ICANN Transcription
Privacy and Proxy Services Accreditation Issues PDP WG
Tuesday 17 June 2014 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 17 June 2014 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-20140617-en.mp3

On page:
http://gnso.icann.org/calendar/#june

Attendees:
Steve Metalitz - IPC
Justin Macy – BC
Sarah Wyld - RrSG
Chris Pelling – RrSG
Osvaldo Novoa - ISPCP
Darcy Southwell - RrSG
Graeme Bunton – RrSG
Don Blumenthal – RySG
Phil Marano – IPC
Susan Prosser- RrSG
Val Sherman – IPC
Tim Ruiz – RrSG
Griffin Barnett – IPC
Tatiana Khramtsova – RrSG
Libby Baney – BC
Susan Kawguchi – BC
Volker Greimann – RrSG
Kathy Kleiman – NCUC
Holly Raiche – ALAC
Alex Deacon – IPC
Tobias Sattler – RrSG
Todd Williams – IPC
Luc Seufer – RrSG
David Cake – NCSG
Stephanie Perrin – NCSG

Apologies:
Christian Dawson – ISPCP
Michele Neylon – RrSG
Jennifer Standiford – RrSG

ICANN staff:
Marika Konings
Amy Bivins
Terri Agnew

Operator: Please go ahead, this afternoon's conference call is now being recorded.

Terri Agnew: Thank you, (Tim). Good morning, good afternoon and good evening. This is the PPSAI Working Group call on the 17th of June, 2014. On the call today we have Graeme Bunton, Val Sherman, Tobias Sattler, Holly Raiche, Osvaldo Novoa, Steve Metalitz, Darcy Southwell, Don Blumenthal, Chris Pelling, Justin Macy, Todd Williams, Libby Baney, Sarah Wyld, Griffin Barnett, Tim Ruiz, Luc Seufer, Tatyana Khramtsova, Alex Deacon, Volker Greimann, Susan Prosser and Susan Kawaguchi.

We have apologies from Michele Neylon, Christian Dawson and Jennifer Standiford. From staff we have Marika Konings, Amy Bivins and myself, Terri Agnew. I would like to remind all participants to please state your name before speaking for transcription purposes. And, David Cake just joined us as well.

I would now like to turn it back over to you, Don.

Don Blumenthal: I appreciate it, Terri. I assume Michele and Jennifer – well I know Michele is playing in the sun in Miami. Normally I'd be jealous but Michigan is not bad today. No there's a hosting conference there so I know it 's taking a lot of people away who will go directly to London from there.

In any event, thanks for – thanks for joining today. First, just want to remind people to update your SOIs if there have been any changes. We did get a new SOI yesterday. We've got a new member, Dan Burk, I think it is. Dan or Daniel, I don't know, I haven't met him. He's from the US Food and Drug

Administration. I was hoping he might be on the call today but I guess not. Maybe we'll meet him in London.

So why don't we – oh, yes. Kathy just joined. I just mention that because Holly had asked in chat.

We're pretty well on schedule, as we've talked about the last few weeks. What I hope we can do at least is conclude our preliminary discussions on D4 which has to do with malicious conduct. And then spend some time talking about the – how we're going to approach the face-to-face meeting in London.

I see Marika's got the language on the screen here, you know, what are the forms of malicious conduct that would be covered by the – scroll over – public point of contact. And I guess, you know, some of the issues here are still just what does it mean would be covered and what are the forms if – Kathy. Yes, actually since there is – they're kind of cross – some cross connections. Yeah, when – that's fine too. Can we take a look at D2, Marika?

Marika Konings: This is Marika. You need to give me one second but I actually need to upload…

((Crosstalk))

Don Blumenthal: Sure.

Marika Konings: …the updated version so maybe you can start talking and then in the meantime I'll get that…

((Crosstalk))

Don Blumenthal: Yeah. Well I guess the question for – I'm sorry, you kind of fuzzed out there, I didn't hear you were still talking. I didn't fuzz out, the WiFi connection did,

sorry. Well, Kathy, let me start, do you have any concerns about the preliminary conclusion for D2?

Kathy Kleiman: Don, can you hear me now?

Don Blumenthal: Kathy.

Kathy Kleiman: Can you hear me now?

Don Blumenthal: Yeah.

Kathy Kleiman: Okay great. First, thanks for going back to this. I appreciate it. Let me mute my computer. Yeah, if the background information, not the preliminary conclusions so much that I wanted to see if we might be able to round out a little bit. On both Questions 2 and 3, it opens – the background information opens with a link to that Whois Privacy and Proxy Services Abuse Study.

And at least one I link to it into the call to the study, not the study itself. So I've offered the revised link to go to the study itself. You know, there's a cover page with the summary and then you can get to the PDF of the full – of the full study. So I recommend that we change that link.

And then in this Privacy and Proxy Services Abuse Study, the really surprising thing is not that people use proxy privacy – to me it wasn't that people use proxy privacy names to some extent for malicious activity. I think we all knew that was going to be a finding.

What the real kind of surprise of the study was that there are a number of companies – legitimate companies that use proxy privacy services at a high rate, not for malicious activity, for completely illegal activity; at least according to the person who did the study.

So I thought that briefly we might share that as well including, you know, the finding that banks, who had not maliciously registered domain names, use proxy privacy services at a much higher rate than the average.

And so I've offered just a few little edits, not taking anything out but just adding a little bit in that kind of, you know, rounds out a little bit more what came out of this very interesting study on abuse and recommend it for both Questions 2 and 3 because it's the same opening in both. Thank you.

Don Blumenthal: Okay, appreciate that. Somebody isn't on mute, if you could please. There is an echo and some background noise here. Yeah, as Steve suggested quite don't we work on edits in the – on the list. If you could send something we'll work it or we'll…

Kathy Kleiman: Don, I did send something to the list.

((Crosstalk))

Kathy Kleiman: I apologize I sent it late.

Don Blumenthal: Okay. Well particularly since it's background information and not to the conclusion itself let's see if we can work it in and focus on the substance of – well unless there are other issues about D2 and 3, focus on the substance of D4. But appreciate it. I think it's been on the record for a while that commercial entities use proxy and privacy for other than conducting business as such but it's – yeah, if we should beef that up let's take a look.

Anybody else have any points to talk about with D3 – 2 or 3 or should we just move on to 4?

Kathy Kleiman: Move on to 4.

Don Blumenthal: Okay, sorry about the scramble there, Marika. Could we go back to D4? Okay, let me open the floor. There's a lot of issues here. Kind of a subsumed in issues of what, the extent to which privacy proxy will have to act, but will require it to act, I guess I should be saying.

If there are forms of malicious conduct that would be covered, is that suggesting that there's some type of forms that would be covered some other way? Holly?

Holly Raiche: Thank you. It's Holly for the record. I'm a little bit surprised by this question because I'm not sure that we actually know all the types of malicious conduct. And if we do, does that mean that we're going to know all types of malicious conduct in the future?

I'm reluctant to have any kind of list simply to say malicious or potentially illegal, because first of all it's going to vary from jurisdiction to jurisdiction what actually amounts to illegal. It's also presupposes we know all types of malicious conduct, which I suspect we don't.

So I'm just interested that we think we can come up with a list. I think I'd be more comfortable if we had terms in there that these malicious or legal or something and then let the law enforcement people – either that or we simply asked law enforcement people for a list and for examples. I would be reluctant to have any kind of closed list on malicious conduct that didn't allow for the fact that there are always going to be new and different ways to be malicious. Thanks.

Don Blumenthal: I'm sure that our new law-enforcement member would agree we with that – would agree with that statement. Okay I had a thought there but let's go to Steve.

Steve Metalitz: Yeah, this is Steve. I agree with Holly, we don't want to have a closed list. But I think it's helpful to have an indicative list. And there are precedents for it as

set out in the discussion column. But I agree, we don't want a closed list because there will be new forms of malicious behavior that we haven't anticipated.

I think the reason to have an indicative list is so that you don't have the argument, "Well that's not covered," you know, for some of the things that are on there. So I think that's probably the best way to proceed.

And I'm not sure that this group has to come up with, you know, with a word for word statement of what that would be. I think to some extent that's an implementation issue. But I think if we give an indicative list that's somewhat open-ended I think it will help to clarify what types of reports need to be dealt with, need to be responded to. Thanks.

Don Blumenthal: Thanks. Kathy.

Kathy Kleiman: Thanks, Don. I was sorry to miss the meeting last week but here's my question, I see long lists – I see a long list of prohibition, you know, long lists coming out of basically the new gTLD discussion, along with some prohibitions against malware and botnets and phishing, trademark infringement, copyright infringement.

Was there any discussion last week about the difference between allegation and almost like an affirmation or proof? So someone alleges something illegal versus someone who has proven something illegal.

And so when I look at the list, you know, be provided in the Beijing communiqué, and I think about implementation at the registrar level or at actually, you know, the proxy privacy service provider level, I'm wondering, you know, malware, spam, some of these things, you know, we have pretty good tools for proving independently whereas other things like trademark infringement or defamation are a little harder to prove without more than independent judiciary or judge.

So I was wondering if there was a discussion last week about that and what people are thinking on that.

Don Blumenthal: I think there's been more than one discussion where we've talked about the issue of what registrars or potentially privacy proxy providers would act upon whether it would be law enforcement or some other kind of submission. I don't know how you would differentiate proof or allegation even in the context of court order. That's not necessarily proof.

But let me ask, to what extent would your question be – come under the heading of would be covered so that we could bring that discussion into D4? What does that phrase mean?

Kathy Kleiman: Well I think – I haven't quite gotten to the standardized forms yet and what those standardized forms are or even why we need them. But certainly if there is some kind of standardization of form there should be a discussion on this issue; what kind of evidence is being presented.

If you're going to reveal someone's personal data it should be on more than just a mere accusation. And so again exploring some of the evidentiary issues and where we would put it.

But more – again because I missed, you know, a number of us missed the discussion last week, what is the threshold – what is malicious conduct? Is it an allegation? Is it an accusation? Or should the accuser be providing – should the person filing the complaint be providing some form of evidence? And is this the proper place to be raising that issue?

Don Blumenthal: Well, we did talk about the idea of forms and the best practices for submitting abuse complaints but I really think that's – in the discussion we had it wasn't, you know, I don't think it was suggested that would be part of our work. Let me move on to Holly.

Holly Raiche: Yeah, thank you. Holly for the transcript record. Kathy, I think we're mixing up two things. One is the extent to which something has to be proven. And I would have reservations about proven in the sense that obviously some things have to go before a court to be proven.

I think what we're probably thinking about is what would be the standard required to get something like a warrant or its equivalent. But I think that's a separate from malicious.

And what I was thinking about in malicious is there may be things that may not necessarily be illegal because, for example, in some countries forms of spam, things like that, are not illegal but they're nevertheless things that we don't want to happen.

So we have to think through – and I think that's why Steve's idea of a list, what do we want to put on that list and the extent to which we put things that while may not be technically illegal in most countries, or many countries, may nevertheless be things we don't want to encourage. Thanks.

Don Blumenthal: Tim.

Tim Ruiz: Yeah, I guess – I don't know maybe this is what staff is asking too, and maybe we haven't gotten there yet. But my question would be, you know, have we discussed – I don't think we've discussed necessarily what the provider has to do when they receive a notice of malicious conduct, you know, those things that we've listed; just that these are the things that they may have to take some action in regards to but we haven't detailed yet completely what that action is.

So part of that might be, at some point, you know, they do some – they investigate further on their own and maybe, you know, unless there's a court order or something that requires them to do something they may have some

leeway into how far they go or exactly what they need to do and maybe in other cases it might be prescribed, you know, with notices or whatever.

But at any rate that what we're really talking about here is what are the things upon which they have to take some action, but we haven't talked about what that action is. Is that where we're at or did I misunderstand that?

Don Blumenthal: Well I think any action they would take is ultimately going to be covered when we talk about reveal. We can – and Steve suggested this – suggested that a lot of what we're talking about here will be covered when we talk about reveal later on. Steve suggested that in the chat. To be honest I'm – this question confuses me a little. And I'm trying to keep up with the chat but I can't so never mind.

Let me toss in, do we need a list of specific conducts given the changing nature or would some kind of cover phrases like security – affecting security and stability of the Internet – be acceptable as either a catch – as either an overall phrase or something that can be added to a short list. I don't know if it would be – it would make sense to make it too long.

Holly.

Holly Raiche: Just a thought, what I was saying in the chat I think we've got two types of response. We've got a 24/7 abuse point of conduct for law enforcement agencies, and we'll leave that definition alone for a while. But that's for the most serious type of, I would imagine, criminal behavior that really would threaten the stability and security of the Internet and criminal activity.

There are, I think, other forms of behavior that might be, say, IP infringement, other malicious activity that are not quite as serious and that would probably require a less instantaneous response but would nevertheless warrant a response. So I think there are kind of two parts to that – to the question about to what do we respond and how quickly. Thanks.

Don Blumenthal: Okay, appreciate it. And responding to something Steve – refining Steve's response as I said toward the end of my thought it could be a catch phrase at the end of a list to try to cover things that we can't anticipate. So where are we here that we should be putting together some kind of a list as something indicative of the types of behavior that would – could be brought to the point of contact. Marika.

Marika Konings: Yeah, this is Marika. Just looking a the notes from last week, I think two examples of language were called out which indeed I think give this kind of indicative list and also this kind of, you know, open ended there may be other practices that are not specifically called out and may also fall under this category.

So I guess the question is partly to the group is there a preference over one or the other or is there agreement that indeed any kind of, you know, reporting should be along the lines of the language that is captured in those two examples? Or is there indeed alternative wording that people think should be considered or referenced here in relation to the preliminary recommendation on this topic?

Don Blumenthal: Okay, thanks. Go back and take a look at that. Excuse me. Steve.

Steve Metalitz: Yeah, this is Steve. Personally I'm happy leaving that as to implementation drawing from those two statements and as long as it's an indicative list with flexibility open ended at the end I'm comfortable with it, thanks.

Don Blumenthal: Yes, the registrars punted this to us so we'll punt part of it to the staff. Good. No but I think you're right that a lot of these are going to be details that'll have to be worked out after we come up with some guidelines. Is the would be covered really an issue or is this just saying what forms should – of conduct should be referred to the POC? Presumably which would lead to our – and we - presume we pick up the details when we do get to reveal and relay.

Kathy.

Kathy Kleiman: Hi, let me ask another question about the discussion last week. Thanks, Don. Was there any discussion about the alleged – the conduct itself, the conduct being alleged, and the link between that and the person who is seeking the information?

So, and let me ask, you know, people on the call who run privacy proxy services: is there something in the inquiry that comes to you? Do you want to know anything about the connection between the person making the allegation, is that person seeking the information, and the allegation that they're making?

So I can alleged somebody is involved with defamation but it has nothing to do with me but yet I'm still seeking that information, you know, I'd still like to know, you know, who's underneath that. I'd love to know, you know, who's behind this certain types of wiki leaks for example or certain types of other leaked material but I have no kind of legal standing in a technical sense to get that information.

Do we want some information here for that contact to know who it is that's making the inquiry?

Don Blumenthal: I've got a thought there, but does anybody else want to jump in? Steve did in chat: Is that really relevant to the forms – to the types of conduct as opposed to what we'll talk about under reveal when it's the types of information or the appropriate complainants that would lead to a reveal or relay? Kathy.

Kathy Kleiman: Yeah, trying to – I'm not sure where the information would go because by the time we get to reveal we're already talking about the process of revealing whereas this is – seems like a question the process of reporting and we're

already talking about recommendations and preliminary conclusion of standardizing reporting forms.

And if we are taking this question, D, Question 4 I think, to standardizing some kind of reporting forms – and I don't know how we jump there from a list of potentially malicious activity, then isn't it important to include in that form who it is that's asking the question and to what extent they may or may not be entitled to the information that they're asking for or have a link to that – a direct link – to the need for that information.

I think by the time we get to reveal we are already talking about the process of revealing. This again is the process of reporting the information that then goes to that designated point of contact in the proxy privacy provider.

Don Blumenthal: Okay, Tim.

Kathy Kleiman: So I think the time may be now.

Tim Ruiz: Yeah, I actually had the same thought as far as the form goes. So if we're – I mean, as long as we're not going to say well we've closed off the discussion on this standardized form, if we can leave that open as we talk about these other things that we've got coming up yet then that's great so that we can say well, you know, this is another recommendation that we might include in our – what we say about this standardized form so that implementation can get all that information together.

So I just don't want these things to get lost. We just say well there should be a standardized form then we leave and go because along the way we might identify things that need to be on that standardized form and those should be included in our recommendation. Thanks.

Don Blumenthal: Fair enough. Steve.

Steve Metalitz: Yeah, this is Steve. I think I would agree with Tim that if we are – I mean, again I'm not – standardized forms is not directly responsive to the question here. I think it would be a great idea to have standardized forms but, you know, I don't know that that's a requirement and, you know, happy to – if we discuss that further we could talk about what would be in those forms.

But I think this is, I mean, who is doing the reporting is quite relevant to reveal because we feel, one flavor of it is you tell the reporter, you don't tell anybody else who the actual registrant is. And so for that you need to know who the reporter is and what is the basis for the report.

So I think it's quite relevant there. I don't think it's as relevant – and certainly not directly relevant to the question of what type of conduct would be covered. Thanks.

Don Blumenthal: Appreciate it. Anybody else? Okay just it's still within our ability to take a look at this prelim conclusion and decide if it needs to be revised in and of itself and just take the reporting form and the other pieces out up here while we keep the issue in mind for as we go along, you know, just make a note of some sort in the template along the lines of well, Legal, what's holding and what's dictum? I think a fair number of folks on the call will have heard those terms before.

But if there's nothing else let's just kind of compare this week's discussion to last week's discussion and go ahead and we'll take a look at the wording in the preliminary conclusion and see what's most – see what's the best wording is to go forward with.

Any other thoughts before we move on to just talking about the London meeting? Okay, Marika, could you bring up – there you go. Mary send out this document I think yesterday as kind of a working document for us to use in London those of us who are there or working group members that are

going to be participating by phone so that we've got a good solid document to work from during the session itself. Excuse me.

You know, I think what we're thinking about is well the usual roundtable introductions and then discussing these – presenting these findings to the audience. I think that C is going to generate a lot of discussion particularly of some things I've been told off-line about who may show up to talk are accurate. I think she's going to generate a lot of discussion so we've put aside a good chunk of time before that specifically.

And then we want to have time just for audience questions in general. That's the overall look at what we're thinking about. The important thing I think in these documents is for everybody to take a look at them and make sure you are comfortable with the kind of abbreviated form compared to our overall templates.

And take a look at our questions for the community. We won't necessarily ask all of them; there will be time in an hour and a half to cover everything. But have these ready, if specific questions about provisions come up or if we need to throw questions out to fill time which I hope isn't the question.

Anybody who's – and then the other thing kind of hanging in the background here is EWG report and the proxy privacy recommendations. I think our preliminary thoughts is that we'll mentioned the report but not necessarily devote any time to it unless we are asked.

I mean, after all the EWG will be meeting for two hours the for we tee up so I'm not sure it's necessary for us to really take it upon ourselves to go into detail on those bases again unless it comes up and we'll have materials ready if we need to.

If anybody has taken a look at what Mary sent out I'd appreciate your thoughts as to the – again, what's in these abbreviated – while the

conclusions aren't but just the abbreviated materials and also the questions that we plan to ask if it comes up, are they good? Do you have any additions?

And I should add that by definition we'll be (unintelligible) in managing the meeting in London, kind of have an overall outline but certainly let it go where the participants direct us to some extent because we talk all the time, they're the ones that we really need to hear from when they have the opportunity.

Kathy. Kathy?

Kathy Kleiman: Oh hi, Don. I just wanted to share that I think, you know, there may be specific edits coming. I'm sure people are still reviewing it. But I think this is a nice presentation. These community questions I think it's presented in a way as opposed to kind of our working worksheets that I think would really frankly confuse people; they're useful for our purposes.

This is really a clear accessible way to present it. And I was going to suggest that whatever the final version is maybe we could have some hard copies by the door that people could take a look at as well. But thank you to the people who worked on this because it's much clearer then I've seen a lot of working group (unintelligible) really be able to use this so thank you.

Don Blumenthal: I appreciate that. Appreciate your thoughts that we're at least heading in the right direction and the idea of having handouts and I'll have to leave that to Marika, Mary, whoever is going to be – whoever the appropriate people are to see if that's possible and arrange to get it done.

But these are too detailed to put up on the screen so I think you're right (unintelligible) question to Marika I guess as we're talking if we could have them – have this document put on the link to our meeting on the ICANN Website.

Marika.

Marika Konings: Yeah, this is Marika. Yes, we can definitely have it posted on the wiki page that linked to the meeting form. And we can also have a couple of copies in the room. And I think we probably should be able as well to have maybe a presentation (unintelligible) so we can project the document and, you know, certain people want to talk about specific question or a topic we could scroll to that, the relevant section, so people in the room can look at it at the same time and obviously also have it up in Adobe Connect so people can scroll through there and look at it there as well.

But of course indeed if we do want to have it posted, it may be good that we set a cutoff date by which edits would need to be received so that we don't have, you know, different versions in circulation or posted. So I don't know if that's possible that we give people a deadline by which they send edits than otherwise this will be the version that we'll put up and distribute.

Tim Ruiz: Might be on mute there, Don.

Don Blumenthal: I'm sorry, I can take myself off mute. Well, you know, will you tell us when you need it by and just set the deadline. Maybe we can talk about this after the call but realistically I can't see that it would be more than a day or so out.

Marika Konings: Right, so this is Marika. As I think, you know, four example I'm starting traveling on Friday as it's fortunately very nearby for me so ideally, you know, close of business on Thursday so first thing on Friday we can just upload it if that's reasonable and feasible, although I presume a lot of you are – will actually start traveling before that so we may need to get it in early.

Don Blumenthal: Okay we'll send this out to the list but why don't we say close of business – have to work on which time zone we're talking about tomorrow but close of business tomorrow so we all had a chance to review a final version before it goes out – we all meaning the chair's group, whatever we want to call

ourselves. I refuse to use the word leadership team; I'm sick of hearing it. Any other thoughts on London?

Could I ask just out of curiosity if people who are using Adobe could put your hands up just to get an idea of who's going to be at that face to face? Good comment nice turnout although there are some folks I was hoping to put faces to names. Oh, more folks are coming up, okay.

And if you'll be there and won't be able to attend the face to face see me or – not in general if you see other members of the committee. Flag yourselves; David did that in Singapore.

So I don't want to – oh Holly. Wait a minute.

((Crosstalk))

Don Blumenthal: Yeah, as soon as I said it I realized, wait a minute, hands are up. But everybody who's got your hand up not to talk take your hand down? Okay. I should have suggested some other symbol, it would have made life easier. Stephanie. Stephanie is your hand – Steph, are you on mute? We can't hear you if you're trying to talk here. Okay, Stephanie, if you can hear me if you could put something in chat.

It's an interesting discussion on spam in the margins here. Something to take up another time. Yeah, I don't want to keep people on the phone if we've really covered everything for today. D4 I think was a little confusing but there wasn't much to it. You know, it's fairly short, there's not a lot of issues to discuss although the issues have some challenges to them. We usually have more than one question to address in a call.

Okay last call for comments or thoughts and we can wrap early for a change? All right, thanks for your – thanks for your time. Hope to see or hear people in

– during the London session. And we will convene again – what is it, July 8 – we won't meet the week after ICANN.

Holly Raiche: Excellent. Thank you.

Don Blumenthal: And keep your thoughts coming on the list.

Holly Raiche: Thank you.

Don Blumenthal: Appreciate it. Why don't we stop the recording and get back to the world?

Tim Ruiz: Thanks, Don.

END