ICANN

Moderator: Gisella Gruber-White
August 26, 2014
10:02 am CT

Coordinator: The recording has now started please proceed.

Terri Agnew: Thank you. Good morning, good afternoon, and good evening. This is the PPSAI Working Group Call on the 26th of August 2014. On the call today we have Graham Bunton, Steve Metalitz, Frank Michlick, Stephanie Perrin, Don Blumenthal, Griffin Barnett, Todd Williams, Justin Macy, Tobias Sattler, Michele Neylon, Kristina Rosette, Alex Deacon, Lindsay Hamilton-Reid, Darcy Southwell, Chris Pelling, Jim Bikoff, Phil Corwin, and Susan Kawaguchi.

Joining us a little bit later on the call will be James Bladel. Apologies for today will be Holly Raiche and Sara Wyld. From staff we have Mary Wong, Marika Konings, Amy Bivins, Danielle Andela, and myself Terri Agnew.

I would also like to remind all participants to please state your name before speaking for transcription purposes. And it looks like Volker Greimann has just joined us as well. I will now turn it back over to you Don.

Don Blumenthal: Appreciate it Terri. Thanks for getting us set up. The weekly -- I am going to try to remember -- call through people who (unintelligible) not any updates to (TSOI). A couple of things to get started that aren't completely on the - well one that's not on the agenda but just a quick update on the face-to-face session.

I'm not sure if we mentioned this last week. I think it happened afterwards, but Thomas Rickert has agreed to be the side moderator or assistant. I'm not sure what the direct term is, but he will be helping out moderating along with the person that ICANN has hired to run the session. I assume that most people - if you don't know. Yeah, facilitator is good. Thank you Michele. Even if you don't know Thomas, you know of him, and I am really glad he stepped forward or agreed to - or answered the call anyway.

Planning (unintelligible) in (Florida) is going along really well I think. There will be a call to get, you know, the staff, and Thomas, and I am blanking on the outside person's name, but get them on the same page. And in September, we will add Graham Stevens in the process after that and just keep - I have got to stop reading chat when I am talking. Well we will keep you all up to date as we go along.

The agenda says we will start with F1. I would like to begin really with what's on your screen there. And we were talking on the planning call yesterday and (unintelligible).

Man: Is (Lizzie) there Don? Don, you are not audible at all. You are - we hear fragments.

Man: Graham should take over.

Man: I think it's actually Steve's turn.

Man: Let's give Don...

Don Blumenthal: Okay, is this any better.

Man: Yeah, I can hear you.

Don Blumenthal: Okay.

Man: We can hear you now.

Don Blumenthal: All right great. We were talking yesterday on the call and just the question under category (unintelligible) is much longer than any other of the categories than we've looked at and a lot of the pieces circled back on each other. We've already discussed some of the things that seem to come up much later in the category, so please take a look at this, and as you are addressing points in F1, keep in mind that we will formally talk about them later. The point you are making may be formally addressed later. I'm not saying don't raise it, but just in terms of keeping the conversation moving, just keep in mind the flow and topics might be more addressed later on.

Having said that, I look at this list and I think I've got a question up front, to which we will have much discussion at all on some of the later ones. I hope that wasn't completely obscure or internally contradictory and the idea is we will be talking about things and just keep these questions in mind in terms of what should be addressed now or later.

And somebody I think anticipated what I was just going to request, which is bringing up the template for F1. Mary distributed this in the last - well I guess

it was yesterday and I just want to begin with the point that was highlighted and in which we discussed online after the call asking how do we go ahead with addressing our (terminology). Early in our lifecycle the idea of publication, disclosure, whatever (unintelligible) and now it is time to really decide how we are going to apply different terms such as (reveal), (publication disclosure) both in terms of how we conduct our discussion for clarity and then ultimately (unintelligible) documents. Are we going to call (unintelligible) different or we get (unintelligible).

So are there any comments right up front on the best set of terms that we should be using? The last one that was suggested there was no comment. It was (publication), which is (unintelligible) database versus disclosing but not (posting). Steve.

Steve Metalitz: Yeah, this is Steve. I'm getting an echo here but I will try to persist. I think I'm fine with these definitions. My only question is on the use of person and we should just be clear that that includes a legal person as well as a natural person. A registrant might be a legal entity, a customer might be a legal entity, but with that footnote, I think these labels make sense and will be helpful to us as we move ahead in Part F. Thanks.

Don Blumenthal: I appreciate it. James.

James Bladel: Hi James speaking for the transcript. Wanted to agree with Steve and perhaps even suggest since the WhoIs field typically also asks for organization if we might consider saying you know person, legal person, legal entity, or other organization if we want to be specific and align it to the fields in WhoIs. Thanks.

Don Blumenthal: Great. Stephanie.

Stephanie Perrin: Thanks Don, Stephanie Perrin for the record. I am being a little nerdy here, but please bear with me. Reveal is not really a noun, so when we say publication means the reveal, what we are really talking about is revelation or disclosure. I understand all of these terms are loaded because they've been using them for years, but before coming up with definitions, can we say revelation of a person's blah, blah, blah?

Don Blumenthal: I'm just thinking (unintelligible) revelation. Pardon.

((Crosstalk))

Stephanie Perrin: (Unintelligible) means to reveal. You could do that, but...

Don Blumenthal: I'm sorry for interrupting you. I thought you had stopped.

Stephanie Perrin: Yeah, I'm fine.

Don Blumenthal: I'm (unintelligible).

Man: Just responding to Stephanie okay for the transcript. Stephanie and I have argued about this for the last two years on and off and I understand where she is coming from because the terminology that's being used for the last I don't know how many years is misleading and well in typical ICANN fashion fairly impenetrable.

I would object to changing the terminology simply on the grounds because that would actually lead to more confusion for people who have been trying to follow this, but I think the - a good compromise would be to explain in a footnote or elsewhere exactly what is meant by the term. I mean the terms that are used with respect to WhoIs, with respect to WhoIs privacy, proxy, and

various other things that are kind of specific twists on words from the English language that take on a slightly different meaning. And I think providing a clear explanation as to what they mean within this context would be helpful. Thanks.

Don Blumenthal: Okay, so let me ask. I've got to flip my audio method here to phone. Let me call on Kathy and then if it takes a few minutes Steve if you could take over.

Kathy Kleinman: Hi Don, hi all.

Don Blumenthal: Kathy.

Kathy Kleinman: Per the chat, well I think James described it too. I think we are talking about three categories, a legal entity, an organization, and the person or traditional individual. So I think we've got it there, so thank you very much.

Steve Metalitz: Okay, so this is Steve. Don, are you back?

Don Blumenthal: Yeah, Steve please pick it up. Please take over. I'm going to switch over to my phone.

Steve Metalitz: Okay, I see Stephanie's hand up. Is that a new hand Stephanie? I think you are on mute, but okay the hand is down. So are we now looking at publication means to reveal a person's legal entities or organizations (unintelligible) and then go on from there. I mean that's not - it's a bit awkward but I'm sure we could you know move the phrases around if it reads more fluently, but we have added in legal entity or organization and we said to reveal rather than the reveal of. Is that - I think that's kind of where we've come out on this unless people have objections to that.

Okay, so it is getting some traction so perhaps we could leave it at that. And if people - and we could accept these working definitions of publication and disclosure. I think if we go back to the questions that were posed, at some point there may be issues about whether the rules should be different for publication or for disclosure. In fact, likely they should be, but at least I think we are clear now what we are talking about when we use those words.

And I see Kathy's recommendation that we talk about publication after disclosure. I mean I welcome other people's views on that. It seems to make sense to me since the main issue here or the first issue is under what circumstances is this information revealed to a complainant or third party that believes this. And then the second issue is what are the circumstances under which this is revealed to the world through publication and in effect (kicked out of the) privacy proxy program, so I think it makes sense to address them in that order.

So let me just ask if people - if we are done with these definitions, at least for the moment whether people have comments that they wish to raise on question F1 bearing mind the other questions that will be following here. And I see if you scroll down through the document, there are provisional answers given to some of F1 by some entities that are represented on this call.

And if any of them would like to talk about what is their provisional responses are, I see we've got some of the (legit script) people here. We have some IPC people here. We have some NCSG people here. I'm not sure we have an ALAC person here, but if any of those would want to kick this off, that might be one way to get started on this.

I see James has his hand up and Kathy, so James why don't you go ahead and we will get started on this.

James Bladel: Thanks Steve, James for the transcript. And actually, I was going to suggest that something similar along the lines that you were saying. If we could perhaps get a volunteer from each of the groups to maybe walk us through their response, but even more I think relevant would be since the responses may be a little bit dated. If anyone believes that their responses have changed since they were originally submitted you know due to some of the conversations that we've had or maybe even changing in light of the refinement of the definitions or something along those lines.

So I was just kind of going to float the idea that if anyone has any notices that their responses need to be modified at this point. I don't know that our constituency submitted a unified response on this, so I don't think that I have anything to offer in that regard, but I just thought it might be a helpful way to go forward. Thanks.

Steve Metalitz: Okay thank you James. Yeah, I don't think your constituency - your stakeholder group has an entry on this chart, but I think it would be helpful if there are any providers of services who want to talk about how they handle this now. We do have - I think the staff compiled some of the policies that are in existence now. I don't know if that document is accessible immediately, but it would be - I think it could be useful to talk about how this is being handled now by individual providers because obviously that could be very helpful in terms of setting accreditation standards.

But let me turn to Kathy who is next in the queue. Kathy, are you with us?

Kathy Kleinman: Okay, sorry Steve. I have another call coming in that I had to decline. So I am actually happy to wait for the providers to talk, because the operational side of

this would be great to talk about. So I (can pause with you) to talk about the present before we talk about the future.

Steve Metalitz: Okay, well yeah, this is Steve and I don't know if that - if it has to be in that order, but I see Don may be back in the saddle again here, so I am happy to turn the gavel back over to him.

Kathy Kleinman: Makes sense and could we put that back on the screen again? I can't see it anymore.

Steve Metalitz: I'm not sure if they are switching to the compilation document or not, but anyway.

Don Blumenthal: Yeah I am back. I am just trying to listen for a second and figure out exactly where the conversation is. So I just kind of - I picked up where Kathy was suggesting she would defer to (writer), so if I could go to James and then I will figure out what you are being deferred to about.

James Bladel: Hi, this is James speaking for the transcript. Thanks Don, thanks Kathy. I wasn't really prepared with anything. I guess I would refer back to the slide deck that we presented. I think it was myself, and I think it was maybe Volker, and Graham, and maybe some others presented earlier on.

But I can at least you know just kind of give a rough overview of how we handle these types of requests now, which is that there has been a change recently in that you know requests to - well you know first off, I would say that for us, reveal was publication. Because if someone - a customer of our service was found to be violating our terms of service then we would simply cancel the service, which of course had the practical effect of publishing their contact details into the public WhoIs database.

Now as far as requests for reveal, I think we clearly had two tracks on this and then a special case that I will mark with an asterisk. The two tracks would be you know just a general third party request for reveal. You know hey I don't like what's going on with this Web site. Tell me who it is. Usually those would be - you know those requests would be denied unless there was some sort of documentation like a court order or something like that that demonstrated that we needed to comply with that request.

I think that we had a separate approach for dealing with requests from law enforcement, particularly law enforcement in our jurisdiction whether that would be the United States or Arizona, or other jurisdictions that we operate in and have relationships with. We had a fairly informal relationship for quite a period of time where a member of law enforcement would request the information and you know upon review, we would either publish the details or relay the contact information to law enforcement as a part of that investigation.

We have increased that a little recently as a result of just some recent incidents. We now request that law enforcement give us some you know objective indication of due process whether that's a court order, a search warrant, a national security letter, or some other documentation that indicates that it's something beyond just a hunch or investigation. That it's something that demonstrates that there is a formal process underway and then we would of course comply with that.

And then finally, the special case is - and I don't know if this falls - maybe my knowledge of our charter is probably worse than it should be, but you know with the - in the case of receiving a response noting that the privacy proxy service is being named as a respondent to a CRT filing, we would typically clarify those by you know reporting the privacy proxy customer's information

to the - you know naming them as the respondent and removing a privacy proxy service from the UDRP procedure. And I think that that would be maybe one example where a non-law enforcement third party would compel a response or a reveal from our service.

So that's just - I mean that's a very rough overview of how we would handle these requests and you know I think that - I don't have our terms of service in front of me so I think that that aligns with what we do. But if I've got something wrong in the details, then please refer to the actual documentation and not the things that I am just shooting from the hip this morning. So hopefully that's helpful. Thank you.

Graham Bunton: Thanks Steve, this is Graham. I will speak again briefly while Don catches up. Don we were just talking about publication and disclosure. We were just sort of wanting to find out what service providers are doing today in this respect and then we will dig into what people would like to do in the future as - from the comments on the charter question.

I am going to echo much of what James just said. It seems remarkably similar to how our privacy service operates. A lot of the requests we will get - we will discover excuse me that that domain is doing something against our terms of service, so that happens somewhat often. And then you know we have direct you know contact with law enforcement and we do try and make sure that there is some sort of evidence of due process there before we do any sort of action.

Yeah, that's more or less it. I would think it is quite similar, but I would also say that I think (unintelligible) and open (unintelligible) and GoDaddy operate a pretty high bar service where we are pretty careful how we operate. Thanks.

Don Blumenthal: Yeah, thanks Graham for the quick overview. I was back but I couldn't remember where the unmute button was on my phone. Well so it sounds like we've moved ahead from the definitions into the substance of when to reveal - I am using the verb form Stephanie. When to reveal I guess as a baseline and when it either should or shouldn't be left to the discussion of the privacy proxy provider.

I'm just making sure that I am not missing something in the chat here. From what I've heard here is we've been focusing on law enforcement and how to address their - when they are making the request to reveal. Is there more discussion on that or should we be looking at say the non-law enforcement. And again, we are talking baseline where proxy privacy providers should be required to publish or disclose. I am going to try to force myself into using the terminology.

Steve.

Steve Metalitz: I think Kathy was ahead of me in the queue, but...

Don Blumenthal: Okay, I thought that was an old hand. I apologize. Kathy was that an old or a new one?

Kathy Kleinman: I was waiting for the proxy privacy provider so it's a current hand.

Don Blumenthal: Okay.

Kathy Kleinman: Okay, so great. I think Steve had asked a really good question which was kind of a summary of positions submitted by the different groups as well as whether those positions have changed in light of some of the discussion over the last few months. So I wanted to respond to that because I think our

position has developed and grown a little bit, so this is for NCSG Commercial Stakeholder Group and we really are very concerned about the publication and reveal and right now we will separate the two.

So disclosure - when we say reveal, we generally mean disclosure to a third party and so we are very interested in seeing what the due process procedures are and what the jurisdiction is.

So recent events have painfully shown us that what is legal to report in one country is completely illegal to report in another country. And the disclosure of a report or a blogger to an entity outside of his or her jurisdiction may mean death and that's the real problem. And also, imprisonment and other things as well as for families, so we are concerned about what the jurisdiction is, what the process is for revealing someone's identity.

Also, I wanted to remind everybody about a discussion or actually a number of discussions we had a while ago and see how we can incorporate them here which is proxy privacy providers having the option at some point of this publication -- I'm going back to publication and the WhoIs, publication for the world -- versus the option of the takedown where the domain name just disappears rather than showing the world who is creating that potentially political speech.

And we do have a new question to add to that list of questions that were there, which is, let's say we do allow a reveal, a disclosure to a third party. Are there any limitations then on what the third party can do with the data? Can the law firm take it and post in on their blog? I doubt they'd do it, but do we want to think about imposing any limitations when the data - the identity and location and contact information of an organization, individual or a company is revealed to a third party? Should we try to impose?

Not that we can completely impose restrictions, but should we even try? And so I'd like to see that added to the list of questions. Thanks much.

Don Blumenthal: Thanks. I'll just move back to Steve.

Steve Metalitz: Yes thank you. This is Steve. And I appreciate having Kathy's, you know, opening statement if you will or introductory summary. Let me do the same for the IPC position.

And there is at least one area where there's been some change there. And obviously, there are also, you know, some questions that need further development and what the IPC has put forward.

We're focusing really on just one part of this. First, we're focusing mostly on what we're now calling disclosure. So, obviously some of our terminology has to be changed here.

And we're just focusing on the circumstances in which the disclosure is sought because the domain name is being used in a way, or its registration in effect infringes trademark or copyright. So that's obviously a subset of the kinds of complaints that could give rise to a disclosure request. But it's the one that were most familiar with.

So our view is that the test should be - that if there's a prime (aphasia) that is on (honest)-based evidence that there is an abuse involving infringement of trademark or copyright, cybersquatting, counterfeiting, basically items that are in the list that we've been talking about as far as abusive activities. That that would trigger the disclosure process.

There would need to be some kind of standard for achieving that disclosure. We do propose, and I think this is an important point and somewhat responsive to what Kathy's been talking about. That at least in most cases, and probably in the cases that we're most focused on, it would make sense to notify the customer before disclosure. And give the customer some opportunity to object to the disclosure, so long as the contact details aren't changed during that period.

So that's obviously a process that would need further discussion. But I think that's a significant safeguard against an improper disclosure.

For our fourth point is - it really goes to the question of I think Don called granularity that are going in view is at least is that if you get a disclosure, you get a disclosure of all the current contact information on file. Not - and that you would be allowed to use that only for dealing with remedying the misconduct or the abuse that's involved.

So that's - I think we're basically in agreement with Kathy's last suggestion about some limitations in the case of disclosure on what you can do with that information.

And then finally, where we do have a change is in our last point. Our last point states, and this is all in the document that had been up on the screen, the (FO) template document. So you can go back and review it.

We talked about escalation to publication when the third party is unable to contact the customer through revealed information. And on further reflection, and also because of the discussions that we've had about the providers having an obligation to, when they find out about, you know, invalid contact information that they've been given, they have an obligation kind of parallel

to what a registrar would have to try to get the up-to-date information. Get it corrected or else canceled the service.

That means I think our fifth point there is probably not as relevant because, you know, especially if there's a pattern where there are reveals from a particular buyer that turn out to be useless. In other words, the information does not enable you to contact the customer. Then that's really an issue of whether they're fulfilling their accreditation standards as far as maintaining up-to-date information.

What really is on disclosure, we don't really have a lot of views about the circumstances under which publication would be allowed, except to note that, you know, that's really a question of when can the provider cancel the service. And thereby put the data into Whois rather than substituting this provider's own data.

That's a broad question. And we don't have a - I think the focus of our answers, our provisional responses has been on what we're now calling disclosure. In other words, revealing it just to the complainant and just for the purposes of remedying the abuse that gave rise to the complaint. Thank you.

Don Blumenthal: I appreciate that. Give you all the detail there. I guess I wanted to just clarify that when I use the word granularity, it was in a, I think it was in a message to the chairs list, not everybody. But that is what I was talking about. So I guess I don't know if it matters really, Volker.

Volker Greimann: Yes, I think for the registrant in certain cases where he really needs his privacy protected for security reasons, the question of whether to reveal to the complainants or law enforcement agency or whether to publish the information, the Whois, is also a very minor circumstance because his

information will have been revealed to the entity that he probably did not want it to be revealed to. And compromising the security in some form.

So the question rather is in which circumstances should it be okay for this information to be revealed? Now law enforcement, I think we could all agree, has the most, how do you say it, rights to have that data revealed to them, especially if they are in the middle of a criminal investigation.

And even there, I would see that this jurisdictional barrier is very important for the privacy service provided to - taken into account. So if there is a request in our case from a privacy - from a law enforcement agency that we would not recognize as competent, we would reject their request to either reveal or publish.

Which ones do we usually consider competent? At that is kind of an established process that has grown over time. A, the location where the privacy service is located; B, the location where the registrar that is using the privacy service is located; C, potentially the area where the reseller to which the registration has occurred is located.

And, you know, we are very cautious with D, the location where the registrant is located because if the registrant is located in what we consider a high risk area, we would not reveal it to the local law enforcement agencies. Even though they might come from the same jurisdiction as the registrant's is originally from because we don't believe that we are in the position that we could risk someone's life. Luckily we have not been in that position of having to make such a decision yet. But that's, on a law enforcement level, where we would draw the line.

Don Blumenthal: Thanks. That piece is quite loaded obviously. You know, and I will just to - in defense of my alma mater, just suggests that we talk about investigations and not specify law enforcement criminal or civil, James.

James Bladel: Hi. This is James speaking for the transcript. I actually forgot I raised my hand. This queue has moved on. But my response was just on Kathy's suggestion of restricting what a requester can do or what actions they can take based on a reveal of how that information can be put to use.

I understand and support the premise. I don't know how we could enforce or impose that on the non-contracted parties in practical terms. My only thought would be that if this is something that we want to - we consider important enough to pursue that we may consider, you know, some sort of an accredited or a known reporting system where the reporters are authenticated.

And they would lose that privilege, you know, based on some sort of, you know, determine the biggest criteria, which may be outside the scope of this particular working group. But I just wanted to put that out there in response to Kathy. And I fully acknowledge that the conversation has moved on quite a bit from that. Thank you.

Don Blumenthal: Thanks. (Shades) of some of the ongoing discussions over the years of nothing else, how to identify if a law enforcement agency is - organization represents itself as law enforcement really is law enforcement. I'm just seeing three letters here. So is that Michele?

Michele Neylon: It is. It is I, yes. Thank you. Michele for the record. Going back to Kathy's thing, I mean at one level it's like oh my God, I mean this is - it's kind of, it's a lot of - it's a lots to be asking a private company to get involved with.

I mean if you turn around to us and say, you know, what you do here will have, you know, the impact of potentially killing somebody. It's like oh God, I'm out because, you know, we provide hosting. We provide domains. We're not into the entire kind of life and death stuff.

And that is the problem. I mean during our work with the EWG, as (Stephanie) or (Carlton) or (Susan) would tell you, I mean we did talk quite a bit about the entire concept of people at risk. I mean based also on conversations we had with Kathy. And it is - it's a very interesting, it's a very difficult, it's a very awkward thing.

I mean the problem though, and this is going to what Steve's talking about is that, you know, from our perspective, law enforcement is one thing. And I'll treat that in a particular way. Court orders are something I can treat in a particular way.

But then people trying to use trademark or copyright infringement claims, it's an area which gets quite gray and quite messy because unfortunately, what we're saying in Ireland and in other parts of Europe is where companies are abusing the copyrights and intellectual property laws in general in order to silence people.

I mean whereas under US law you might have a concept of freedom of speech. You don't have a concept of freedom of speech in a lot of European territories. So we see regularly, people trying to use copyright and trademark infringement to take down (gripe) sites or sites that are being used for various campaigns either in favor of or against particular companies, particular movements or whatever.

We've also seen people trying to get access to some of our clients who like to write about organized crime. And the certain parts of this country where if we were to do that that person probably couldn't go home in the evening. So thanks.

Don Blumenthal: Interesting. And for what it's worth, there have been attempts even in the US to go after (gripe) sites about - there have been attempts. I don't know how often they've been successful.

((Crosstalk))

Michele Neylon: The kind of thing we see Don is somebody puts up (gripe) site. Let's say if I was to put up a (gripe) site attacking - I'll pick on Go Daddy because it's big enough and (ugly) enough. A (gripe) site in the US would be able to put up a version of the Go Daddy logo. And Go Daddy may not like it, but they would have a particular level of protection. Under Irish law, that level of protection is practically nonexistent.

Don Blumenthal: Okay.

Michele Neylon: So they'd use - they could say oh, this is - you're breaching our trademarks or copyrights, et cetera, et cetera. And take the entire site down.

Don Blumenthal: Yes. I appreciate the difference now, Justin.

Justin Macy: Hi. Can you hear me?

Don Blumenthal: Yes.

Justin Macy: Great. So I think that I'd just like to jump on to what Michele and Kathy said. That there are definitely certain times where there are lives in a position of danger. But that kind of falls on both sides of the coin.

It seems that there's a risk if we prevent privacy proxy providers from being able to (sheesh) a relationship with a registrant if they know or have reasonable knowledge that there's criminal activity going on.

Just like in the situation where a registrar may decide hey, I'm out. When they website kind of gets to a level that they think that it's probably facilitating criminal activity and may involve. And may involve someone dying as a result of it.

Privacy proxy providers need to have the same ability to kind of back away. And they don't have the tools necessarily to shut down the website. I think they're kind of only left with the possibility of may be notifying and ceasing to provide the privacy layer on the registrant account. Because otherwise they might be stuck in a position where they are knowingly facilitating or being involved with criminal activity.

And they have to have a way out of that in our accreditation standards. So that's it. Thank you.

Don Blumenthal: Thanks, James.

James Bladel: James speaking for the transcript, and just to respond to Justin's comment, I agree. Service providers, you know, are businesses. And really would rather not be dragged into some of these very complex issues and questions.

I think that the way out in many respects is, particularly for our service, I can't speak to the structure and procedures of others. But for our service, you know, if - because we are the listed registrant, we have the authority, I don't know if we ever use it, but we have the prerogative to cancel the domain name entirely without disclosing anything if we are not the hosting provider.

So that's it may be one option that the privacy proxy service might have, you know, aside from publication and aside from just the dragged it to some inter-jurisdictional privacy or fair use or free speech or religious speech type of action. Is just to say, you know, I'm the one that's listed as the registrant. I'm using this domain name so, you know, so I'm out of it.

Don Blumenthal: Okay. Justin is that a new hand?

Man: I think that's his old one Don.

Don Blumenthal: Okay.

Justin Macy: Yes, sorry.

Don Blumenthal: All right, Michele.

Michele Neylon: Yes, no just to, I mean also speaking to Justin's point. I mean Justin works for the LegitScript. So I mean when he talks about life and death, he's talking about, probably talking about (fake pharma) and things like that. And I think, you know, that's a different conversation that I think is much bigger and much broader than just simply privacy and proxy.

You know, some of us have agreements with LegitScript or with other entities to do things - certain things with domain names when we receive notification from LegitScript. That would include us.

You know, (Black Knight) will - has an agreement with LegitScript. And will quite happily remove domain names based on a report from LegitScript. LegitScript on their side better not screw up. I mean if they tell us to start taking down legitimate domain names, then I'll be very, very upset with John Horton.

But that's, you know, that's - and if, you know, if for example I don't know, somebody was involved in some kind of serious crime, then I'd think, you know, we might have to deal with that. But that's, again that's a bigger thing.

I mean if you look at the new TLD contract for example, there is an entire section within that contract about various things to do with illegal activities. And it's - and the same thing has been passed through to the registrar/registry agreements in a lot of the TLDs.

So I think, you know, this is something again which I think is just, it's beyond this privacy proxy thing. And while interesting, I guess I wouldn't want to (conflate) them all too much.

Don Blumenthal: Yes, that (conflation) is a good point. And before I jump to Volker, I just - well just going back to the idea that we're looking for a baseline here. You know, the examples of how things work in practice are invaluable in terms of coming up with that baseline.

But what Michele was just talking about I think is a good example of what a proxy privacy provider could do. As opposed to where it would be required to

do a disclosure. And transferring Michele's example into the disclosure realm, Volker.

Volker Greimann: Yes, thank you Don. Volker speaking. I think we've touched upon very important point here. The baseline has to be something that works for providers in all countries.

And we shouldn't try to be solving problems that are not necessarily with service providers per view or a problem that's related to a Whois privacy service provider.

If it's a problem like unlicensed or fake pharmacies, I don't think that's a privacy proxy problem because you don't - you want the domain name down, not the registrant revealed. That's something for the registrar or the hosting provider and my view. That's not something that the privacy proxy service should be primarily involved with.

And even then, laws may be different for when we talk about baselines. If we have an Indian registrar or a privacy proxy service provider providing services for Indian pharmacy that is licensed in India. That happens to send out their licensed product to the US, which may be illegal in the US, but may be perfectly legal in India, is that a problem for the privacy proxy service provider? Is that a problem for the accreditation? Is that a problem for the registrant? I would say no. And that's what the baselines would have to take into account.

Don Blumenthal: Thanks. Yes, no that's a good teasing out of the point I was thinking of. Again, transferring the example over to a disclosure discussion, Steve. Steve?

Steve Metalitz: Sorry. Can you hear me now?

Don Blumenthal: Yes, got you.

Steve Metalitz: Okay I'm sorry. I guess I was on mute. The - we've heard several references to - and that descriptions that James and Graham gave at the - earlier in the hour to violations of terms of service for the privacy proxy service.

And I certainly think that they should have - that these services should have the ability to enforce the terms of service. And that in some cases, again where they're not serving as the registrar, this may be all they can do to deal with illegal activity that's taking place in connection with a domain name for which they provide this privacy service.

But there's also - and again, we heard from the existing provider that this is a - this is something they do today. I think that's pretty common for all of the providers that if you violate the terms of service, you can get kicked out, which in effect in the terms we're talking about is publication.

But there's - there really is a lot of overlap I think between - in many cases between those terms of service and the kinds of abuses that we're talking about here. And I guess that the issue is if a violation is brought to their attention, will they either reveal to the complainant or publish?

And from the perspective of the IPC, we're not that concerned. We're not pressing for publication necessarily. But if that makes - if that fits better into the model that the service providers are now using that when they get a complaint like this they will kick - they will cancel the service. And as a result, publish in Whois the contact details. That certainly achieves our goal, although it's broader than what we're looking for.

So I guess I think we should just bear in mind that when we have all of these references to violations of terms of service, there's a lot of overlap potentially between that and the kinds of complaints that we're talking about. Thank you.

Don Blumenthal: Yes definitely. And I would - okay. I'll just go on to James.

James Bladel: Hi Don. This is James. And I do want to just kind of express my agreement with a lot of what Steve has offered here. It feels like a lot of what we're discussing is some very heavy, very complex issues regarding, you know, free speech and, you know, free expression and fair use and criticism.

And what I just made up a term. I should probably go register it, digital asylum or people, you know, who feel like they can't trust a service provider in their jurisdiction. So they're, you know, purposely seeking out of jurisdiction that they believe will protect their identity.

I think these are important issues. But I do sort of acknowledge that if we were to look at the 80/20 rule, they are probably (edge) cases. And so I think that when we talk about setting baselines, we should probably recognize that there will be some mechanisms necessary for service providers to address these situations when they arise. But we shouldn't let the exceptions follow the rule necessarily.

And what I mean by that is I just keep coming back to this idea of, you know, providing some level of, I want to say discussion on how the service provider is going to act situationally, depending on whether this is an intellectual property issue or a pharmaceutical issue or, you know, if it's legitimately an issue where someone's life may be jeopardized by revealing their name.

Or if the law enforcement is, you know, the FBI or Interpol versus, you know, a different kind of group that is perhaps not a legitimate authority and is simply masquerading as one to, you know, to persecute the registrant.

You know, I just, I feel like we could try to solve those issues in this working group, but that might be (falling). And instead we should maybe perhaps provide - and this goes back to what Justin was saying, provide sufficient escape hatches for registrar, or sorry, for service providers to, you know, extricate themselves from these situations, you know, as much as possible. Without necessarily jeopardizing or creating a liability by jeopardizing the safety of their clients.

So that's my thought here. And it just kind of goes back to tying together I think more agreement than not on some of these issues, particularly that third-party and law enforcement requests should be treated differently. And even then, law enforcement probably has a higher bar that it has to jump over. So thank you.

Don Blumenthal: I see what you mean. Since we're at 11, I'll just take an opportunity for the final word. I agree with what you're saying there. But again, just point out we're talking baseline requirements.

But all we're doing is going to be say broad brush baseline requirements. And while I think a lot of the discussion were having is going to be very useful for ICANN staff to play with. I think we just need to be aware of is how we ultimately - be aware of all these issues to guide us when we ultimately (draw out) what our policy recommendation is going to be.

So with that, we're still at 11. So I can say we have wrapped up on time. This has been a good discussion. I see some things we could tease out to start with

next week, both on this but also I think there's a lot of very logical segues in today's discussions to the other questions in (F).

And let me suggest, and I'm not sure that it's going to be very useful to follow (F) in order. We may want to some groupings. But we'll talk about that during the week. Thanks for your time and talk to you next week.

Man: Thanks Don.

Man: Thanks Don.

Woman: Thanks Don.

Woman: Thanks Don.

Man: Thank you.

Woman: Thanks everybody.

Man: Thank you.

Coordinator: Once again, the meeting has been adjourned. Please remember to disconnect all remaining lines. And thank you very much for joining.

END