ICANN Transcription
Privacy and Proxy Services Accreditation Issues PDP WG
Tuesday 16 September 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 16 September 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-20140916-en.mp3
On page:
http://gnso.icann.org/calendar/#sep

Attendees:
Steve Metalitz - IPC
Graeme Bunton – RrSG
Griffin Barnett – IPC
Frank Michlick – Individual
Don Blumenthal – RySG
David Heasley-IPC
Jim Bikoff-IPC
Chris Pelling – RrSG
Kathy Kleiman – NCSG
Justin Macy - BC
Susan Kawaguchi – BC
Kristina Rosette – IPC
Darcy Southwell – RrSG
Paul McGrady – IPC
Phil Marano – IPC
Sarah Wyld – RrSG
Victoria Scheckler - IPC
Michele Neylon – RrSG
Lindsay Hamilton-Reid – RrSG
James Bladel – RrSG
Val Sherman – IPC
Luc Seufer – RrSG
David Hughes - IPC
Alex Deacon – IPC
Carlton Samuels – At-Large
Todd Williams – IPC

Phil Corwin – BC
Michael Palage - RySG
Sean McInerney – no SOI

Apologies :
Holly Raiche – ALAC
Christian Dawson – ISPCP
Volker Greimann - RrSG

ICANN staff:
Mary Wong
Marika Konings
Amy Bivins
Danielle Andela
Nathalie Peregrine

Coordinator: Recording has now started. Please proceed.

Nathalie Peregrine: Thank you very much (Damon). God morning, good afternoon, good evening everybody and welcome to the PPSAI call on the 16th of September 2014. On the call today we have Graeme Bunton, Val Sherman, Don Blumenthal, Steve Metalitz, Justin Macy, Sarah Wyld, James Bladel, Phil Corwin, Todd Williams, Griffin Barnett, Michele Neylon, Alex Deacon, David Heasley, (Doug Charvo), (Ben Weikauf), Michele - sorry, Michael Palage, Lindsay Hamilton-Reid, Chris Pelling and Phil Marano.

We received apologies from Holly Raiche and Christian Dawson. From staff we have Mary Wong, Marika Konings, Amy Bivins and myself Nathalie Peregrine. I'd like to remind you all to please state your names before speaking for transcription purposes. Thank you very much and over to you Don.

Don Blumenthal: Okay. I appreciate it. As usual just to remind new people to post updates to your SOIs if there have been any since the last time you heard the request. Try to remember each week.

We had a really interesting presentation from staff last week. Mike Zupke and Amy Bivins talking about where - what staff has been looking at in terms of implementation of any accreditation program and the avenues that might be useful.

And there was some discussion right after but then it - haven't seen much in - since I guess last Wednesday. Just want to take a few minutes to see if anybody had any follow up comments on thoughts on what we heard; directions that we might want to start thinking about in terms of how we look at implementation when we're doing the face-to-face.

We certainly are going to try to schedule time with the Registrar Services Team to explore what we're doing and what they're doing; some valuable face-to-face with them and some with us.

But we just throw this out for any follow up thoughts in general on the issue of registrar responsibilities enforcement and whatever else might be appropriate. James.

James Bladel: Hi Don. James speaking for the transcript. So maybe this came across in my comments last week to staff and I don't mean to pick on them too harshly. But I don't - I feel like this is a dead end - what they're proposing as far as piggybacking any kind of accreditation requirements or obligations on the registrar contract.

You know, I believe that there's an opportunity here to deal with this narrowly and specifically. And, you know, there is certainly the possibility that independent service providers will spring up that are not affiliated with registrars.

That registries, especially new TLDs might, you know, get involved in this service area here and that would, you know, change things. I'm not sure that it's implementable or workable. Certainly it's an additional burden to

registrars. And I believe just procedurally that this was kind of the direction that was coming out of the Whois Review Team.

So I don't know that it's appropriate to have - to change direction so abruptly simple because, you know - well, recognizing that it's going to be a lot of work for staff. But not really I think onboard with the idea that we just fold this into our insisting accreditation framework.

So that's all. I mean I'm sure that that was pretty apparent from my comments last week. I just wanted to get that on the record to your response to your question. Thanks.

Don Blumenthal: Okay. I appreciate it. I think that definitely was clear last week in the follow up. I wasn't necessarily looking to aim at that issue. But it was a natural one to latch on to since it is the one that generated the most discussion on the call and shortly afterwards. Any other immediate thoughts or that we should explore concerning that or move on to more substance from -- (a second) -- or move back into the substance of what's come on the list this week?

And if folks could go on mute I'd appreciate it. Okay. We had - after that discussion we had talked about trying to get some examples of privacy proxy service policies. And James forwarded what -- (we go) -- domains by proxy, uses in the trademark and copyright area.

Graeme follow up with an email I guess yesterday or this morning. I'm traveling again so timeframes are a little loose for me these days. Graeme followed up with some materials concerning what Tucows does.

Granted these are in a focused area of the broad spectrum that we might be addressing but I think they give some good outlines that - of what's being done and how it could be extended. It gives us some ideas on how it could be extended.

To be honest, I was a little - particularly given the way discussions have been going concerning automation, I was a little - I was intrigued by the level of examination seems to go into these although granted this is - I can say (radio). Can't do that. Publication as opposed to disclosure. No, that's the same thing. I told you I'm traveling. You know what I mean. Yes.

So again, let me throw it open to see if this has produced any thoughts on - I know what we've been talking about concerning what the rules should be and what the processes should be in general for - I'm sorry. I thought I heard a voice there.

Hello. Just saw James' text. Okay. Go ahead. All right. Yes. (Can't lose) me that easy James. Anyway, back to using what Graeme and James provided as a launching point for our broader discussion of examining of how we would suggest policies for disclosure publication. Steve.

Steve Metalitz: Yes. Thank you. This is Steve. I just - I'll just kick things off by saying I think it is very helpful to have this material from James. It gives kind of some concrete - it puts some concrete criteria in place really going back to the question I think Kathy Kleinman asked a couple weeks ago, which is what do you have to do beyond a mere allegation to try to get a disclosure.

So this spells it out for two categories - two or three categories of complaints. Obviously not for all. What it - I guess two things. First, it would be great to see - to get the views of other providers on whether these are the right criteria in these cases.

I guess - I take it from Graeme that for Tucows they're not and even if you add all this information, if it involves content on a Web site, generally they will not investigate. I take that from his comments that he posted last night or yesterday. But I'd be interested to hear from other providers on this. That's Number 1.

Number 2 of course this comes up and the punch line here on this document that's on the screen is we'll initiate a claim investigation. But then the next question is well under what circumstances will you actually disclose, you know, under what circumstances - given all that you've met these threshold criteria where there's a complaint attached, under what circumstances will the provider disclose?

So any additional guidance that James could provide would be great but it would also be good to hear from other providers as to whether they follow these same criteria. Thanks.

Don Blumenthal: Okay. Well let's start with Graeme since he jumped in first.

Graeme Bunton: Hi there. Graeme for the transcript. Just clarify briefly Steve, we investigate sort of every complaint but, you know, Tucows doesn't do any hosting whatsoever. And if it's a content issue and that's outside our realm, we will encourage people to contact the registrant or the Web master and/or ultimately the host to deal with the content issue. But we do look at every single complaint that comes in. Thanks.

Steve Metalitz: Don, can I just (unintelligible)?

Don Blumenthal: James.

James Bladel: Okay. Go ahead.

Don Blumenthal: Oh sure. Go ahead. Sure.

Steve Metalitz: I just (unintelligible)...

James Bladel: I think Steve wanted to follow up.

Steve Metalitz: Yes. It's not a question. And I - it's - you're right. It's not a question. Just an investigation. But we're focused here on disclosure. So in terms of what Graeme put forward, it doesn't really say under what circumstances they will disclose the contact information for their customer. So maybe it would be - just be helpful to have that as well as from other providers. Thank you.

Don Blumenthal: Yes. Sorry James. Steve said he wanted to clarify. I thought it was appropriate.

James Bladel: Yes. That's fine. It's actually helpful because I was going to follow up on some of those points as well. So this is James speaking for the transcript. And I just - I want to point out first of all I'm probably not as familiar with the standards that are applied during our investigation as I should be. So rather than confuse the issue, I'll probably just, you know, take that question back and see if I can share any other information on that.

I wanted to share this because I know it's public and it's out there and it's something that we need - we use to help educate our customers. So I know it's fair game.

I just wanted to mention something that's kind of a philosophical issue really, which is that as a - we are both a large registrar and a large hosting provider. And often when we encounter, you know, people doing bad things, you know, on our networks, we have more discretion under our hosting agreement, which is not covered by an ICANN obligation than we do as a registrar.

So we always try to act, you know, I think most expediently against infringing content as a host or at least let's say it's easier for us to do that where we feel that where our hands are tied if we don't - as a registrar, you know, if we don't feel that the situation exactly fits something that falls under our ICANN remit, we really don't know that we can take a lot of particular actions without, you know, perhaps exposing ourselves to some liability.

So, you know, the general philosophy is if we can take action as a host, we prefer to go that way because we can be faster and we have more latitude. And I'm saying this because, you know, for this group in particular as we're developing, you know, standards and requirements and I think that, you know, the temptation is going to be there to narrowly and explicitly define and prescriptively define a step-by-step process by which an investigation should occur.

And I would just caution perhaps against that. Because I think that the unintended consequence is that it will perhaps, you know, like we've seen with the registrar versus hosting issue, it could slow down, complicate and ultimately limit the effectiveness that a privacy service (can take) in these situations.

So that's just something I wanted to put in, you know, on the pile for discussion because it is something that comes up fairly frequently in dealing with abuse. Our networks, you know, as a host we feel like we almost can do whatever we want with our customers. They sign the agreement. They're doing something that is even questionable, we'll take action. But as a registrar we feel like we're handcuffed.

And I would want to be sure that anything we design for a privacy service doesn't involve, you know, the handcuffs that we see for registrars. Thanks.

Don Blumenthal: Appreciate it. As long as I've got you, can you see the question that Kathy raised about the ability to respond?

James Bladel: I do not know that answer.

Don Blumenthal: All right.

James Bladel: I apologize Kathy. I will get that to you. I will say that most of the actions taken by our privacy service are publication and not disclosure. Though this

would be a cancellation of the privacy service, which is the practical effects of (posing) the customer contact data in Whois.

I will get back to you on that. And I well also if there are any scenarios where we would disclose to a complainant without publishing in Whois. I think I'll take those two questions. Thanks.

Don Blumenthal: Appreciate that. Michele.

Michele Neylon: Yes. Michele for the record. No, just in support of James. I mean some of the - you know, for us we are primarily a hosting provider. We're also a domain registrar. We provide transit - IP transit bandwidth to third parties. And so, you know, it does get a little bit confusing.

And, you know, there's an awful tendency within the ICANN world for people to try to kind of pigeonhole, you know, registrars are in this little - neat little box over here. Registries are a neat little box over there. There's proxy privacy providers in another neat little box with a nice little bow tie around it.

And the reality is there's lots of gray areas. There's lots of overlap. So, you know, you know, basically a lot of what James is saying we'd be in a similar situation when it comes to general kind of abuse complaints, takedowns and everything else. Thanks.

Don Blumenthal: I was just having visions of boxing matches at ICANN, which might not be a bad idea now that I think of it. Kathy.

Kathy: Hi. Thanks. Hello everybody. I wanted to ask a follow up question to James and the proxy privacy providers. And I can totally understand that everybody doesn't have the answer now because I'm sure this is kind of a, you know, a discrete part of the company that works on these things.

The follow up question is especially prior to publication, so especially prior to the cancellation of the service and the disclosure of all the information, the publication of all the information to the whole world, is there notice to the customer?

That's a little - that's different than asking if the customer has the right of response prior to a decision. But after that decision is made, is there some notice? I would certainly want to know before my home address was published to the world so that frankly I have the option of taking down the domain name instead.

But, you know, you can see situations that are, you know, where someone uses the trademark for a critique site of a kind of freedom of expression site, there's a trademark infringement claim, the proxy privacy service provider makes the call, which is fair, because in their discretion makes the call, decides it's trademark infringement and not freedom of expression decides to disclose, you'd still, you know, publish.

You know, does the person - does the customer know ahead of time? And I'd like to add to the notes if I could that that's certainly a case where we would want to let the customer know if their information - I can understand kind of in the one-to-one disclosure. That's a different discussion. So law enforcement comes and wants the information. That's one kind of reveal.

But this publication to the world I think raises a whole different set of issues. So I'd like to propose that the group could strongly consider notifying the customer prior to that publication with a publication date. Thanks.

Don Blumenthal: Appreciate that. And I just want to (grow) caution. I think the stipulations of publication with or without notice certainly in some cases I think will involve a freedom of expression situation but in others may - they may not. And I think we'll want to do some differentiation when the time comes to zero in on the issues. James.

James Bladel: Hi Don. James speaking for the transcript. And to respond to Kathy, I actually heard two questions. One is is the customer notified and two, do they have - do they have any options to respond or take any other actions prior to publication?

So I will get those two questions answered. I apologize. I don't have them - I don't have them handy or at least not in the position where I can speak confidently that I'm not wrong, so. Thanks.

Don Blumenthal: Thanks. Graeme.

Graeme Bunton: I can respond to Kathy from a Tucows context. Sorry, this is Graeme for the transcript. We do notify a customer if we're going to remove the privacy and proxy service from their domain.

At the moment we don't have any codified sort of other options like allowing them to delete the registration or something like that. But that's something we've been discussing internally since we started working on this working group because it's an interesting option. Thanks.

Sorry. This is Graeme again. The customer can respond. And we encourage them to do so. A lot of what we're trying to do and what I was trying to describe there is that we're generally trying to encourage a dialog to occur.

Don Blumenthal: Okay. Appreciate the excellent input and covering the (dead to my) - my window minimized so it couldn't find the button to take myself off mute. Michele.

Michele Neylon: Yes. Thanks Don. Just - I mean this is more to do with kind of general how we would handle any kind of takedown or issue with - involving a domain or a (size) with a proxy - two different things.

Speaking to Kathy's query. From our perspective what, you know, if this action is taken against anything on our side, we would inform the client. The fact - but that would be probably at the same time as the action is taken.

So for example, if you're spewing malware across the entire bloody Internet and we happen to have the ability to stop you from doing that, then we're obviously going to stop you from doing that and tell you however at the same time. But that's an internal thing to us.

I think part of the stuff around this is really - it should be up to the provider to decide how they want to deal with a lot of this. I mean I'd be very wary of ending up in a situation where as, you know, we're being kind of tethered to some contractual obligation because that can cut both ways.

That can end up - I think James touched on it previously. That can end up where it's slowing certain things down or having other adverse effects, you know, be that, you know, positive or negative depending on your perspective.

But ultimately you don't want to end up in a situation where you've ended up creating more problems through contracts than you've actually solved. Thanks.

Don Blumenthal: Thanks Michele. Certainly a topic we're going to have to focus on fairly closely before we publish or are in the process of writing our draft report. There's a lot of variations, mutations, whichever. Is there anything else we want to - excuse me. Any other comments based on what the discussion or what (games) or (plan) (unintelligible) this week? Steve.

Steve Metalitz: Yes. This is Steve. Based on what I think I saw in the chat although it was flying by pretty fast so I may have missed it. But I saw several providers saying we do - we agree with Tucows or with what Graeme posted.

And as I said, that - what - that doesn't - it doesn't really get to the question - what Graeme posted doesn't get to the question of when Tucows service will disclose to a complainant what, you know, the contact details.

What James posted says well here's the stuff a complainant has to come forward with if you want to get anywhere on this - in this process, you know, give us these - this information and then we'll investigate. And he's going to come back to us about in what circumstances they would use disclosure rather than publication.

But I still would like to hear from other providers as to whether - what their standards are for disclosure. So I'd just encourage the providers to step forward with that either now or if they need to check with others in their organization; I think it would just be useful to have that as we try to come up with a standard in this area because it's always helpful to know what's the current landscape. Thanks.

Don Blumenthal: Agreed. And thanks Steve. I'm not even sure - and certainly there are certain folks active - more active than others on the list. I'm not quite sure who all does offer privacy proxy services who's involved in the workgroup. But certainly if others besides the usual suspects are, yes, it'd definitely be helpful to hear from a broader group.

All right. If that's the extent of this conversation - it's been a good one. I think we did a good job of exploring with the examples gave us and what we still need to find out before moving forward on publishing disclosure. Can you get the next document? (Unintelligible). That's it. Yes. Thanks.

Going off for just a - again. Okay. This had gone out a few weeks ago - couple weeks ago, whatever it is. And it - I think it's just - well we bounced around a bit. I'm just ready - yes, I agree. (Kristina) gave an additional item to be - would be helpful just to give us an idea of the sense of the industry. Want to be - we want to be dragged back to reality every once in a while.

Any event, to just go down this methodically. We've done a lot of bouncing around, which is good I think to - had a lot of good substantive discussion. But at some point I guess it's worthwhile to just focus so that we can make sure we cover all of the issues and move on to (D).

And to be honest, I'm hope we could get through F before we're - before ICANN. And I may be pessimistic here. Maybe that's - we'll start moving quickly. But we - this topic I think is going to be the critical one for a face-to-face. It's going to grab a lot of attention.

I know from a law enforcement we're going to be in Los Angeles. I assume it will be of interest at our regular open session. So I'm just kind of focusing on moving forward here. In any event, hang on. Okay. Bouncing on and off seem usual this week.

So let's just start with the baselines. And I'm seeing answers in the chat to so many questions posed. So appreciate the quick follow up. How are we going to tackle - or should there ever be any differences in terms of the processes if it's law enforcement - I want to say law enforcement here. I'm going to assume that we're talking about separate from court order. Court order in - assuming we're talking about competent jurisdiction as its own rules.

But will we suggest separate policies if inquires come from law enforcement or private parties? Michele.

Michele Neylon: Don, Michele. Okay law enforcement is a term we have to be very, very, very careful about because that needs to be clearly defined. It isn't as much of an issue for us as a company - as a company based in a country that has essentially only one law enforcement agency.

However, in the US where you're based there are, what, 40,000 or 50,000 law enforcement agencies? And that's a bit of a problem since law

enforcement has repeatedly shown itself to be incapable of providing registrars or registries with an actual - some way of self-certifying that they are genuinely law enforcement.

And I'm sure Kathy or somebody else is going to raise the issue of, you know, surely one should treat differently a dog catcher from an FBI agent. While I could imagine a scenario in which an FBI agent or another three-letter acronym agency that is involved in dealing with serious crime may wish to investigate stuff surrounding a domain name and may wish to get the information related to a domain name from a registrar or a privacy provider, I would have great difficulty in imagining a scenario in which a dog catcher would have the same rights, abilities or excuse.

So I think the actual terminology, "law enforcement," needs to be fleshed out a little bit because otherwise you're opening up a very, very nasty can of worms. And, Kathy, to your query, don't forget I did spend a very long time with Carlton and others discussing all of this. Thanks. Bye.

Don Blumenthal: Well as a former law enforcement person, yes, that's a question that's been floating since, you know, since these discussions have been going on: what is law enforcement, how do determine it.

The numbers in the US aren't quite that many. Roughly 20,000 agencies report - put statistics into the FBI annual crime stats. Not all agencies contribute so the numbers in the US are north of 20,000. Add to that that civil law enforcement agencies...

((Crosstalk))

Michele Neylon: Don, I mean, the thing - Don, the problem is very simple. Just come back on this, okay? If, under contract, registries, registrars or privacy providers are expected to do certain things in a particularly different way when dealing with

law enforcement that is not an issue for a lot of us in countries where we only have one or two law enforcement agencies. But...

Don Blumenthal: I realize that. What I was trying to do there is correct something you put on the record, okay?

Michele Neylon: Right, now - but the problem from our perspective is, you know, what the hell is law enforcement in terms of how are we meant to know whether or not a law enforcement agency is legitimate or not? There's other people that put up their hand, I'll leave it to them.

Don Blumenthal: Okay now I will complete my point, okay? The numbers in the US that you put on the record are not accurate, okay? I was just trying to correct that. I understood your point completely. The numbers in the US roughly are maybe 22,000-23,000. Still a ridiculous number, still a number that it's impossible to verify within the US much less outside the US but I just wanted to put that out there.

For you to understand who's legitimate in law enforcement here is going to be a mess. For us to understand who's legitimate law enforcement in a country, for example, that may have law enforcement that doesn't comply with - as a law enforcement role that may not meet US sensibilities is another issue that's going to play in here.

And I think at some point we're going to have to get to a discussion of is law enforcement definition something that this group should be focusing on or should we lay out law enforcement and turn that into an implementation issue? James.

James Bladel: Yes, so thanks, Don. James speaking for the transcript. And just wanted to point out that we wrestled with this issue for, I don't know, months during the RAA negotiations; what is law enforcement?

And there's a definition in the new RAA, it's Section 3.18.2 - sorry, dot 2, of law enforcement as, law enforcement, consumer protection, quasi-governmental, other similar authorities designated from time to time by the national or territorial government of the jurisdiction with the registrar is established. Why don't - or maintains a physical office.

Why don't we just - I mean, I don't mean to diminish what Michele is saying but I feel like we've got a serviceable definition of law enforcement in the existing contract so maybe we can just modify it to the purposes of this working group and move on from this topic. Thank you. Maybe wishful thinking on my part but just wanted to put that out there.

Don Blumenthal: No, fair enough. I think that definition is a good start. Kathy.

Kathy Kleinman: Hi, Kathy for the record. And, Michele, I appreciate your anticipating the dogcatcher question, it's always a good one. But a good starting point for us might be the one that Don mentioned and that's why I'd gotten in the queue originally; jurisdiction.

As a starting point perhaps we could have agreement about law enforcement from the jurisdiction in which the proxy privacy provider is located. That - it sounds so basic that even putting that down as a baseline might give us a starting point because of the issue that Don raised, that different law enforcement from different countries operate under different laws.

And so it sounds like everyone works within the framework of the laws within their countries. So if we create that baseline it gives us a starting point. Thanks.

Don Blumenthal: Thanks, Kathy. Yes, the law enforcement definition is going to be really difficult if it's possible at all. And again my comment about competent jurisdiction lent to the issue of court order primarily. But will we be suggesting that the rules for reveal processes using the broad term will be different if it's

a law enforcement request submitted for voluntary action as opposed to a private hardy submitting for voluntary action.

And, Carlton, let's not talk about (unintelligible), that's another ugly topic.

Yes, I've got to stop reading the chat, it's very distracting. You know, we've gone over I think in just today's call a lot of these questions as I'm reading now. I think we need to start formulating some answers to them instead of just raising questions. Sorry, I don't think I got on mute quickly enough there. Steve.

Steve Metalitz: Yes, thanks. This is Steve. I would agree with James a suggestion to use this 3.18.2 definition at least as a working definition but then it gets to the question of whether you treat these differently and I think from complaints coming from entities that aren't described in this definition.

I noticed that Domains by Proxy have a privacy policy that addresses this and really kind of deals with law enforcement and complaints about law violations coming from private parties on a similar basis. So I actually tried to post that in the chat but I think it's a little too long; there must be a character limit in the chat.

But I think that's a useful approach. And it also, by the way, gets to Kathy's earlier question about notification to the customer. So again I would support James is suggestion that we use for working purposes anyway let's use this definition.

It doesn't necessarily mean there's only going to be one; there could be a large number. It also depends on how many countries the registrar maintains a physical office, is established. But at least it kind of put a frame around what we're talking about. Thanks.

Don Blumenthal: Yes, appreciate that, Steve. I hate to go down point by point - point by point here so let me ask you, everybody has the ability to scroll - scroll the document. I think for a lot of the (unintelligible) that we've heard over some calls, we might be able to come up with a summary of what we think the group has expressed. Come up with a summary of consensus but at least different viewpoints.

But I'd like to raise the idea that we at least - if people could take a look at, say, the questions here under Sub Group 1 and contribute your thoughts at random or just anything that jumps out at you here doesn't get too wrote. Again, this is kind of a - I think possibly the most important topic we're going not deal with in terms of community interest so I want to - really want to make sure we cover everything.

Steve, is that a new or an old hand?

Steve Metalitz: That's a new hand. It's in response to your request about the sub points.

Don Blumenthal: Okay.

Steve Metalitz: Yes, I think, again, I think what James circulated goes to G. I won't say minimum standards of proof; that may not be the right phrase. But it just says here's the information you've got to include in order to try to get - in order to try to find out who has registered this domain name that you believe is being used to infringe your rights.

So, you know, I think that's very helpful and still not clear on what the other providers would say in that circumstance. But I think that's a - perhaps that's a model we can build on.

And I'd also say on 1(i), the last one down there on Page 1, that I don't think - there's a problem with that if, again, in the disclosure situation, not general

publication, and I recognize that for some providers they may use publication more than disclosure.

But in the 1:1 disclosure situation I think it makes sense to require that the information only be used to try to deal with the issue that's raised in the complaint and not for other purposes. So I don't think there would be a problem with that. Thanks.

Don Blumenthal: Appreciate that. It was - the lawyer in me is wondering how would you enforce if somebody violated that agreement but that's way beyond our scope. Any other points to raise concerning this initial section?

Steve Metalitz: Well, Don, if I could just respond to that. This is Steve again. And also to the little remarks in the chat. I'd like to ask any of these people if they've had a problem with this? Have they revealed the contact information of a customer to a requestor who showed adequate evidence for the complaint and then that information was abused?

And again, this is not a publication situation where it's, you know, where this contact information is appearing in the Whois; it's a disclose situation where only - it's only being revealed to the requestor. Has this been a problem? It would be great to know what the real world side of this is.

Don Blumenthal: Yes, back in the world again. Kathy.

Kathy Kleinman: Well I'd certainly be happy to wait if anybody wants to respond to Steve's question, that's a good question.

Don Blumenthal: James, was that on Steve's point? James?

James Bladel: Sorry, I was speaking into the mute button so you'll just have to take my word for how witty and enlightening and funny it was. But this is James speaking

for the transcript. And in response to Steve's question I will say that - and I can't go into too much detail here.

And I'm not sure it's exactly what he's looking for but there have been situations where the disclosure or reveal of underlying information has turned out later to have been perhaps the wrong decision based on the information - it was the right decision based on the information and the materials that we received at the time but later turned out to be - that we were basically we were misled or deceived and/or the information was not used for the stated purpose.

So this has happened on at least a couple of occasions. And I really just am very reluctant to say much more than that. Thanks.

Don Blumenthal: Again, the lawyer in me appreciates your reluctance. Kathy.

Kathy Kleinman: Okay I'm going to respond to two things. One, to support what Steve is saying; and then to move on to G briefly. So in terms of - I'm not sure we should be worrying about enforcement right now. We have a lot of things where we're setting out the record and notifying both sides, information and notification seems to be one of our themes across a lot of the work that we're doing here.

So setting out the baseline that the requestor agrees to use the reveal data only for the purpose for which it was requested, it seems like a very reasonable and no-cost option that we can kind of support. I don't see a downside to it.

If something happens later it may be a - something that the customer him or herself will be following up on. But setting the baseline that if you get this data know that it's private and know that you have limitations on how you can use it seems very reasonable. Again, I don't see a downside. And it could create a basis for record for following up later if there is some kind of abuse.

And in G, so to - I think we're going backwards up some of these sub points now. What are the minimum standards of proof? I haven't studied James's document closely but this concept of a good faith and a penalty of perjury that the person making the allegations, and here I'm thinking particularly of private parties, that the party making the allegations truly believes that there's some kind of a legal act as set out in the materials.

Again, enforcement, perhaps a problem; but setting it out there creates the record and I think that's really an important aspect of what we should be embracing. So thanks.

Don Blumenthal: Yes, appreciate that. I hope I didn't confuse things by tossing in the thing about enforcing because that is - yes. I'm rethinking when you just said, no that was on point to what I was saying. I apologize.

James, is that new or old?

James Bladel: Sorry, old hand.

Don Blumenthal: Okay. You're forgiven. Okay let me just then follow up on something Kathy suggested. Is perjury - penalty of perjury going to be a meaningful term universally or might we think about something just concerning future ability of a requestor to request and have somebody pay attention.

You're back, James.

James Bladel: And thanks. James speaking for the transcript. And I do - and I think I've said this before borrowing from the EWG concept, I think I do agree with the idea that, you know, someone could lose their privileges as a reporter or future complaints.

However, I would point out that if you are the one and only person - or entity that was on the receiving end of having your information incorrectly or inappropriately exposed and published then that really doesn't do you any good, you know, as a victim of that kind of abuse.

So I think it helps but it really, you know, it's kind of like, okay, you can only commit murder once and then you can never, you know, commit murder again or something like that, you know, it feels like if you were the - even if you were the lone example of someone abusing that status that it wouldn't help you much just to know that they - their future privileges had been revoked.

But I do - I don't want to throw the baby out with the bathwater, I just want to point out that it's probably not enough.

Don Blumenthal: Okay. Good point. Michele.

Michele Neylon: Michele for the record. Yes, just picking up on that point, I mean, this is something that, you know, during the EWG's work we did spend a lot of time discussing. And, yes, James is right, I mean, it's - the analogy, you know, (unintelligible) he only committed murder one time; it was only just that one time that he murdered somebody so that's okay. He won't be able to do it again. Obviously it doesn't help.

I mean, it's a good analogy. But the problem is, you know, how do you get the balance right? I mean, some of the - some of the concepts that, you know, some people have put out would be, you know, let's say if you are a reporter/requestor that you would have to - you would have to, I don't know, have a lot of skin in the game so maybe making a large deposit or something that you would lose if you abuse the data.

I mean, these kind of concepts have been put out there but they're usually rejected by some people who think oh, you know, you're making - you're

setting the barrier too high. But if you abuse that trust then, you know, is any barrier too high. And it's a problem.

And I don't know what the answer is; I honestly don't know what the answer is because, you know, the thing is that, you know, if you can - you can always look at the extreme cases. And, you know, I'm sure Kathy and others can provide very good examples of situations in which publication of data could put people's lives at risk. And I think that's something that we need to be conscious of.

But we shouldn't be driving all policy decisions on either end of the spectrum. We need to find something that is - that kind of works well for most people, most things, within the system. I think there has to be a balance there. Thanks.

Don Blumenthal: Agreed. And, yes, there's no question. There's - we're too varied, too many countries, too many situations to cover all bases, absolutely. Susan.

Susan Kawaguchi: Yes, I just want to make the point that we need to also think about balancing the penalties or the requirements of the requestor with that of the registrant or the licensee of the domain name. You can easily register a domain name and slap a proxy on it with no - very - the bar is extremely low.

And then if you do - if something is - if that domain name is used in, you know, an adverse manner, you know, and violates the terms of service of the proxy then they might lose the ability to use that proxy service. But there's very little to prevent bad - there's nothing to prevent bad behavior. But even when bad behavior is, you know, is noted on the domain name then there still there's very little recourse actually.

So I think if we're going to - I get protecting people's information but when somebody acts badly and you can prove it then I don't think the requestor

should have a lot of barriers put on them. At least let's keep that level. So, you know, this is an easy thing to do to get a proxy registration.

If you want an iron clad protection of your information then you may need to use a different process or a proxy provider that, you know, you're going to pay a proxy provider a lot more to protect your information. So it's lightweight going in so it may be lightweight to be revealed or disclosed. If it's heavyweight and lots of requirements to use the service then you have more protection on your data, in my opinion.

Don Blumenthal: Okay, Vicky, did you drop out on purpose?

Vicky Scheckler: Yes, because I think Susan covered the points that I wanted to raise.

Don Blumenthal: Okay. James.

James Bladel: Hi, Don. Well I know we're up to the end of the call so I'm just going to drop this bomb on us here. You know, but wondering if we couldn't tackle this question and all of its sub questions by establishing just, you know, without putting too much detail just saying like where do we think that the barrier to access the responsibility of use, etcetera, should be, you know, on each of these questions?

For example, like I believe that the barrier to - or the accessibility to a privacy service should be low because any additional barriers means that there's something suspicious about wanting to protect your privacy. And I think that that's not the message, you know, that should be coming out of this group.

On the other hand I believe that the barrier to accessing a complaint reporting system should be also low. That anyone who believes, you know, the member of a public that something is abusive, even if it's, you know, hey, somebody's got a Website and they're criticizing my sports team and I don't

like their sports team or something like that. You know, what the heck? You have to be open to accepting, you know, spurious complaints like that as well.

But the threshold to actually taking action on those complaints perhaps should be where the choke point is, not in closing off access to the service or closing off access to the complaint tool. So that's just maybe something that perhaps would help us navigate - this is a really tricky question and I think a lot of these different sub questions are dependent upon each other as well. So that's just one thought on how we can maybe untangle this. Thanks.

Don Blumenthal: Yes, I like your suggestion. We are at 11 o'clock so why don't we - when I say "we" the staff and our small group try to distill today's discussion and with that in mind. And then send something out and then we'll also move on to Sub Group 2 next week. Appreciate your thoughts here. And again, talk to you next week.

END