? Or should I pause and we can kind of discuss as we go. I'm open to either.

Graeme Bunton: Let's take (James') comments and try to keep the comments relevant to the section we're discussing is what I think - I hope will happen. We can move through that way. So if you're open to it, (Todd), then we can hear from (James).

Todd Williams: Yes. Absolutely.

(James): Thanks (Graeme) and thanks (Todd). Just a question about the addition of the word (vexatious). Can you give us just a little bit of background there on what drove that inclusion? And the impact of that is both from a legal and non-legal context.

(Todd Williams): Right. So that was based on the comment from (Nick Odell) who -- in his comment -- just said, "There should be some prohibition against (vexatious) requests" basically. So we added that. In terms of the -- I guess -- substantive work that that word is doing. And how it -- I guess -- adds to frivolous or harassing. I mean, frankly, I don't necessarily have a clear distinction on that. I mean, we could talk about it at the working group, what that means. I mean, do you have a concern about it?

(James): No. Not a concern. Just I wasn't clear on what that - kind of what you just said. I was unclear on what that brought to the table that wasn't covered by frivolous or harassing. Just thought it was already covered. Thanks. And mainly just making sure that there wasn't something that I was completely missing. That there was something - you know, I didn't - you know, go to law school. I didn't know if there was some secret legal meaning behind vexatious that I wasn't picking up on. Thanks.

Graeme Bunton: Thanks (James). I also see (Holly's) got a hand up too. So maybe we'll go to (Holly).

(Holly Raiche): Thanks. First (James) vexatious - just for those of us who have gone to law school, is a (unintelligible) cries about. (Vexatious) and it just means either

calls made without substance or something that is done with some kind of a bad purpose in mind. It's just a standard phrase. I didn't even think about it. And I wouldn't be concerned about it. I would like to stress though, in the inclusion of the phrase verifiable evidence of wrong doing. That seems fine. Everything that follows the group has agreed meets the test of verifiable evidence. And we sort of haven't got there yet. So this phrase is very much a placeholder. And it will require just a little bit more thought and discussion amongst the working group as to whether that stays there or not. Thank you.

Graeme Bunton: Thanks (Holly). And I think it's pretty clear that we're going need to spend a bit more time on that particular phrase and what that means to us. And what we want that to mean going forward. So let's go back to (Todd) and continue working our way through the document. And I'm not sure that discussion around defining that term is going to be something we do on this call. Or if it's something we add to our list of issues we need to come back to. (Todd) if you could continue.

(Todd Williams): Great. So back in (2A) change the (2A) to adding the words "if any." And that was in response to a comment from (RIAAISPI) specifically wanting to make explicit that use of a previous relay function was not required. So that's what work those are doing. (2A5) Addition of if applicable twice per multiple comments that we reviewed. And then addition of and the data first used and/or of application and registration of the mark, per a comment we received from an individual (Tim Cramer).

The "if applicable" is in response to comment that common law march ought to be eligible for the system in addition to those for which - that are registered. And in the data first used from this comment from (Tim Cramer) about wanting to include that in what it is that the request you're providing such that if the registrant had priority. Had the domain name before then. That's something that we could point out in that response.

All right. (2A6B) is substantially reworked. And this is - you're going to see again in (2B and 2C). And this was per comments from the (NCSG) and (Cyber Invasion). Basically the requestor would have to kind of agree to certain things in the request as far as what they will do with whatever information they are given once they've got it. So, one is only use it to determine whether further action is warranted to resolve the issue to attempt to contact customer or a legal proceeding. And that was already in there. It's just all been moved to the first kind of section.

And then (2 and 3) are now new. One is to only retain it for as long as is necessary to achieve whatever it is they're doing in the first section. And then the third is to comply with whatever applicable data protection laws while they have it. So for (2B) some of the changes are repetitive of what we just talked about in (2A). So I won't go into those again. I will highlight the ones that are new.

The first is a change to (2B1), per a comment from the (RAAIFFPI) about the exact URL where the allegedly impending work is located or representative samplers where such work is located. I've got two hands so I think I'll stop.

Graeme Bunton: Yes. That last point is curious. I'm not exactly sure what that would mean. I would be interested in examples if anyone knows what the (RRA) was specifically mentioning there. And then I see (Steve) and (James). (Steve).

(Steve Metalitz): Yes. This is (Steve Metalitz). And I was a little slow getting my - clicking on the hand there. But I really was going back to this - these changes to (6B). And I guess because - and we have (James Gannon) on the call. We have others from (NTSG) on the call. So maybe they can explain what was meant by "requiring compliance of all applicable data protection laws while retaining customer's contact details." Is this a security concern? Or, I'm just not sure what that is - exactly what that's driving at. Oh, an explanation of that would be great.

Graeme Bunton: Well, it looks like we've got (James) with his hand up.

Man: It's Cyber Invasion.

Graeme Bunton: Yes. I see James with his hand up right after you. So and Cyber Invasion. I think is (James Gannon). Let's hear from him.

(James Gannon): (Unintelligible) (NTSG's) action on this about (unintelligible) invasion. So given that information regarding the policy, we need to potentially account that in certain jurisdictions. The requestor will be in the role of data controller. Taking into new legislation and some (unintelligible) legislation as to privacy and need to reflect that with the policies in certain jurisdictions. And it can be -- you know -- applicable worldwide and (unintelligible). And maybe a quick data protection laws thus the request the provider needs to be aware of how they are in process and (unintelligible).(Unintelligible) may be somewhere else. And should be something in here to convey information between the provider and the requesting party if disclosure is required. You know there is security standards that will be abided by those two parties to ensure that the grows and potential data lawsuits (unintelligible) focus.

Graeme Bunton: Thank (James). That last piece is interesting. I'd be curious to hear from other providers on that and whether they do encrypted communications for this sort of thing currently. And whether or not that would be our juris to set up. I see (Susan) and (Holly), then (James). (Susan), please go ahead.

(Susan): So I'm curious about (B2 62). Only retain customer's contact intel for as long as is necessary. And I apologize (James). But somehow, when you were speaking, it sort was fuzzy on my phone. You may have addressed this. But is that something - you know, there's a lot of different jurisdictions. So if I'm requesting that information and haven't received it from a specific proxy vendor, is the proxy vendor going to inform me of those - of the time stand that I can retain that data? And then exactly how to go delete that data.

Graeme Bunton: That's a good question (Susan). I don't know if that would fall under the data protection laws or whether we want to specify. But I don't know how we could because we don't know how long whatever process takes place. And certainly I wouldn't expect a service provider to understand for each jurisdiction that they might be dealing with, how long those rules are. I would think it's up to the requestor. But I don't know how that is enforceable. I see (James) with his hand up. And then (James Gannon). (James Gannon) are you responding directly to that question?

(James Gannon): Yes, if you don't mind. I've actually (unintelligible).

Graeme Bunton: Sounds a little better to me.

(James Gannon): (Unintelligible) I actually agree with (unintelligible) so we're (making reference to 61). It's fair to say in certain jurisdictions, yes it would be a requirement (such personal) data was not retained for a period greater than the use of the actual data. So if an attempt of a situation where there was some flexibility for jurisdictions and requestors that we will be dealing with. Both the providers, in an attempt to have a policy that's workable on a global scale. I think having the statement in there that as long as necessary to achieve the objectives of -- for example -- Section (1 and 2) so they can deal with all of the issues. The requestor would no longer retain that later.

So I think that would be a broad policy statement that would work at a global level. The requestors use their own jurisdiction as long as they adhere to their national laws. So that's nothing that I think we should be going to road. For example, if we had an IT firm here in Ireland, they would absolutely adhere to our state of protection legislation which would mandate us to (have up to) about 60 days to destroy the data after that. But we need to allow a global policy some flexibility for individual requestors to adhere to their national guidelines. But over that base level, I think the wording that we have it at the moment, which is as necessary to achieve the objectives (unintelligible) statement for global policy.

Graeme Bunton: Thanks (James). I'd be curious to hear from other people as to whether they think that flexibility in the language we've got there is going to be sufficient. I've got (James Bladel) and then (Steve Metalitz). (James).

(James Bladel): Hi. (James Bladel) speaking. Thanks. And some of my questions or comments have already been covered. But I'm just kind of still reacting to the specifics presented by (62 and 63). I wanted to make sure that we're being sufficiently explicit perhaps in (61) even about what is not permissible on the part of the complainant in terms of the use of this contact information. For example, you know, storing it, collecting it in a database, aggregating complaints over time. And then publishing that to third parties or even just putting it on the general public.

And then I think that what I would be more comfortable because of the concern where - and I think (James) touched in this, where we have complaining party in one jurisdiction. You know, privacy provider in let's say, U.S., where there are no specific data protection laws. Then the customer being in a third jurisdiction. I think I'd like to see some language that specifically says something along the lines that the customer - I'm sorry. The complainant will indemnify the privacy service provider against any misuse of the data. And I think that - I think that will be key. Because -- you know - or at least allow carve out so that that could be included in the provider's terms and conditions for filing a complaint.

And my concern here is that we're creating a loophole where it will be like a slow leak. And eventually the services will be collected and tabulated over a number of complaints. And that data will be misused. Thanks.

Graeme Bunton: Thanks (James). I suspect the idea of an indemnification might be a hard sell. But perhaps there is language that we can come to there that sort of addresses both (James Gannon's) concerns and yours there. Let's hear from (Steve).

(Steve Metalitz): Thank. This this is (Steve Metalitz). My concern was really with the practicality of this which I think have already been raised a bit. But - and so I guess I'd just like to ask the following of the proponent. So let's say I'm a complainant. I do obtain the contact details, because -- you know -- after going through this process. And I either contact the customer - try to contact the customer, can't reach them. Decide not to pursue it or I contact the customer. And possibly - you know, the problem is resolved. Or you know. In other words, I do what Number One says. Then Number Two, in the future I make a second complaint about a second domain name.

And I find - it turns out that's the same registrant. I go through the same process. And the same registrants name comes up. Now would I be able to actually associate those two? And note that this is somebody who is - where the issue has arisen twice. And that might make a difference for me in determining what action to take. But it almost sounds as if I have to forget about the first one. And purge that from my records. And therefore just assume that this person has never - you know, the issue has never been raised before with regards to this registry. Is that was intended here and if so, why?

Graeme Bunton: That's a good point (Steve). I would think that using the language we've got there you would be able to keep the registrant name. It's just the contact details. You'd still possibly be able to relate those. But you may not have that full record from the "who is."

(Steve Metalitz): Guess that's a possible reading of this. But my problem there is -- of course -- this person just uses a different name. But maybe all the contact details are the same. And that's the way that you know that it's the same person and stuff. I'm just asking what's that - what Two was intended to prevent? I understand it's intended to prevent (James Bladel's) scenario of going into the business of -- you know -- selling databases to bad actors or something. But from the viewpoint of a complainant who's not interested in that business,

but just interested in protecting your intellectual property rights. It just seems this could really hamper efforts in that scenario.

Graeme Bunton: Thanks (Steve). I see (James Gannon's) got his hand up. And then also (Susan). So let's go to (James Gannon).

(James Gannon): Thank you and I accept that is a business issue for the requesting parties. However, you know, we need to accept that in a global policy, we need to be observant of individual data protection legislation in various jurisdictions that we're working under. And I would see better attention issues with retaining data in that manner. And while providing a method by which bureaucrats can request this personal information is something that I think is obviously a thing that the group has decided that we need thankfully that we've made some (steps) from requesting that information to allowing the requestor to compile that information even for internal purposes within their own company.

Though we can always go to the example of -- you know -- selling a database of personal information. Even for internal purposes we haven't made that leap to say that we're also able and going to enable it. I think if we are going to make that leap, that's a discussion that we need to have in the working group, that if we're going to enable it. And even internal database development that we need to have a wider discussion over that point. But I accept (Steve's) (unintelligible) that it would be a business issue for...

Graeme Bunton: Thank (James). (Susan).

(Susan): So back to point two of this, only retain customer's contact details for as long as was necessary, you know, if when there are security issues on the Internet that, you know, Facebook is, you know, usually one of the many targets we share information all the time so with other security departments because, you know, then we can act in a unified manner.

So I'm assuming that if I request proxy, you know, the underlying data in a for a proxy registration and then but I'm working on an issue that has - that it's obviously targeted several major companies which is really not targeting the company the company is targeting users.

And so if I, you know, find out one piece of the puzzle and share that with other major security departments is that going to be a violation of the request process?

Graeme Bunton: That's a good question (Susan). I think...

(Susan): And then...

((Crosstalk))

Graeme Bunton: …right now looks like it quite possibly is.

(Susan): Okay. And then the follow-up is if I share it then am I responsible because I've requested it to ensure that everybody that I've shared that with because this is a bad actor, this is someone who's basically, you know, taking money from individuals.

Am I responsible for ensuring that they then delete the data when they - when we've resolved that one issue?

Graeme Bunton: I think you are responsible if you've shared it. Sorry if I'm editorializing. Because it's not proven that this is a bad actor.

It sounds like at this point you've met a number of the requirements that we think it's possible that it certainly hasn't gone to a, you know, formal legal process to determine it's a bad actor.

So I think there is a reasonable assumption of risk on your part but if you're going to take that information and share it that you would have some responsibility for that information.

I see James Gannon and James Bladel...

((Crosstalk))

(Susan): Yes, can I just...

Graeme Bunton: ...feel free to respond.

(Susan): Can I just add one more little element to that?

So often times when I am making a request to either proxy either to a proxy provider or just to a registrar because they are hosting the content that I forward that information which is usually contact details that connect domain names involved in a scam.

I forward that back to a registrar. So is the registrar bound to then comply with all of this what I've agreed to do and then delete the data that I've sent to them?

Graeme Bunton: I'm not sure. Let's hear what James and then - or other James and I think James had to say. James Gannon?

James Gannon: Thanks (Graeme). So there's two issues I found here. And so I agree with part of (unintelligible) which we have to remember that (annex) here which were talking about is for intellectual property infringement and not malicious use.

So we haven't examined the framework and releasing details due to malicious use. So they're two slightly different things.

And also on the point of threat intelligence sharing and in my experience -- and this is an area that I work extensively in -- the majority of threat intelligence sharing and through (unintelligible) areas of this one is more on IP address side.

So yes there is some unofficial methods for sharing threat intelligence on registrants. However it's not a heavily formalized area and it's not something that's used widely enough.

It's believed to be this objective that's (not) in the framework just yet. And the majority of threat intelligence is based around IT addresses and non-bad actors within (AS) numbers and various (unintelligible) methods.

And there's not the huge amount of commercial work done on registrant threat intelligence. And I would have concerns about automatically assuming that a registrant is connecting to one malicious domain name that and automatically we're going to view the domain that has been used under the same registrants because there's many issues.

We talked about this before around an involuntary hosting about where and other issues. So we went into that detail before so I don't believe that it's really relevant too technically at the moment. But I accept that we may have to look at this in the future at security focus.

Woman: Hello? (Graeme).

Woman: Hi this is - I think we lost audio for (Graeme). (Graeme) if you're speaking we can't hear you.

Man: I don't see anybody else in the queue. Or is -unless (Graeme)'s back maybe we could just ask (Todd) to just pick up with his walk-through because I think we've had a good discussion on this one topic.

(Todd): Sure. This is (Todd), happy to do that. And just for the sake of time I would propose we jump forward to Section 3 and specifically 3B and then we'll kind of see how far we get on that. Are you there?

Man: Yes.

(Todd): I think that was odd, okay. So 3B, four specific changes. The first is on the timing. We've replaced the X with three calendar days after receiving customer's response or one calendar day after the time for customers response had passed.

In the document that we circulated we noted that there were alternative formulations. One was 14 days total. One was ten days each, et cetera. So, I mean we could debate which of those we think is appropriate. But those are all outlined there in the document for your consideration.

The second propose change is from (Vanda Scartizini) and the individual suggesting changing the language from shall to is encouraged but not required to.

The third is the addition of using secure communication channels for how the disclosure actually happens. And that's per comments from NCSG, Cyber Invasion and (Reagan Lynch) who's an individual.

And then the fourth is changing what is actually disclosed from the previous formulation which was the contact information it has for customers that would ordinarily appear in the publicly accessible Whois for non-proxy privacy registration to main mailing address and contact information for service of process that it has for customer.

And that was based on a public comment from an individual (Reed Baker) whose argument was that what was disclosed should track what would

typically be available in a public records database if you were looking at for example a corporate entity.

So I think I'll stop there because that's a lot of kind of substantive changes. And I assume we'll have discussion on some or all of those four.

Graeme Bunton: Can you hear me now?

Man: Yes.

Man: Yes we can.

Graeme Bunton: Oh, I wonder what happened there? That was curious. Thank you and thanks for stepping in there Steve and (Todd). I see James has got his hand up. Let's go right to James.

James Bladel: Thanks (Graeme) and thanks (Todd). Just two quick points, first of all those date ranges are from an operational standpoint probably unworkable.

Three calendar days or one calendar day, you know even for a large registrar that has 24-hour teams responding to requests like this I think we're probably going to miss I don't know, 20% to 50% requests outside of those windows. So that's comment number one.

I think, you know, let's look to some of the other policies that exist that usually I think five calendar days is where they seem to land on a standard.

And then the last one here secure communication channels. I don't know how that can practically be established, you know, unless the - there were some developed portal for these disclosures. I'm concerned that that is also a pretty heavy lift to put on service providers and also you know, on complainants.

You know, I think that if, you know, if the request is made via email there'd be a form that it would transmitted that way as well.

And then finally the information, you know, sending information that is a subset of or a superset of the information that is included in the Whois record or would've otherwise depending on Whois records to me is not, you know, I just I feel like that's not really the purpose of this particular working group.

I think that, you know, it's really just expose the information as that it wouldn't normally appear in Whois so it's the simplest and most straightforward approach to a disclosure.

So those are just my reactions to Section B. Thank you.

Graeme Bunton: Thanks James. If I can respond myself hey I can see James scanning the chat saying PGP encrypted email wouldn't be a big ask. I wish that were true.

It's probably a bit of work. I don't, you know, unfortunately it's not common. I wish all email was encrypted. That would make life better.

But it - that's not the case and I think that would require a fair amount of work to be able to communicate with people that way.

And then the alternative is that we, you know, all providers end up having to build a sort of secure Web site to communicate back and forth with requests - requesters and registrants.

And that's a fair amount of development and you want to make sure you get that right so it raises the bar offering these services in a way that might be problematic.

I see Steve Metalitz and (Val) in the queue. Steve?

Steve Metalitz: Yes thanks, Steve Metalitz here. I would agree with what James - two of James us points about your communication channels and about the last change here to be little one.

I actually wanted to mention the one change you didn't talk about. And that's the change to (Vonda)'s suggestion to change it from service provider shall do one of these things to encourage but not required to.

I mean I think this is kind of motivated by some, you know, it goes back to the very first exchange that (Todd) walked through that to make it clear that you're not - if there's any automatic disclosure under this system.

I think that's what's motivating this because read literally this really just would make this a worthless template.

You know, because the expectation the whole idea here is if you put certain things, information forward in your request you're going to get an answer either yes or no.

Either the information's going to be disclosed or it's not going to be disclosed and a reason will be given.

So to say that the service provider doesn't have to do either one of these things after receiving the complaint and forwarding it to the customer and getting the customer's response back and then they don't have to do any - you know say anything that would kind of eliminate the purpose of this. So I think we - I would have to oppose that second change in the - in B.

I think it really results probably from a misreading or misunderstanding of this. And I think it really goes more to the issue of whether there should be automatic disclosure. Thanks.

Graeme Bunton: Thanks Steve. And that seems pretty reasonable to me. Let's see if anybody else objects. But I can see Bladel on the chat is agreeing.

I will also support James' comments that three calendar days is probably not enough time. Five is far more sensible.

(Val) please?

(Val): Thanks (Graeme). This is (Val).

I'll make this very brief as Steve just said precisely what one of my concerns is about this encourage but not required section. It would, in fact it seems to me nullifies the standards all together. So keeping brief I would have to object to that as well. Thanks.

Graeme Bunton: Thanks (Val). I see James Gannon in the queue again. James?

James Gannon: Not surprising that I would support the retention of the encouraged to but not required to language. I that getting in new providers flexibility in this area would be a useful tool for the acceptance of (unintelligible) by the greater public invite as to commenters essentially looking to get rid of Annex C entirely I think this would be a way to make it a little bit more palatable. And I think that takes into account the fact that we have many people who didn't want Annex C at all anymore. So we need to retain that flexibility.

Yes, sorry as well as (unintelligible) add into the comments there that as long as we're keeping their ability to refuse that we're not going to an automatic and disclosure process then we might be okay. So we need to be careful with how we tweak language in this area.

Graeme Bunton: Thanks James. I have a sense that I think we're covered there that you've retained the flexibility and so reinforcing it here in 3B is perhaps not required.

We've got about 14 minutes left and still a good chunk more of this document to go. So I want to see if we can get to the rest of it before we end the call.

(Val) is that an old hand? Yes - oh yes it was. Okay. (Todd) if you could continue please we'll move on from this point and keep going.

(Todd): Great. So the next 3C several different things to highlight, two and three these are sections where in our initial report we have put out two alternative formulations of what the language out to be and basically received more public comments in favor of what is now here included as opposed to alternative formulation. And so that's just reflected in two and three.

In four per the comments from NCSG and cyber invasion there is language that is added making that requirement that basically surrender in lieu of disclosure is not just on option but is something that is available across the board.

And then there is a new Subsection 6 added for comments from CDT open technology NCSG and cyber invasion basically tracking the language of five customers, providers or providers found significant information facts or circumstances but then adding this part about showing that disclosure to the requester will endanger the safety of the customer.

So there's a lot substantively there. I think we all stop there and probably talk about this.

Graeme Bunton: Thanks (Todd). I put myself in the queue just to see if we have any sort of clarity on what it would mean to surrender the domain. Is - does that mean the domain transfers an ownership to the service provider or are we deleting the domain?

And do we need more clarity on that or is just surrender satisfactory in text, (unintelligible) to others?

I also don't see any other hands in the queue so pending more of that then perhaps we carry on.

(Todd): All right just moving on.

Graeme Bunton: So clearly I inspired (Holly) and Steve to get in the queue next so (Holly)?

(Holly): I think surrender's not the best word. I think the idea is - the idea was if the in customer simply does not want an end (unintelligible), does not want - recognizes that their information (unintelligible) should be given the option to (unintelligible) I just want to give up the whole thing, I do not want to be contacted at all I think that makes sort of a - and I don't know the proper word for that (unintelligible) anger.

Graeme Bunton: Okay thanks (Holly). And Steve?

Steve Metalitz: Yes this is Steve Metalitz. I would kind of defer to what the - I want to hear what the service providers think about Number 4 there because we had this discussion before about whether this should be the mandatory policy.

My question actually goes to six and whether is that a subset of what we already have there in five about the pretext or is this - I guess is there anything that wouldn't, you know, would fall out?

Can we substitute six for five or is there something - how much overlap is there between these and how much congruence is there between these two reasons?

So I guess I would just, you know, ask that if - I guess that's for - also from - that's from CDT and open technology, NCSG, cyber invasion. So if anybody wants to comment on that. Thanks.

Graeme Bunton: Steve and James you guys have a good here's my question lineup for response process today.

Nine minutes left and we still of a bit more document to get through, so James if you could respond but with haste please.

James Gannon: With haste. Me and Steve are (unintelligible) a call for (unintelligible).

And so on the surrender domain name I would be off support and transferring to the domain name to the complaining party that opens the security consideration that will need to be addressed as well.

And on the merging of five and six as well as we retain the additional text so no, I have no issue with merging those into a single and section for that additional text, I think is clarification that's required.

Graeme Bunton: Okay thanks James. I see James Bladel just hopped in the queue and I think that's an old hand from Steve.

I would think that those domains end up deleted the ones that are surrendered because I would be very surprised if a service provider wants to be responsible for them. James Bladel?

James Bladel: Yes just real quickly the reason is here we can't write a policy for a service provider assuming that they are also registrars because a service provider would not have the ability necessarily to transfer the name to third-party. That would be either a function of a registrar or some other or a reseller or some other intermediary.

So just wanted to make sure that we're focused on surrender is deletion. Thanks.

Graeme Bunton: Thanks James.

All right we need to think a little bit more about five and six there and whether they overlap enough as per Steve's question. But let's hear from (Todd) and see if we can get through the rest of this.

(Todd): Sure real quick. So 3D and what you were looking at an Adobe you won't see anything because we didn't touch the language.

But in the document we circulated we just noted in the comment box that we received comments on both sides basically of 3D.

3F is deleted. That was per multiple comments that we received expressing concerns about certain aspects of the appeal process that we had outlined.

But basically those concerns came from opposite sides essentially of that process whether that was not robust enough, to robust, et cetera.

They tended to merge in the sense of just suggesting that it be scrapped and so that's why that's the way that it is.

And then 3G, you know, we had put two potential options out for comment on the Annex and received more comments in support of Option 2 than Option 1. So that's why that's drafted the way that it is.

But you'll see in the comment box that we included in the draft that we circulated there was really not very much commentary on kind of either side of that.

I think it was may be two comments to one or three to one. And so I would just flag that as kind of an issue for kind of further discussion amongst the working groups. And then that's it.

Graeme Bunton: Thanks (Todd) and thanks again to you and your whole sub team for working through these issues and presenting them today. There's been a good discussion.

So I see we've got about six minutes left here. I don't think we're going to get into part three of the public comment review tool though I would say that next week's call is going to be the last call for issues from Part 3.

Do we have any thoughts on these last couple sessions that (Todd) has raised for us here or the - where we're at with this entire document? We'd like to hear those now. We've got a few minutes left.

I see Steve's got his hand up.

Steve Metalitz: Yes thank you. Steve Metalitz. And I would just echo what you have said about the sub team's work. I think that you've really advanced the ball here considerably with these - with this markup.

And just looking at this Annex 1, annex to the annex about, you know what happens, you know, resolving disputes about well the title may not be exactly right.

I think what - as we think about this you have to go back to the section we talked about before about using the customer's contact details only for certain purposes and how long you retain them and so forth.

Because I think what was intended here in the original draft was that this annex gives you two options for how you resolve complaints arising from misuse of the material as well as all statements made in order to obtain the contact information. I don't think our title in the annex was quite right there.

So just to, you know, and just to point out that this whole question of what process is put in place and, you know, if you go back to G it's based on false

information but then the question is what about the misuse of the information, how is that covered so just to say that as we discuss that we need to keep both those in mind. Thanks.

Graeme Bunton: Thanks Steve. Four minutes left and we've got James and (Holly) in the queue so you've got two minutes each tops. James?

James Bladel: Thanks (Graeme). I'll be very brief. Thanks again to (Todd) and the Working Group for their work on this.

Going all the way back to Page 2 which is Section 3B I'd like to put a marker down for future conversations that the deletions of 1B3 is something that we need to discuss a little bit further.

I realize that some comments do not want there should be a fee associated with filing or resolving complaints or requests of this nature.

However that does not change the operational reality that service providers will either have to hire people to process these requests or repurpose existing employees.

So that the cost is real and it's not going away. And in fact we can expect that it will increase significantly with the adoption of these accreditation frameworks.

So I just want to put a marker down for that section that we need further discussion on 1B3. Thank you.

Graeme Bunton: Thanks James. Fair enough. (Holly)?

(Holly): Yes I also want to put a marker in. And it's just against - again that phrase of verifiable evidence. We the group need to have a little bit more discussion on that and then the group itself needs to have a bit of a discussion on that.

Graeme Bunton: Great, thanks (Holly). I can see that (Mary) just captured that there.

(Holly): Okay.

Graeme Bunton: And so that is a discussion that we should figure out where we've got time for and have that relatively shortly.

Ten fifty-eight. I think that will wrap up this call. (Todd) and sub team again great work, thank you very much. And it was a I think productive discussion today. We flagged some issues for clarification, none of it to me is terrifying so that's always positive.

We'll see you next week. Let's make sure to have a bit more discussion on the list. It's been a little quiet. And again last call for issues arising from part three of the comment review tool.

Thanks everybody. Have a wonderful Tuesday.

Steve Metalitz: Thanks (Graeme).

End