ICANN Transcription Privacy and Proxy Services Accreditation Issues PDP WG
Tuesday 25 August 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 25 August 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.

Attendees:
Graeme Bunton - RrSG
Val Sherman - IPC
Kathy Kleiman - NCSG
Stephanie Perrin - NCSG
Terri Stumme - BC
Todd Williams - IPC
Sara Bockey - RrSG
Roger Carney - RrSG
Frank Michlick - Individual
Steve Metalitz – IPC
Volker Greimann - RrSG
Sarah Wyld – RrSG
Darcy Southwell – RrSG
James Bladel - RrSG
David Hughes - IPC
Phil Corwin – BC
James Gannon - NCUC
Holly Raiche - ALAC
Paul McGrady - IPC
Dick Leaning, Individul
Susan Prosser RrSG
Susan Kawaguchi – BC
Vicky Scheckler IPC
Alex Deacon - IPC
Luc Seufer RrSG
David Cake- NCSG

Apologies :

Don Blumenthal - RySG
Michele Neylon - RrSG

ICANN staff:
Marika Konings
Mary Wong
Amy Bivins

Nathalie Peregrine

Coordinator: Recordings have started. Speakers you may begin.

Nathalie Peregrine: Thank you so much. Good morning, good evening, good afternoon, good evening everybody and welcome to the PPSAI Working Group call on the 25th of August 2015.

On the call today we have David Hughes, Phil Corwin, Graeme Bunton, Steve Metalitz, Holly Raiche, Val Sherman, Dick Leaning, Sarah Wyld, Darcy Southwell, Jim Bladel, James Gannon, Sara Bockey, Volker Greimann, Kathy Kleinman, Susan Prosser, (Perry Sterling), Susan Kawaguchi, Stephanie Perrin, Paul McGrady, Todd Williams, (Vicky Secor) and Alex Deacon.

We received apologies from Don Blumenthal and Michele Neylon. And from Staff we have Marika Konings, Mary Wong, Amy Bivens and myself, Nathalie Peregrine.

I'd like to remind you all to please state your names before speaking for transcription purposes. Thank you ever so much and over to you Graeme.

Graeme Bunton: Thank you kindly. So this is Graeme Bunton. I'll be your Chair for today's call. Before we get going now's a good time to let me know if you've got updates to your SOI.

And actually I'm going to pick on Dick Leaning because I'm pretty sure he retired Europol.

Nathalie Peregrine: Yes.

Graeme Bunton: So he probably has which I guess is just a friendly reminder to make sure that we've all looked at our SOIs in recent history and that we keep those up to date.

So on today's call we're going to hear from Subteam 1 on Section 1.3.2 and this is hopefully a final report although who knows? We may see that there's some more work to do there.

We'll have some discussion on that and then we're going to take a look at the - if we get this far to a public review tool on Section or Recommendation 16 through 20.

That document came out on the 21st of August. And then I think shortly before we wrap up we'll take a look at the issues we've identified that we need to come back to and we can have a - think about how we're going to approach those.

So without too much more ado let's get into our report from Subteam 1, which I think is Alex Deacon and Lindsay Hamilton-Reid and I think Val Sherman was in on that, who I've heard by the way have done excellent work so far in that subgroup that they've been working really hard, so thank you very much to them and we should all be quite appreciative of these efforts. Alex you want to take it away?

Alex Deacon: Sure Graeme. Can you hear me okay?

Graeme Bunton: Yes maybe a little bit quiet but reasonably well.

Alex Deacon: Okay I'll try to speak up. So for our subteam we've been working on kind of distilling the comments into a set of updates and recommendations to the report.

Unfortunately I have - because of holidays and other issues I've not had a chance to put pen to paper for the first question. But the plan is - for the first part of 3.2.1 is to this week do exactly that, which is start writing and suggesting updates to the report based on the input we - we've received from the community and review that and present to the greater Working Group sometime this week so that's the plan.

I apologize for not doing that before this call. It was my hope but I didn't get a chance to do it. We have - we had a little bit more progress for question - the second part and so to give you an update on that I'm going to pass the baton over to Val. Val are you on?

Val Sherman: Yes I am Alex. Can everybody hear me okay?

Nathalie Peregrine: Yes.

Graeme Bunton: You're coming through clearly.

Val Sherman: Okay wonderful. So as you know - and I see that the summary - the 2/2 summary has been posted up. So as you know a good initial step was to develop some of these at their current (unintelligible).

And since our last call we've really with Mary's help included in our consideration several additional comments as discussed in our previous - in our call last week - our subteam call last week.

But in my view those comments did not significantly alter the takeaways from the comments or also the summary. As you know questions are really composed of (unintelligible) sub questions and in some instances there does not seem to be a single, clear direction or answer to be gleaning some public comments.

So keep that in mind as you review the draft recommendations that we have prepared per - in the consideration of the Working Group. And coupled with this call you have - not every member of a subteam has provided feedback just yet - only Staff recommendations but to the extent on how there has been a discussion - some discussion of support.

So at this point I'll briefly summarize the comments to each question and draft recommendation. Is that all right with anyone? I probably would encourage our group as a whole to discuss what we think and whether and how the questions - two questions should be addressed in the final report.

So Question 1 is, "Should it be mandatory for accredited providers to comply with express requests from LEA in the provider's jurisdiction not to notify the customer?"

So overall most of the comments were that - clearly that it should not be mandatory to comply with express requests from LEA unless required by applicable law of either the requester or the Registrant.

There were - there was some support for Registrants to always be notified but this was also carried with the fact that it may be possible in some instances such as with abuse allegations or the - whether requests are deemed valid.

Some suggestions - some suggestion was to differentiate between local LEAs across and those of other jurisdictions and so forth. And you could see there's some reason this screen - so I won't unless you want me to spell out exactly what each one said.

So as far as the recommendations the general takeaway appeared to be that accredited providers should comply with the express requests from LEA not to notify the customer where required to by applicable law.

And the Ws - the ones we're going to consider were to adopt this message explicitly in our report, given that the number of commenters did not zero in on that phrase in the provider's jurisdiction and indeed some pointed out that there might be differences with - depending on whose jurisdiction it is.

The Working Group may also wish to consider whether it should be mandatory for providers to comply with requests from LEA in other jurisdictions such as those of the requester or the Registrant.

So that's kind of the draft recommendations from that particular question. And I can keep going through all the questions if you would like or we can stop and discuss.

Does Marika or Mary or (unintelligible) have a recommendation on that?

Graeme Bunton: Basically we don't. I think I have a sense that these questions might bleed together a little bit, so maybe we can carry on and we can take some hands if we see them but let's keep moving. Thank you.

Val Sherman: Sounds good. So Question 2 is whether it should be - whether there should be mandatory publications for certain types of activities such as malware, viruses or violation in terms of service for these (unintelligible).

Roughly half of the commenters didn't address this question, and the general feeling amongst those who wanted - 39 out of 82 roughly is that there should not be mandatory publication for a variety of reasons such as search engine malware, and also that the privacy proxy providers should agree to take reasonable steps to investigate and respond to complaints.

A few comments did advocate publishing if illegal activity was established (unintelligible) would be appropriate when the two - so the DNS and then if the terms of service legal certainly is established.

But also noted that provider action presumably a person that did the terms of service want to include other perhaps even more severe responses. Several comments did note that perhaps publication - the sensitive action is appropriate but publication may not be - may not necessarily be the answer.

So the next step or the recommendations rather - it kind of takes, you know, getting from all the comments overall there's a high degree of reference - which you'll notice particularly early in response to Question 3.

But there's a high degree of reference to contractual agreements in terms of service between the providers and their customers. It seems that given that fact that contractual agreements could/should similarly control whether the (unintelligible) that violate those terms of service.

So therefore the - there's a likelihood of - consider whether to recommend the policy should be mandatory for those certain types of activities - the standard that would be reflected in the terms of commission and enforced accordingly.

We also believe that's good (unintelligible) which to consider and what's appropriate and that - ensure that these that should be appropriate as well as whether there may be any other remedies dictated by the terms and conditions other than publication to temper or commit effective investigation of the alleged abuse.

Moving on Question 3 is, "What if anything should be the remedies?" I'm sorry, "What if anything should the remedies be for a warrant to publication?"

And all in all in just seems that the majority of commenters believe that there is sufficient remedies under contract law. So many noted that it should be a matter between the provider and the Registrants and dealt with under the terms and conditions and the local law.

Some noted that there should be a penalty such as loss of accreditation. Many noted that there's really nothing that could be done once, you know, once the damage is done.

So the next steps - the final takeaway is essentially that contractual agreement and the relevant local laws' controls and - are sufficient to remedy and warrant a publication.

The Working Group should consider whether language specifying this sentiment should be included in the report. Perhaps it is only inherent in the status quo or whether the Working Group should consider additional remedies to warrant publication.

Question 4 is, "Should a similar framework and other considerations apply to a (unintelligible) other than LEAs and intellectual property rights holder?" Roughly 50 out of the - I'm sorry.

I'm hearing a little bit of an echo. Can everybody mute their phone? Okay so anyway roughly 50 out of (unintelligible) question. The majority of those roughly 40 out of 50 who did comment were not in favor of a framework for requests for - from third parties other than LEA or intellectual property rights holders.

So those individuals - to summarize in my opinion question in the subsidy of a framework for those third parties or thought it should be restricted or safeguarded, and many thought that the processes in place are sufficient.

So the next steps on - are essentially that although a number of those who responded to this question questioned the necessity of such a framework for third parties other than LEA and IP rights holders.

Not many of them expressed exactly why they thought it wasn't necessary. And we have deliberated related issues as a Working Group for some time,

and several answers again for other groups may be applicable here, because many commenters were concerned with safeguarding the privacy and this is apparent throughout the comments.

Applicants should remain on balancing privacy interests with other interests to make sure that there are adequate safeguards in place and any trademark for disclosure to (unintelligible) and IP rights holders.

Just as kind of a side note there appears to be a level of trust of the community in the providers to investigate allegations of abuse, the conduct that is against the terms of service and which are again apparently, you know, that are obviously controlling and are accepted as such by many and to respond fairly to those components.

So because of the apparent reference to contractual agreements between providers and their customers, there were some good - was to consider specifying in the report that certain types of activities are prohibited or should be prohibited by the terms of service and that any framework that's designed should show consistent - restricted and balance (unintelligible) to address any of these components.

I also want to note that the answer to this question may to some extent depend on the framework established for LEA and IP rights holders. And perhaps - and then know entirely what, you know, how this would be done but procedures for disclosure on other such calls could be implemented after the accreditation comes into port.

So that is the latest summary and the draft recommendations and I invite everybody to comment on those and provide us with your ideas and thoughts. Thank you.

Graeme Bunton: Thank you Val. That's a - that is a whole lot of work and an excellent summary. So we've got sort of four questions there to deal with. I see James

is in the queue - James Gannon, other James, Irish James is in the queue already.

We'll take James and then maybe what we'll try and do is go through those questions one by one just to see if we can make sure those are covered and we'll see where we're at. So James?

James Gannon: Hi. James Gannon. I apologize if there's any background noise. So I have a question about Question 4. So obviously the question as we framed it was LEA and intellectual property rights holder.

Having gone down through the responses that we have listed in the column here on the table for Question 4, I notice that the majority who are saying no are also saying, "No, it should be LEA only."

So did the subgroup assess the - kind of the subset of Question 4 responses that indicated that they were comfortable with LEA only, or did you go into that kind of specific detail because that's an important consideration to make?

We can't sufficiently answer Question 4 or come out with a recommendation until we make sure that the responses that we're using to form that recommendation are actually applicable to the whole question rather than just the LEA subset.

So did the subgroup go into that at all and if so what was the outcome of those discussions?

Val Sherman: This is Val speaking again. So the - what we did was we really just, you know, and in light of some timing constraints we really wanted to focus on answering the exact question posed.

And to the extent there might be issues that are relevant to other subgroups perhaps we tried to flag them. So you could see - in the summary for

Question 4 you could see that we did flag the comments that said that, but that we - like you can't actually see the commenting here but it's actually - it's the comment that suggested that perhaps this is considered as a, you know, perhaps Subset 3 or following our answering a specific other question. So we tried to answer and we didn't quite get there.

And as far as whether it's - whether our response to other - if I understood you correctly whether there was - whether what we developed for LEA or IP rights holders would affect this.

You know, that kind of recommendation was perhaps we could consider exactly what framework should be for those other parties after the accreditation is in place. I hope I answered your question James.

Graeme Bunton: I think I see...

James Gannon: Yes you did.

((Crosstalk))

James Gannon: Yes sorry. Yes perfectly. Thank you.

Graeme Bunton: Thanks Val. I see Steve has got his hand up.

Steve Metalitz: Yes thanks Graeme. Steve Metalitz. First, thanks Val and to your - you and your colleagues for a very helpful report and this really gives us I think something to work with.

I really had two reactions and one is going to Question 4. I agree that there are some people who said to use that as an opportunity - although that wasn't really the question.

They used that as the opportunity to say that they - there should only be disclosure to law enforcement. So I think that is an appropriate subject for Subteam 3 to look at.

I think that they had kind of divided the responses they'd reviewed into those who accepted the premise of Annex E that there should be some mechanism for intellectual property interests to obtain disclosure, and those who did not accept that premise and I suppose those - the two comments in this group that would fall in that latter basket.

So I think that would be a good approach to - the other reaction that I had was - and again more on Questions 2 and 3, which I think is basically supportive of the approach we took, which is that a lot of these issues about publication and so forth should be handled by the terms of service.

And we - I think our recommendations in the initial report really stressed that that Registrant's customers should be made aware of what the terms of service are, what's the kind of uses of the domain name that could lead to publication or to disclosure and that all that be laid out more clearly than the current specification requires for a subset of the privacy and proxy service providers.

So, I mean, that's kind of my takeaway from 2 and 3 is that we - we've kind of addressed that in other recommendations where we did have a tentative view in favor of better disclosure by providers to customers and what might lead to publication.

So I think perhaps we can view those as reinforcing those recommendations. Thank you.

Graeme Bunton: Thanks Steve. I don't see any other hands at the moment, so let's just make sure that we - we've - we're feeling good about these questions. And the - these summaries that we've got there, which is the first one was, "Should it

be mandatory for accredited privacy and proxy service providers to comply with express requests from LEA in the provider's jurisdiction not to notify a customer?"

And my understanding from the summary was that it was no they're not required unless required by law. Did we have any thoughts on that one? We can move on? I see your hand is still up Steve or is that a new one?

Steve Metalitz: No that's an old one.

Graeme Bunton: And then I see Holly. Holly you have a comment on that?

Holly Raiche: Yes I do. I guess when you summed that up what do you see the difference or do you see the difference between as required by law and as required by law enforcement agencies? Are you making a distinction or not?

Graeme Bunton: My understanding, and please someone correct me if I'm wrong, is that unless required by law a privacy and - or that could be a court order or something like that.

Then even if law enforcement says, "Also please don't," then a service provider could actually inform the customer of the request. I think that answers it. I see James and then Stephanie.

James Gannon: Hi. James Gannon. So I can actually speak to Holly's question. So this is actually a really important distinction. So there is a very clear line between - like we'll take the U.S. for example - between when the FBI comes and asks enough to - between for example the National Security letter which you weren't bound by law not to.

So that's a very important distinction - being a civil request from a law enforcement agency, which may or may not be honored I suppose would be

the word by the person who is receiving your request, whereas something like a National Security letter you are bound by law not to inform the person.

So that's a very important distinction and it's something that I think a lot of providers would be very adamant on. I'm not saying the provider but, you know, somebody who works in the space where this is a very important distinction.

I think that it's something that we should not go near. It's something that is very clearly set out in national laws and it's a very important distinction between the two things.

Graeme Bunton: Thanks James. I've got - and hopefully that clarifies things a bit for you Holly. I've got Stephanie then James and then maybe we'll close out Question 1 and try and have a little chat about Question 2 and 3 and 4. Someone has their mic open. I bet it's Stephanie. Stephanie go ahead.

Stephanie Perrin: Thanks. Sorry to open too soon. Stephanie Perrin for the record. I'm just not - I usually don't disagree with James but I'm not so sure that it's always that clear - national law and that's why I raised my hand.

I just wanted to say that we should not be directing providers not to reveal as a general detailed position if asked, because a variety of laws can require that they inform the individual.

Could be in the telecom law. Could be in the privacy law. It's more likely to be in the privacy law of course and if they don't have any you still might have something in some other kind of law depending on who's coming in there.

Getting - that gets us back to the rather muddy question about what law enforcement agent are you dealing with? So I think we should be quite clear in our directions that a provider should be governed by local law including

privacy law just so that they don't wind up in a default position of saying yes to agency requests. Thanks.

Graeme Bunton: Thanks Stephanie. I think that's sort of generally agreed that, you know, we can't make people do things that is in - against local law for them in whatever their jurisdiction is.

And we also can't make service providers comply with, you know, law enforcement requests from outside the jurisdiction. So no disagreement that we can maybe make that a little bit clearer but I think we're on the right track there. I see James and then Paul.

James Bladel: Hi Graeme. Thanks. James speaking. So just, you know, generally I'm on board with where it sounds like the subteam and the larger Working Group are coming in for a landing on this recommendation but I would want to add -- something to the effect -- that this accreditation program establishes some minimum practices or minimum standards of behavior.

And that providers are free to develop their own -- perhaps more stringent -- requirements. You know, over and above what may be required by law enforcement.

So as long as that's disclosed in terms of service with the customers. I can think of a number of situations where a provider may opt to honor say a request not to disclose when it was not obligated to do so. You know, but you know, and I think that's where we're going. And I just want maybe explicitly call that out in our final report. Thanks.

Graeme Bunton: Thanks James. Stephanie, your hand is still up. And I think that's a good point. That these recommendations don't limit a service provider from having more stringent conditions in the terms of service. And so long as those are robustly displayed and made clear, then that seems reasonable. I see Paul McGrady's hand up. Let's go to Paul, please.

Paul McGrady: Thanks. Paul McGrady for the record. James addressed one of my two questions which is whether or not anything we do here would prohibit a provider from cooperating -- in such a manner -- with law enforcement. Even if it was required under applicable law.

And it seems to be the answer is, no, we wouldn't prohibit that. Nor should we, as long as we disclose it. As long as the provider discloses it in his terms of service. So that's great. And I think we should capture that in our final report.

The other question I had is just maybe a word selection. We used the word "local" law. And I wondered if what we really mean is applicable law. I'm concerned that a provider that doesn't have an in-house council staff or access to -- you know -- attorneys who can field questions throughout the day might believe that maybe the law of the province where they are governs rather than a national law or some other obligation.

Or they might not fully understand the extent to which their business model exposes them to the laws of other jurisdiction. So would there be a lot of objection if we changed "local" law to "applicable" law? Thank you.

Graeme Bunton: Thanks Paul. I'm not a lawyer, so I don't think I can answer that effectively. Stephanie Perrin is saying, "Yes. It needs to be applicable law which includes international." Seems to be a reasonable amount of support in the chat for that suggestion. Any disagreements? Paul, that's a widely appreciated change, I think. So thank you.

Let's move on then to Question Two which - should mandatory publication for certain types of activity, malware viruses or violation of terms of service relating to illegal activity? And the general recommendation -- from my understanding again, correct me if I'm wrong -- was that there should not be mandatory publication for certain types of activity.

I know we've discussed this in the past. But that seems to make sense to me. In that it would be an easy vector to expose someone by hacking the site. Putting up something against like a malware on a hacked WordPress site which is extremely common. And then use that to expose the registrant.

That would be a concern for me. And certainly there are many holes in many content management systems. And that could be a problem. I see (James') hand. James.

James Bladel: Graeme, thanks. James speaking. So just want to make sure that the inverts of what we're saying is not necessarily prohibited. Providers should be free to pick service for either malware or spam abuse or other violations of their terms of service. And they should be able to terminate that which has the net effect of publications, right.

If you are not the - if you're a practicing provider -- but not necessarily the sponsoring registrar -- you can't do anything with the domain name. You can suspend the privacy service which has the net effect of publishing in the contact who is.

But I just want to make sure that we're not painting providers into a corner here where someone who is -- you know -- operating a questionable, you know, outside of terms of service here. Is claiming that the provider does not have the right to publish their information. Because -- you know, again -- as long as we can - we carve out explicitly that providers are free to go above and beyond these minimum baseline requirements. So long as that's disclosed in the terms of service, I'm fine with that. Thanks.

Graeme Bunton: Thanks James. Any disagreement on ensuring that providers have discretion there? James.

Steve Metalitz: Not technical disagreeing. But I think it opens some interesting questions up. I haven't actually thought about. So when we have a situation such as that, I'd say the original thing of a genuine privacy proxy user has their site hacked as a result. Through no fault of their own than for security practices.

A non-registrar affiliated proxy provider which is to terminate service. How do we make sure that we don't get into a situation where we end up publishing innocent people, saying details into the "who is" into the public "who is" when it may not have been their - moved them indirectly at fault. How do we manage that risk? I notice James has his hand up. So he might have an answer for that.

Graeme Bunton: Thanks James. And I think I was more or less saying that question beginning is that's why sort of a know it mandatory is all right. And it's certainly a possible scenario. And this is why most providers will look carefully at those sorts of requests. But I'll let James respond. James Bladel.

James Bladel: Thanks (Graham). (James Bladel) speaking in response to (James Gann). So I'm sympathetic to that situation. I think the bet is plausible. And is something that we need to be aware of. And I think that - I don't know that we can write an effective policy that captures all of those -- you know -- possible situations.

I just want to point out that -- you know -- it's probably outside of the scope of what a service provider would consider a part of their service. It would be - truly it would be just another element of collateral damage as to having your site hacked. You know, and you have data stolen. And you have you're loss of reputation. And you lost your privacy service and all that.

You know, I mean, let's just put it on the list of things - the negative consequences to that. And I understand that they may be blameless in that particular situation. But I don't think that we can count on the privacy service to always infallibly make that distinction of the intention of the person.

Whether they are blameless or -- whether they are someone who's spreading malware and -- simply hiding behind the claims that they were hacked.

And I think that' - you know, I can see it cutting both ways. And certainly we don't want to carve out any protections that would be abused by the actual bad guys. So -- you know, I think -- as long as we can preserve some degree of provider discretion, the ability for a provider to examine these complaints. To take a look at the -- you know -- all of the factors. Including, perhaps, their history with that particular customer.

Make a determination and then give them the cover -- under either ICANN policy or their own terms of service -- to take action. I think -- you know -- I'm fine with that. I just - I don't know that we're going to come up with a universal recipe here. But I am sympathetic to the situation that you described. Thanks.

Graeme Bunton: Thanks James. I see (Phil Corwin). And then we'll try and move on to three and four real quick.

Phil Corwin: Yes. Thank you. Phil Corwin for the record. I just want to express a bit of concern. Not an objection. But to the concept of what we're doing here is establishing standards for privacy proxy providers via law enforcement and possibly other powers. Other requestors for communications and publication or whatever. But that there's (unintelligible) the customer, the registrant is that there's no down side to what the proxy and privacy provider can do as long as they're providing notice.

You know, we've seen links to various (PP) providers where they say, "You know, we can basically take action and list the ser - and terminate the service without even giving you notice and an opportunity to respond."

You know, we - I believe we address things like that in the overall policy we're recommending. But I think if we're going to have a policy here that establishes baselines, it's got to be some baselines (unintelligible) the

customer at all. We can't just take a position that anything goes (be it be) the registrant and there's no liability on the provider as long as they're unreasonable policy is first fully disclosed.

Again -- I think -- we address a lot of that in the overall policy. But I just wanted to raise concern about the concept that's being advocated there. That anything goes via the registrant. So long as it's disclosed up front. We're setting minimum standards here. And there shouldn't work for both law enforcement and other requestors. As well as for customers. Thank you.

Graeme Bunton: Thanks Phil. That's a good point. I see James has got his hand up. So we'll hear from him.

James Bladel: Yes. James speaking. And to (Phil's) point, you know, I agree with him. We shouldn't allow providers to simply put what they want in the kitchen sink into their terms of service. And -- you know -- give them that much latitude. But -- you know -- I trying to find that Goldilocks area here where we have sufficient discretion.

And -- I think that -- by having some robust policies that there are backstops behind these minimum best practices. You know, that giving providers the ability to go over and above this is not necessarily a bad thing. That's all we're talking about. I don't think we want the exception to drive the rule. I certainly agree with you there Phil. But I do think it's important to at least...

Steve Metalitz: I'm with you there James. You might want to back up for a moment and try that again. I can't hear you if you're still talking.

Phil Corwin: This is Phil. Just let me jump in while James is trying to regain his technological voice here. I think a lot of this can be just addressed by minimum procedural standards. I mean it becomes a much less concern -- you know -- if terminating the privacy proxy service for violations of terms of service like using the Web site for distributing malware virus.

So long as the registrant - the customer, the registrant, is given notice and opportunity to respond. Even on an expedited basis. So they can say, "Hey, wait a minute. My Web site which was hacked this morning. And I'm not doing that deliberately. And we're working to fix it."

It's just the concern that actions could be taken without the customer having any notice or opportunity to respond at all if that's not in terms of service. And again -- I think -- we've addressed some of that in the overall policy. Thank you.

Graeme Bunton: Thanks Phil. Yes. I'm not sure -- off the top of my head -- how we would work in whether you make it sort of a mandatory response period from the customer. Or you include that as a general recommendation that customer's should be able to respond to a complaint of malware virus in terms of service violation. James, are you back? Did you have more to add? No. Not back yet, I guess. Yielding to the queue. I see Stephanie Perrin and then I'd like to keep going. Stephanie.

Stephanie Perrin: Thanks very much. Stephanie Perrin for the record. This is a - you can file this under stupid questions that I persist in raising. Do we have a procedural mechanism whereby ICANN would step in -- upon receipt of complaints -- when an accredited privacy proxy register wasn't acting in bad faith? Let's say I'm a journalist within a conflict area.

And my buddies and I discover that -- somehow law enforcement or a government agency or -- a political party that's out of favor is finding out who we are. Will ICANN investigate if there are allegations that it's -- in fact -- our privacy proxy service provider?

Graeme Bunton: I feel like we may be lost a little bit of that last. Your mike is still open and quite loud Stephanie. And ICANN as teams point out in the chat, would only get involved if they violated their accreditation agreement. I'm not - I building

a sort of regime I think you're talking about would be beyond our scope. And so that's worth thinking about. Maybe we can elaborate that a little bit more in the list. We'll see if anyone has any other response that we can come back to it.

Moving on now, I think - your microphones open again Stephanie. Right. On to Three. So remedies from warrants and publications was that there is general recommendation that there is sufficient remedy inside of contract law. There was some suggestion that ICANN could step in and you could lose your privacy and proxy accreditation. If you're frequently an exposing registrant needlessly - I have to go back to the recommendation very briefly. So relevant local law should be sufficient. As I think where that recommendation lands.

Is there any thoughts on that one? I feel like that's reasonable. Okay.

Moving on then to Question Four, which was "should a similar framework and/or considerations apply to requests made by third parties other than (LEA) and intellectual property rights holders?" And the recommendation on that one, scrolling down to the bottom of the document. So they were not in favor of a new framework for third parties other than (LEA) and intellectual property rights.

And -- I think -- we logged some of this onto the plate of sub-teams three, was it? They've - I mean I don't know that we've spent time identifying other third parties. And the framework is relatively specific for intellectual property. So I'm a little bit curious as to what that would look like to build. And it would have to be -- I think -- reasonably specific for each other sort of category of third party. I see (Steve's) hand up. So let's hear from Steve.

Steve Metalitz: Yes. Thanks. This is Steve. Yes. I think that in general a lot of - it seems as though a lot of the respondents didn't really answer this question. Maybe we didn't ask it very clearly. But let me just make a couple of points about

requests from law enforcement, from intellectual properties and from others. First -- on law enforcement -- my understanding is maybe we need to say this explicitly. That if there is a law enforcement request for information about a customer from a law enforcement agency within the provider's jurisdiction.

Then -- without regard to whether this is a question we've been discussing has been whether that request has to be disclosed to the customer -- leaving that aside for a moment. My assumption is that if the provider receives that request, it's supposed to (take test to comply). So that's one category.

Intellectual property's is spelled out in (NXE). And I would point out that in (NXE) if the intellectual property provider - excuse me, owner provides certain information. And depending on what the receipt. You know, that has to be communicated to the customer. Depending on that response, the information may be disclosed. But it's not mandatory. And there are stated reasons - stated grounds on which the (NXE) on which the provider can decline to disclose. That's the second category.

The third category is everybody else. And we've identified these many times. We've talked about malware. We've talked about spam. We've talked about other kinds of abuses uses of domain names. And we haven't come up with a framework for those.

We've suggested that (NXE) may provide a template for that. But, obviously the information that would have to be provided in a malware situation in order to trigger disclosure would be quite different -- than I would expect than -- the information that they would have to be provided in the intellectual property step.

So -- I think -- the question is -- you know is -- this something that this group can undertake to try to develop similar types of frameworks for other non-law enforcement and non-intellectual property requests for disclosure of customer information. I'm not sure that it is.

I don't think that we - I think as we move along here, if we can come to closure on the first two categories, law enforcement and intellectual property. Then it may be that the others simply have to be developed during -- you know -- the life of an accreditation system. And has to be some process for doing so. Unless people think that these are much easier to resolve. And that we can get the people with proper expertise to the table here within the next -- you know -- 10 days or so. Or two or three weeks.

I'm just not sure it's feasible for us to include in our final report. Similar provisions and effects similar to annexes that dealing with other types of requests. So that's kind of how I look at this. I think that's consistent with the responses we've received.

Although I would have to defer to the sub-team on that. But -- I think -- that maybe a useful way of thinking about this. That we have a law enforcement track, again, within the jurisdiction law enforcement track. We have an intellectual property track. And then the other tracks may need to be filled in later. So that's how I would approach this question. Thanks.

Graeme Bunton: Thank Steve. And I agree that we don't have immediately -- at our disposal is my sense -- the, you know , a broad enough section of experience from -- you know -- those third party you mentioned or otherwise too build that in the time that we have before us. And so what we might want to do is think about the mechanism for a coalition or group of third parties to come up with that - what that other spec might look like. That other annex. And how that would get adopted. And I'm not sure what the process for that would be. But it's something that we should probably think about. I see (James Cannon's) hand up.

James Gannon: Hi. It's James Gannon. I'll be very brief. I broadly agree with the categorization. But it seems to me that when it comes to the law enforcement issue. I want to point something that may come out of Sub-team Four.

Though there is, however, a very important differentiation within law enforcement between a law enforcement request to a provider. And a provider being compelled to disclose by law. So this comes back to the issue of court orders and everything else. And a lot of our commenters have chosen to speak about.

And -- for example -- we can call out (REE's) example. Recently the city of London Police and Flexible Property Crime Unit has been blazing a trail and sending out official looking requests to (OECD) providers. And asking them to take down domains. But these are just requests coming from a law enforcement agency.

They're not backed by a court order or any other legal instrument. So we need to be very careful when we're talking about - we need to - when we're talking about law enforcement requests, we need to be very specific when we're talking about them. Because they're two different things between court orders or legal instruments by a court. And just a request.

Graeme Bunton: Thank James. That sort of speaks to conversations we've had (effort) to protest. So that brings us to 10:56. And I think we did some really good work there. Working through those recommendations. And again, thank you to that team for developing them. My impression was that (Alex) was going to send out another summary of the work today. And we'll look forward to that. Thank you. Going forward, I can't recall who's going to be presenting next week. But maybe (Mary) can mention that in the chat.

What I would also strongly encourage every - okay. Sub-team Two. That would make sense. Given today was one. I would strongly encourage everyone to take a look at the documents that (Mary) sent out. So that would Public Only Review Tool Versions Three and Four for Parts Three and Four. So three has recommendations 16 to 20 and four -- I believe -- has other comments that were collected. I think we're somewhere now over 200 pages

of - (Mary) has collected comments. And that's a herculean effort. Thank you again, (Mary).

And then maybe we've got three minutes left. (Mary) if you can put on the screen the other document you shared. That is the topics we still have to come back too from our issue spotting's. (Mary's) pulling that up. And this is just to reinforce everybody's homework for our discussion on the list.

And next week's call is that one go through Part Three of the Public Review Tool as well as Part Four. Have a look at the list of things we've identified here. And maybe we can dig into start thinking about how to come up to some compromise and consensus on these issues that we're still facing.

And that brings us to 10:58. And unless there's anything else, I think we'll give you back a wonderful two minutes. And thank you all for coming and participating today. It was some good discussion.

Nathalie Peregrine: Thank you.

Coordinator: Thanks very much. That concludes today's call.

END