ICANN Transcription
Privacy and Proxy Services Accreditation Issues PDP WG F2F meeting – Part 2
Friday 10 October 2014

Note: The following is the output of transcribing from an audio recording of Privacy and Proxy Services Accreditation Issues PDP WG F2F meeting on the Friday 10 October 2014. 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.
On page:
http://gnso.icann.org/calendar/#oct

Thomas Rickert: Can we get the recording started again please? It's already running? Excellent.

So welcome back, it's a little bit - we've paused three minutes later than we should have but let's get back straight to the discussion.

Okay, Don?

Don Blumenthal: I hate to channel back to my law professor days - not law professor, university professor days. But if folks could kind of focus on what we're doing here, we'd appreciate it. I mean when email starts to come to us unrelated to the meeting, it's just a little peculiar, so another request to kind of focus on what we're doing. We're providing breaks and whatever else or other stuff; appreciate it.

Thomas Rickert: Thanks Don.

So let's now discuss relay issues. And Marika, you have to help me out who we had told to - so Graeme, it's your turn.

And can I ask you, you know, just for the whole team, the idea was for Graeme to give us a very brief and high level introduction as to what the state of the discussion is so that we can then continue discussing very specific questions. Graeme.

Graeme Bunton: Thank you Thomas. This is Graeme Bunton for the transcript.

I appreciated being volunteered to do this last night about midnight when I got in, but it's not a big deal because I think - we don't have it on screen right now, but there was sent out a pretty good summary of where we were for Category E questions around relay. I'll just go through those questions right now so they're in our heads.

E-1 was what if any are the baseline minimum standardized relay processes that should be adopted by ICANN accredited privacy/proxy service providers.

E-2 was should ICANN accredited privacy/proxy service providers be required to forward to the customer all allegations of illegal activities they receive relating to specific domain names of the customer?

And we certainly bounced this topic around for quite awhile and we made some reasonable progress, and there's a couple of issues that are still outstanding. We'll get to that in a moment.

There was general agreement however amongst the group - and we discussed this a little bit earlier - that sort of all consensus policy emails, contact stuff for registrants would be forwarded. So those would all be relayed; I think we were all agreed on that.

We got to sort of - two places that we could agree that this might work and that was all communications required by - oh sorry, that's bad. There were sort of two options floated; forward all electronic requests received including emails and Web forms, but the provider may implement commercial reasonable safeguards to filter out spam and other forms of abusive communications. So in that scenario, a service provider is just forwarding everything with commercially reasonable safeguards.

And then the other one was that they forward all electronic requests and those received from law enforcement authorities and third parties containing allocations of domain name abuse. And that gave some flexibility for service providers to act how they would see fit within their business.

The big questions that we didn’t get to - and maybe not necessarily big but they are questions we didn’t get to - which was around physical mail and should service providers be required to forward physical documents. And as a part of that because of the cost incurred, should service providers be allowed to do some cost recovery on that.

And then there was one more which was - let me find it - if a provider chooses not to forward an allegation of illegal activity, should there be an obligation to inform the provider - or sorry, the requester the reasons that that request was not forwarded.

There was another question - I think is captured here and I’m not sure where we stood on this, but it might be worth discussing as well which was if the relay fails, are the service providers required to inform the requestor also.

So those are sort of the big questions that we have left to tackle.

Thomas Rickert: Excellent, thanks Graeme.

Graeme Bunton: Oh yes, you can see it on the Adobe Connect. This is a rather humorous example of what happens when you agree to forward physical communications. There is - this came in to our contact privacy service. One was a piece of satanic art and then a letter burned into a piece of wood. And the other was a, you know, communications written on a diaper. It was clean.

Man: Wait a minute, wait a minute. You get clean diapers?

Graeme Bunton: I guess it's probably that there's an interesting equivalent there to running probably like an actor agency where people send the craziest things to the actor's agents that they want to get there.

We get lots of interesting stuff to our contact privacy physical address, and so we just need to think about the whole breadth of interesting things that contact privacy providers might receive.

I don't think you want to know. There's fire, there's demons, it's - I mean I don't know that it's actually satanic; it's just, you know, has that impression.

Thomas Rickert: Thanks Graeme, that's been very helpful. James, you wanted to comment?

James Bladel: It looks like every bad 80's heavy metal album cover that I can remember.

So yes, I just wanted to mention - although Graeme's got some humorous things, maybe some less humorous things that we've received; complaints.

And we had a little contest at one point receiving complaints where we would see who could win by showing the complaint that was measured in pounds. And the winner was 19 pounds of paperwork in complaints.

So let's be mindful that when we say relay, we're not necessarily saying that I'm going to send a letter...

Paul Diaz: James, I'm sorry about that.

James Bladel: Don't apologize to me. I think (Barry Hill) won.

Thomas Rickert: That was Paul for the transcript.

James Bladel: But I think let's be mindful we're not talking about taking a letter and putting in a new envelope and sending it through. These are (edge) cases to be sure, but we certainly don't want to open the door to be ICANN obligations where someone can kill us with stamps, or more appropriately, kill us with UPS.

And I think that physical relay is important, particularly when we're talking about court documents or legal proceedings. But I think we need to also establish that that should not be free, and I don't think that a legitimate proceeding would really care about shipping costs.

David Hughes: So - but plus one on the second part. I think that if you've gone to the trouble to send court orders or something, paying for the additional - that's not the issue.

But I think the scenario that's most likely here is that somebody is going to contact the privacy and proxy service electronically. They are going to try to forward the electronic notice forward. If I'm wrong, please correct me.

It bounces back and then we make a request and say, "Can you please try to contact them physically." It seems to me that's the scenario that's most likely to occur.

I mean if from the sending side, if we can send a PDF electronically rather than a FedEx, I mean there may be legal obligations in some cases but we're going to send electronically if we can.

And I thought - maybe I misunderstood, but in this scenario, the ability to contact the registrant electronically failed so that we say, "Well please try to contact them physically, and if that costs you something we can discuss that cost."

Am I misunderstanding the scenario?

Thomas Rickert: I don't think so - it’s a toughie.

Kathy Kleiman: Can I ask a question? So you send a letter or an electronic notice. And are you asking - and this maybe too much detail. Are you asking the proxy/privacy provider then to print that out, put it in an envelope?

David Hughes: Well we’re asking them to forward it electronically, and then in the case where the electronic forwarding is not successful, we would ask them - assuming there’s - in some cases, there may be an obligation to have it forwarded if it’s a legal document depending on the territory. But in most cases I think what we’re saying is that if you try to contact them - if you try to forward this electronically and it failed, please try physically.

Kathy Kleiman: But you want the proxy/privacy provider to literally print out your message that failed electronically. Print it out...

((Crosstalk))

David Hughes: Yes, because we don't know, you know, clearly we don't know who to send it too; so yes.

Kathy Kleiman: Okay, so just trying to clarify. Thanks.

Thomas Rickert: Excuse my ignorance. I haven’t followed the whole discussion by the group so I might be entirely wrong. But I get the impression that we’re trying to fix something with this hard copy thing or, you know, post coming into the privacy and proxy service that’s being passed on that maybe we could otherwise resolve.

You know, I understand that the issues that you will move to hard copies whenever relay of electronic communication fails.

So wouldn't the remedy rather be looking at something, let's say, such as the EWG has suggested in its report to have a designated privacy and proxy contact to ensure that there is availability and that the privacy/proxy service can be reached in terms there are relay issues.

Steve, I'll get to you in a second. Because I would have thought when reading these questions in preparation for this meeting that it should be up to the privacy and proxy service provider to state in the Terms of Conditions whether or not they pass on incoming hard copies of correspondence or (unintelligible) or whatever it might be, and this close to their customers whether or not they're going to add an additional charge or not.

So if we're just focusing on the situation where relate hails, then we might address this otherwise in it.

Steve, please.

Steve Metalitz: Yes this is Steve Metalitz.

I'm not sure that you're understanding this Thomas because I think we're not talking about a situation where you can't reach the provider. We're talking about a situation where you reach the provider, ask the provider to forward something, and then that forwarding fails because the address given by the customer is in operative, for example.

In that case, two things should happen from our point of view. One, we should be told about it - and this was the add-on question I think that Graeme mentioned. Although I think it may be kind of covered implicitly by some of the stuff we've already decided.

And second, should we have the option at that point to say, “Okay, the address that you’ve been given by your customer is bogus or doesn’t work, but we would like you to print it out and forward it to the physical address that you’ve been given by your customer.”

That’s the scenario we’re talking about. So I’m not sure - this is assuming it’s something that is being forwarded under one of the two options that we’ve already agreed upon.

So it’s a forwardable piece of mail, it’s not succeeding in getting forwarded because the email address doesn't work so should those two things happen; one, complainant is notified, two, complainant is able to say, “Okay, now we want you to send it to the physical address to try to reach the customer.”

Michele Neylon: Thanks Thomas. Michele for the record.

Since you did mention the EWG, and as far as I know I’m the only person from the EWG in the room, just speaking to that briefly.

The entire kind of handling of proxy/privacy notifications, all that stuff, was something we spent in EWG a very long time discussing in fine detail trying to understand the challenges, you know, what people were trying to achieve, what the issues were in the current status quo.

And then once we kind of got past that - I mean one of the biggest problems we found, I mean being really honest, was that, you know, the conversations kind of went round in circles to a certain degree because people were kind of going, “Look, you know, this is what we’ve been trying to do, this is what we’re running into, this is the constant problem we face.”

And then trying to get past that to kind of go, “Okay, look, imagine a scenario in which the privacy/proxy providers have certain obligations that they cannot avoid. What would you like to see?” And then once we kind of got to that conversation, then a lot of issues that Steve and others would be speaking to would kind of disappear.

Because if the privacy/proxy provider has an obligation to send abuse reports through and to give some kind of level of - I'll be careful what word I use here, but let's say transparency probably isn't the best word - but giving them some kind of assurance to say that, "Okay, Steve Metalitz submitted a complaint to the provider at 9:01 am in time zone A. The provider relayed that through, and as far as the provider is concerned, that got sent through to the user."

Now their were certain limitations around this because ultimately, if you're doing it electronically, I could send you email to a valid email address or you could send me mail to a valid email address, there's absolutely no way of knowing whether or not I'm bothering to check that email. You know, the email address could be valid but I just don't read it.

So you know, there are certain kind of gotchas there that people can ignore emails; you can't force them to respond. But what you could do is set up a situation whereby the proxy/privacy provider, in the paradigm we put forward, would have this kind of dedicated contact point and have a process for ensuring that the stuff was being sent forward, sent on or delivered in some way.

But again, there is no way to force anybody to actually reply, which, you know, ultimately that can end up causing the problem where the complainant feels that it hasn't been delivered whereas it actually has been delivered; it's just that the person receiving it just isn't responding. And I don't think there's any simple solution to that one.

Thomas Rickert: Steve.

Steve Metalitz: Yes, Steve Metalitz.

Yes, this repeats almost verbatim a conversation, Michele, that we had two or three months ago in the working group, so let me just cut to the chase.

We're not talking about most of the scenarios you're talking about. We're talking about a situation like what is dealt with in the domain discreet DotCom terms of service. So they say if - when they forward an email to the address you listed, if the email address you listed becomes non-functioning or email to such address bounces, they're not going to try to contact you by any other means. That's the - we're drawing a line here between forwarding that's not responded to and a forwarding that doesn't go through.

And again, Alex and others are much more convergent in the technical details than I am. But I think there is a distinction that in the vast majority of cases can be made between those two scenarios.

The first scenario we're not suggesting there should be necessarily an obligation with regard to relay in that setting. But in the second scenario, we're suggesting that A, we be told; and B, we have the option of trying to get this material to the customer at another contact point that he/she or it has provided. Thank you.

Alex Deacon: So - Alex Deacon for the record.

Right, so I think it's important to think about kind of the scenarios when we try to reach out to an individual behind a privacy/proxy and we don't get a response. Maybe they choose not to, maybe it goes into a mailbox that they never check and that's fine.

I think in that scenario our organization would probably then follow-up with a physical communication and try that way, and if that didn't work we would, you know, there may be other means here.

But in the case where there is an indication that communication between the privacy/proxy provider and the registrant, their customer, fails, we'd like to know. And then I think at that point, there's also obligations Whois accuracy and so on which would also proceed.

So I think we're kind of on the same page. I don't see too much - you know, I think where we ended up, you know, three or four months ago is pretty well laid out in the conclusions - the preliminary conclusions that we came up with.

Thomas Rickert: And that's what I'm trying to drill down too, you know, where the differences still are.

Michele, you raised your hand.

Michele Neylon: Yes thanks. Michele for the record.

I think Steve is misunderstanding what I'm talking about at some level. What he is talking about it - unless I've misunderstood him completely - is that he's submitting a complaint using the email address that is available in public Whois. I'm not talking about that at all; I'm talking about submitting the complaint directly to the proxy/privacy provider in relation to a specific domain.

So the thing is this entire thing about email addresses that are valid, invalid, or whatever, is completely irrelevant. Because if you submit an abuse contact to us, for example, in relation to one of our clients, we can forward that complaint in some way to our client who's in the contact details that we have for them, which may or may not have any relevance or be in anyway linked to what is available in public Whois.

So you know, if for example if our privacy service, for example, rotates the email address on each domain every 24 hours or every 48 hours or whatever, it wouldn’t matter because you’re sending the complaint to the privacy/proxy abuse reporting contact which is completely separate.

So I don't understand...

David Hughes: No, we are talking about exactly the scenario you just said. We send it to you...

Michele Neylon: Yes.

David Hughes: ...and with a request to relay it on - to forward it on - and we don't care or know what address you’re sending it too.

Michele Neylon: Yes.

David Hughes: But if you send it and you don't hear back from them, we want to know so that we can send something else like a request for a physical delivery.

Michele Neylon: No but - okay. But I think we’re kind of going around in circles here. Because if we send the - okay, let me just...

David Hughes: If it bounces back.

Michele Neylon: Yes, hold on; hold on.

If I send a notice to one of my clients using whatever means of methods and contact points that I have, and it bounces and I’m aware of the bounce, then I would probably have to look at some way of sending it to an alternative address.

David Hughes: Yes, this is the scenario.

Michele Neylon: So I don't understand what the problem is. I mean if I have the obligation to do that...

Steve Metalitz: If you have the obligation to do that, then we’re fine.

Michele Neylon: Yes, okay. But...

David Hughes: Thank you; confused. This is David Hughes for the record saying thank you.

Michele Neylon: I’m confused now.

Thomas Rickert: Before I move to Kathy and then to Holly, I guess the disconnect between the two of you may be that you are looking for an address that you can provide service too. And if the privacy and proxy service provider...

Group: No, no, no.

David Hughes: No, we’re not asking - we’re just asking for him to forward whatever we sent to him to the address he has on record. This isn’t about reveal; this is just about relay.

Michele Neylon: Which I’m happy to do. I mean I don't see what the problem is.

David Hughes: Okay, so the discussion is over. Thank you.

Thomas Rickert: If the discussion is over, then I think we should note it.

Kathy and then Holly.

Kathy Kleiman: I think it’s still going on this side although it’s nice to see convergence.

First, I want to make sure that we don't ascribe to bouncing of some kind of negative or horrible or underground motive.

Just by analogy, I love trying to get on to my bank and doing my reconciliations on Saturday night at about midnight, and the system is almost always down. It doesn't mean the bank is down, it means they're doing their, you know, upgrades. And so, you know, that happens for everybody from time to time, so a bounce can just be the system is down. So let's not ascribe any motives to that.

But and also - and I think this has been consensus already that not responding to a threat or (cease) letters also is not, you know - in the real world, I can get a (cease) letter and choose not to respond.

But it seems like we're drilling down to specifically a bounce notice - and this is where I thought we got stuck last time. But if you've reconciled that it's fine, that if the proxy/privacy provider knows about a bounce, that then they should let - what you're asking is that they should let you know so that you can ask them to print it off, send it by hard copy, and I thought then we also got not stuck, but of the issue of cost. You know, is there a cost for that kind of time whether it's printing off one page or 20 pages or whatever.

So those were - I mean if I understand, then I think we know what the points are. And thank you.

Thomas Rickert: Please.

(Vicki): This is (Vicki) with the Recording Industry.

I think what David is talking about is when there's the initial delivery from the privacy/proxy server to the client, and the delivery doesn't go through; not whether or not the client responds but if the delivery doesn't go through. Does that end the inquiry or will the privacy/proxy try an alternative method to make the delivery.

And Michele just said that he would try the alternative method which we appreciate.

Michele Neylon: Well I mean yes, I mean that's - if we're talking hypothetically that this is what we have proposed, if you're contacting the privacy/proxy provider in much the same way as contacting our Abuse Desk, there's need from our perspective - I mean just speaking on behalf of my company, not speaking on behalf of anybody else.

You know, if you submit to us what we would consider to be a legitimate abuse report, we want to get that through to our client. Now, we've get plenty of illegitimate abuse reports; I just got one ten minutes ago where yet again some idiocies is trying to get us to comply with US law. Now I haven't told him where to shove his US law yet, but I probably will do if he replies we quoting the same legislation.

Thomas Rickert: James.

James Bladel: So I just want to emphasize first that Michele is probably going above and beyond what would be considered I think a minimum baseline into some other things that we could do, you know, as a value-add perhaps, but not necessarily include as part of the minimum baseline requirements.

I'd like to say bounce message might include a number of failed attempts within a certain timeframe so that we can weed out just singular sorts of issues like what Kathy was discussing so a single bounce doesn't trigger it. But let's say, you know, two failed/three failed attempts in a two-hour period or something like that. Who knows what the numbers are, but something like that. You know, X-failures in Y-window.

To Kathy's point, there is a cost associated with this. And you know, internally, we have a number; I don't want to say what it is. But whenever we get outside of a system that doesn't scale and can't be automated in code and we start getting into human beings that actually have to touch emails and print paper and stamp envelopes or whatever, then, you know, then that - I mean just because of the volumes and the speed that we're dealing with in this industry that that now incurs cost.

So my question is should there be a fee service attached to relay if there is, you know, a requirement to go outside of something that can be automated and go into a situation where we are providing hard copy or an evidentiary trail or something like that for the complainant. I think that's fair; I don't really feel like the complainant or the customer should be able to put that burden on the service provider.

Alex Deacon: So I just wanted to go back to the conversation that we had earlier and Michele's points around the difference between sending a request to the email address in the Whois system or directly to your abuse. Because I admit, I think when we talked about this two or three months ago, I think I missed that point.

So I just wanted to make sure we're all on the same page. I mean when - if we pop up a level and there is need to contact the registrant behind the privacy/proxy, usually what happens, at least in our organization as far as I understand it, is that we will look on the Web site to see if there is any identifying information - usually there is not.

The second thing we'll do is we'll look in Whois, and in the case of a privacy/proxy service, there's usually an email address and we will try to reach out to the registrant using that method.

And now, I think what Michele is saying is that if that fails - and when I use the word fails, if we don't get a response within some amount of time or we - if there's an indication that there is a hard bounce back to us, then the next part in this process would be that we would reach out to the privacy/proxy abuse contact.

Is that kind of the process that we're kind of thinking about and we have in mind here?

Michele Neylon: Yes, I think so. But I mean, okay, James has said - I mean there might be - because I'm just looking at it in terms of how that could work. I mean it could be a quick case of, you know, if you want - I mean one of the things we have discussed within the EWG was this idea of kind of a guaranteed delivery type concept of a complaint or a process or something like that.

And as James says, I mean the thing with all this when it comes to scale and everything else is there might be a cost associated with that. And we're not talking kind of like thousands of dollars or anything like that, but once you start getting into some of the more manual stuff, there might be something there.

But in terms of the process, I mean just from my perspective, you know, just relying on an email address that's in Whois to be something and then if for example the privacy/proxy service rotates that every few days, we all damn well in larger organizations, you know, by the time you start something and somebody else finishes it, you know, the time lapsed could be quite substantial.

I mean we've had UDRP verification requests where the domain name had been deleted for several months, so it no longer existed by the time we got the verification which was kind of amusing in a kind of oh-my-God sort of way.

Alex Deacon: Could I just ask a follow-up to that? So are you saying that the process should be - I mean this is totally one scale. But are you saying that the process should be to go directly to the abuse contact for the privacy/proxy service or should we use the email address in the Whois first?

Michele Neylon: I’m not saying anything. Look, what I was trying to do was trying to offer alternative routes to resolve an issue.

Okay, personally, as a service provider, I want you, globally, all of you, to resolve your issues with my clients with my clients; I do not want to be involved. I don't want to be the arbiter, I don't want to be the judge and jury, and I really - and you know, processing those complaints, as I say, some of them are dead easy; you read it, you go, “(Grammed), that’s fine.”

The Web site in question is distributing malware, it’s you know, child abuse material, it’s something where it’s clear-cut. Usually the word illegal can be complicated because you could argue that torrents are illegal or that a lot of other things are illegal where as that’s getting into copyright which is something we don't want to get involved with.

So if you can resolve all your issues directly with my clients, I’m a much happier camper, because unfortunately a lot of the complaints that do land on everybody’s desks are far from clear-cut.

I mean we’ve had situations with complaints where I think we had six backwards and forwards with a particular German company who were incapable of telling us what the hell the infringement was although they were very, very confident that there was one. They wouldn’t tell us what the trademark was or give us an example of what the hell the infringement was. It was just a massive bloody waste of time.

Whereas if they just dealt with our client, who by-the-way had published all their contact details on their Web site and wasn’t using proxy/privacy or anything like that, it would have been so much faster and easier.

So I mean I think, you know, the thing from my perspective is like ultimately, you know - no, I’m not going to reveal. If you can't get through using one method, then maybe another method should be available for you be that an abuse contact or some other kind of contact specifically for that purpose.

I mean the other thing is have a look at what Chris Pelling has been putting on the Adobe Chat about other aspects around the existing contract.

I mean ultimately, we are a small company; the volume of abuse tickets we would get and volume of UDRPs we handle, all that is timing. For a registrar the size of (unintelligible) of Go Daddy, the volumes and scales they are dealing with are completely different.

So I can speak to what I'm willing to do, but I don't want to end up in a situation where you take this back going, "Oh, all the registrars said X," where it's just I said it, not everybody else. Thanks.

Thomas Rickert: So I have Phil next and then I'd like to ask Mary or Marika to maybe sum up Chris's comments for the group.

Phil Corwin: I just have a couple of questions to make sure I understand what the general procedures are at registrars that operate these services.

Are most of the communications you're being asked to relay, aside from the diapers and the (unintelligible), but I'm assuming there's the outwires that the vast majority are received is email? Is that correct? So forwarding it is very - I wouldn't say no cost, but it's standing by saying, "Oh, we need to pass this on to this customer and we forward it with our standard, you know, communication that orders worked up pursuant to your agreement, you know. You've agreed not to do certain things and someone - we're passing this along, you know. Deal with the complainant, etcetera."

So it would only become a serious cost issue if it bounced back and then you have to get somebody to start chasing down the customer and trying to communicate.

Am I correct on that, that it’s a very not no but extremely low cost to operation if it comes in an email. Is that right, anyone? Registrars want to nod or - okay.

They’re nodding affirmation. By the way, Phil Corwin speaking.

Last question; does any registrar ever check to see that the registrant actually got it? Let’s say the registrant - let’s say the complainant is mistaken and the registrar would like to know that someone has a mistaken notion of what they’re doing with their Web site before it turns in to a UDRP or a court case or something like that.

Is there any like, you know - do you ever ask, you know, for a red acknowledgement for the registrant to let you know they got it to make sure it didn’t wind up in a junk field? Because every week, I get communication from clients and people I communicate with all the time, and suddenly they’re going to my junk filter, I don't know what happened, and I’ve got to correct it again. But that does happen; people have a valid email address and something is sent there from someone. It should go right through but some filter diverts it, and if they don't check those filters regularly they may not see it.

So if there’s ever any check to see that the registrant - if it doesn’t bounce back to see that the registrant actually received any request for acknowledgement.

Michele.

Michele Neylon: When I’m speaking about this, I’m speaking generally about abuse reports that we receive.

The way we handle it and this is, you know, for all types of abuse because ultimately the volume of abuse reports we get about our Whois privacy service is negligible. I mean I think we've probably had less than a half dozen ever, so you know, I just lump them all in with all the abuse reports we get of all types.

If the abuse we're dealing with is something which I could see as being in the kind of realm of abuse of the DNS, so, you know, malware fishing, that kind of thing, then we would probably follow up on it. If it's some kind of copyright thing then no.

Because I'd look at it in terms of, you know, that Web site being online probably hosted by us, distributing malware, just doing something like that, we would probably take the site offline because there would be a breach of our terms of service.

Whereas, you know, somebody sending us some kind of badly worded copyright complaint, we might not follow-up on it.

Phil Corwin: So that would be not follow-up to make sure the registrant customer got the relay, but following up by removing the domain if you think there is...

Michele Neylon: Well the way - look, we've had situations...

Phil Corwin: ...shown evidence that (unintelligible).

((Crosstalk))

Michele Neylon: Okay, we've had situations where clients have ignored communications from us.

Thomas Rickert: And Michele, can I suggest that you take this offline? Because I understand that you're not even asking for a confirmation of receipt, so I think this is more for your information Phil. So for the sake of saving time, maybe you could discuss this during the break.

And if relevant for this discussion, we can bring it back in. Is that okay?

Phil Corwin: It's okay except I think I would like the group to think about if we're going to require relay, whether there should be some requirement to make sure the registrant actually receives the communication. It that just assuming that if it doesn't bounce back, doesn't actually always mean that the registrant customer saw the communication.

Thomas Rickert: Understood. Mary, can I ask you to inform the group about Chris Pelling's comments in the chat?

Mary Wong: Sure Thomas. This is Mary Wong from ICANN Staff speaking for the transcript and the recording.

And (Chris's) point was really about the registrar obligations under the 2013 RAA. And Michele, you referred to that as well, that essentially in summary, if a registrar knows that there is an accurate contact information for a domain, it is in this an obligation including to verify, or reverify as the case may be, potentially to suspend. And his reference was 3.7.8 of the RAA accompanied by the Whois accuracy specification primarily Section 4 and maybe it was Section 5.

So I guess the overall question here is what is relevant? And Chris also notes that, at least in his case and perhaps in others as well, what they do is follow that to the letter. And they do, and I see some nods around the table as well that they do therefore actually get a response from the domain name holder is there actually is a suspension.

Thomas Rickert: Now I think that - Steve, please.

Steve Metalitz: Yes, thank you. This is Steve Metalitz for the transcript.

Two points; first, obviously the policy and the requirements of the different services are different, and a lot of this material has been compiled by the staff already. James' company obligates its contacts, its customers to reply, to respond to the DBP email, and if the correspondence involves a dispute of any kind. And if there's no response, they may immediately reveal the identity or cancel the private registration service, in other words publication. So that's how his company handles it and other companies may handle it differently.

I'm wondering if some of what we're talking about here can really be addressed by - if you go back one slide and look at the things we have already tentatively agreed on, one of them is that there would be a point of contact, published, for requestors to contact to follow-up on or escalate their original request. So that could raise a lot - I mean a lot of issues could be dealt with there.

For example, if there's been a bounce back. We think that the provider should tell us if there's been a bounce back, but this would at least provide a mechanism for finding that out.

If a service provider decides to follow Michele's example and when they get a bounce back, they proactively try another means of contacting the customer, that could also be communicated in that way.

Additionally, if you look, you know - one of our unresolved questions is we've agreed that providers aren't required to forward every single thing that they get as a relay request; there are some criteria. And this escalation point would be the way to find out if you haven't forwarded it at all.

In other words, we send in the request saying, "Please forward this. If you determine that it's not an allegation of domain name abuse," for example and you're working under Option 2, "then you should tell us." So then we would know it wasn't forwarded. Maybe we can revise our request or make it clearer or in some way bring it within your criteria.

So I think if this third point about a mechanism, a designated email point of contact to follow-up on or escalate original request, I think if that were flushed out a little bit about the types of issues it would handle, that might resolve really some of our open questions here, really most of them. It obviously wouldn't necessarily get into the fee issue for forwarding.

But I think a slightly more robust explanation of what this third point is that we've already agreed to might really help in this case. Thank you.

Thomas Rickert: Thanks Steve. I have Don next.

Don Blumenthal: Just a point of clarification. We've slowed back, unfortunately and understandably I think, we've slowed back back-and-forth between talking about proxy clients and registrants.

So taking off from what Steve said to the providers here, are you suggesting that you would not forward relay materials based on substance or were you talking about you would not do a takedown or some other adverse action based on whether it's DNS abuse or a poorly worded intellectual property issue? Is there any issue floating here about forwarding relay request based on their substance?

David Hughes: I feel like we've already addressed that.

Don Blumenthal: And I wasn't clear from something Steve just said there, so I just want to make sure.

Steve Metalitz: Well I was just referring - I'm sorry, this is Steve. I was just referring to what we already agreed too; that they can have one of two policies about what they forward beyond RAA ICANN consensus policy.

So some things won't meet that test. They may say, “Oh, this was caught in our spam filter.” I mean it shouldn’t have been maybe, but at least we should know that if we go escalate.

Thomas Rickert: Okay, can we maybe try to capture some interim results. Because we started off this discussion by having pictures of voodoo sculptures and diapers, and I think that that’s not what we’re actually discussing.

I think that what we’re discussing is...uh? Okay, so Michele would like to dive deeper into this diaper thing.

But - so I think what we’re talking about is communication that can also be conveyed electronically, so whether it be sculptures, diapers, anything that can only be transported by postal mail, that’s not what we’re discussing.

And for that, I guess it should be in the discretion of the privacy and proxy service provider to say whether or not they send on such communication and whether they want to attach a cost to it or not.

What we’re discussing is communication where establishing contact with the registrant or the beneficiary owner has failed. And in that instance, it’s my understanding that we should maybe try to jot down an approach whereby let’s say you as a requestor use the email communications channel.

And if you get let’s say three bounced within 48 hours, you would then stop trying to contact the registrant or beneficiary owner directly. But you would then go to the designated contact point saying, “We tried to contact the registrant, now it’s your deal, privacy/proxy service provider, to make that contact on and help us with this.”

Right? Steve.

Steve Metalitz: Well that's not exactly it. We start with using the address that's given for sending an email which may - I mean obviously different systems vary and some of them use Web forms; we talk about that in our conclusion. So you use the Web form; whatever the system is.

Thomas Rickert: Yes.

Steve Metalitz: Then it's opaque to us what happens after that. So if what happens after that is the bounce three times in 48 hours or whatever the right numbers are, then A, we want to know about that, and B, we want the option to ask that the material be sent through another means and through another contact point that the service provider has.

Again, that could all be handled through this designated point of contact, but there's some information that we need to know.

Thomas Rickert: You need some trigger point to escalate. And then the question to the registrant is would it be feasible for you to offer this?

They're using the Web form or the email address that they find for the domain name, they contact it, and it bounces without the requestor being notified of the bounce.

So can you strip that out and let the requestor know that let's say there have been three bounces in 48 hours? For then the requestor to be able to contact the designated contact point to escalate the matter.

Michele Neylon: I'm getting quite confused by what you're asking.

Like are you talking about somebody submitting contact - trying to contact the email address that's in the public Whois, or are you talking about them sending a request via some other means. So I'm confused by the question.

Thomas Rickert: Either the email address, which is typically converted to the real email address so it’s passed on, or the Web form.

Michele Neylon: Okay, so I’ve already answered that one. But this Web form thing I know nothing of so I’m not answering this one.

Thomas Rickert: Kathy.

Kathy Kleiman: So I think Steve’s summary, if I got it right, makes sense. So if it bounces a certain number of times within a certain period, then the accredited proxy/privacy provider would go to hard copy, and then I just add the word subject to a reasonable fee.

And we actually know - we probably know - attorneys in the room probably know a lot more about that reasonable fee because we deal with it. Every piece of paper we touch, everything that comes out of our copiers, everything that comes out of our fax machine has a specific cost attached to it in our law firms. And we charge reasonable fees for the copies for the faxes.

And so we’re probably not talking - you know, it’s actually - we may be able to take something from our world, the legal world, that may help the registrars think about how to process this because it’s not a concept that they have, but we do it all the time.

Thomas Rickert: But Kathy, maybe it’s just me but I, you know, now that you navigate us all to this discussion, I’d like to get clarity on your summary of Steve’s summary.

I think the issue Steve was that you as a requesting party don't get information on the bounces. So we need to work with the registrars of the privacy/proxy service providers to provide you with that information so that you can then escalate.

You're immediately jumping to another communication's channel i.e. hard copy versus electronic. And I think we should further work on staying electronic but just using another electronic channel before we talk about...

Kathy Kleiman: How many electronic channels are there?

Steve Metalitz: What electronic channel are you talking about?

Thomas Rickert: Well if you use the Web form or the email that you find in...

Steve Metalitz: You've already tried that; those have failed, those have bounced.

Thomas Rickert: But Michele has offered earlier that if he gets a notification to his abuse point of contact or the privacy/proxy point of contact that the EWG has suggested, then they would themselves try to make contact with the registrant, which I think would be good enough for you.

And if they can't make that contact...

Steve Metalitz: But that's not through an electronic means I don't think because we've tried the electronic means. I think he was talking about - I'm not sure what he was talking about.

Thomas Rickert: Well, they might have a different email address for the account holder which is not published in Whois. And so you could stay electronic but you would not try to approach the registrant, you would approach the privacy/proxy service provider or the registrar or whoever we use, and get what you need.

And in case they fail getting access to the account holder or the registrant, then they would invoke 3.81 and suspend.

David Hughes: Thomas, it's David Hughes.

I think there's an assumption here that is there is a contact address in Whois, and we send it to that, then the registrars converting that to the customer's email address and forwarding it on. So whether that goes through the abuse desk or whether it goes straight through, I don't think that makes a difference.

Michele Neylon: (Unintelligible).

David Hughes: Does it?

Michele Neylon: It does.

Thomas Rickert: I think it substantially does.

Michele Neylon: Yes.

Thomas Rickert: You are correct that some of these services manually take the information and then pass it on; others do that automatically. But I think the issue - and I may get things wrong. But I think this is opaque for you, as you call it, that's the issue, that you don't obtain that knowledge.

So we - I'm trying to learn from particularly the registrars whether the registrars are in a position to provide you with this intelligence after bounce has taken place to that you can then use the registrars of privacy/proxy service providers designated point of contact or the abuse point of contact as another alternative communication's channel so that they can take action.

Graeme.

Graeme Bunton: Sorry, I'll pop in briefly. This is Graeme for the transcript.

In a retail registrar or service provider scenario, they may well have contact information for the person who purchased the domain that is not the contact in Whois. And I think that's what we're getting at here.

So that, you know, emailing through the Web form or through the email address listed in the, you know, Whois, you know, that doesn't work three times in whatever period or however that is, then the service provider can then try that other contact information they have for the person who owns the domain name or who owns the account that owns the domain name.

I think that's what we were just getting towards, right.

Man: (Unintelligible).

Graeme Bunton: Right, so that we can stay electronic in that place, and we don't actually then have to go to physical mail.

Thomas Rickert: Correct. Steve? I think you're...

Graeme Bunton: Sorry, let me just very briefly, that that may not work in wholesale scenarios. That information may not exist for someone like (two cows) that doesn't have the relationship with the end user.

Thomas Rickert: Okay. Steve.

Steve Metalitz: That's fine. As I said, there's a variety of models and there could be different ways that electronic delivery is attempted. But when this fails, tell us, and give us the option of asking you to use another method. That's what we're seeking.

Thomas Rickert: David.

David Cake: I just wanted to have an attempt at summarizing what I think we're talking about is the procedure which is that we've all agreed. That, you know, there will be attempt at relaying via email, we all understand that that may bounce, and that we want there to be some way of being informed that that has actually bounced and actually failed. But we all understand that even in the case where it does go through, there's no way of guaranteeing that the email is being read.

Many people use proxy/privacy providers in order to minimize the amount of spam mail and they may, you know, there may be reasons why that they are not getting it. And at that point, the proxy/privacy provider may have other means of contacting the client possibly because they have, you know, more information about the customer than just the straight Whois record. Almost certainly they may, for example, also they can be able to find the customer or record, you know, and say read your email.

And then at that point, if those methods fail, we go to a point where we will want to relay paper mail and so on. And we all understand that there may be - there may be a need for some fees to be associated with that, and that is probably a proxy/privacy - why we want those to be reasonable, that's probably a proxy/privacy provider specific thing. Some may allow, you know, include some facility for relaying paper mail directly and the fee, some may only change if, you know, you wish to send a large satanic statue or something specifically like that to fully express you opinion.

So we're all - that's the scenario we've all basically agreed on. And our points of diffusion are really at which point - how exactly do we determine when bouncing has been sufficient that we can ask the proxy/privacy provider to use whatever other means they may have at their disposal. That's the sort of summary we're all roughly agreed with.

Michele Neylon: Thanks Thomas. My learned friend across the room has actually covered off some of what I was going to touch on.

Technically, there is a significant difference between somebody sending an email to an email address published in some form of Whois versus somebody contacting a help desk/support desk/abuse desk/service desk; call it what you will.

Depending on how mail servers operate and what they do and how your own mail server operates, I can send mail through. It will get relayed by our servers. You know, the receiving server on the far end, God only knows what he’s going to do with it. So I mean we might - there’s a big difference.

Whereas if you submit something to us via, you know, an abuse contact point or a support desk, then we know exactly what’s going on. We have a much better visibility on what’s going on and can contract things a lot more - well, how would I say - consistently, let’s just say.

Of course it’s not going to be perfect. Another stupid anecdote story for you where somebody submitted an abuse ticket to us and our abuse system sent out an acknowledgement to acknowledge the receipt of the abuse ticket. And the idiot then reported the acknowledgement back to our abuse desk.

This created a rather introducing circle of abuse tickets, but you can't say we weren’t responsive.

David Hughes: I think in response, just conceptually, maybe we’re talking about this cascade of you try it fails, you try it sells.

So electronic transmission to a fax, for example, if we’re going to do a use case scenario or something, that would be a logical thing to do. You have a fax, you’ve got a PDF, you forward it on, you don't have to print anything out. Maybe that’s - sort of that sort of logical progression of best efforts to get to the customer.

Thomas Rickert: Steve.

Steve Metalitz: Yes, I think David Cake really summarized this quite well about where we are. And I think, as I said, the two things we are looking for are to be aware when the electronic means provided by the provider is not working, and to be given an option to ask them to try another method using information they have and we don't, which is the other contact information for the customer.

Now the issue of fees has come up. And I think, to be honest, I think there are two sides to that question. At one level, I think for most cases, the fees would be fairly nominal.

I know if Paul has 19 pounds worth of paperwork, it might actually cost quite a bit to send that, but in most cases it’s going to be pretty nominal and it’s a cost that, you know, if we’re serious enough of trying to reach the customer, it makes sense.

On the other hand, you know, a privacy/proxy service provider is in business to provide a service, and the service is not just to hide the Whois data of the registrant. The service should be to provide a mechanism by which communications can be made to the customer. Yes, such as through relay.

And when that fails, I’m not quite sure why the cost of that should be imposed on the third party who is simply trying to get the provider’s service to do what it’s supposed to do. And if it fails to do it, and I agree it may not be the provider’s fault at all, but isn’t that just a cost of doing business for the provider. That if you have customers who give you bogus email addresses, maybe you have to absorb a little cost in order to fulfill your job which is, again, not just to hide the Whois data, your job is also to provide a channel for making these communications in appropriate circumstances.

So I think there’s kind of two sides to that argument. I think in most cases, it is not going to be a big deal. The costs are going to be fairly minimal, as Kathy said there are ways to calculate them. And I suppose if the costs were really absorbent, you could, you know, challenge that.

But I think there is another side to that story. Thank you.

Don Blumenthal: I think we should distinguish here between what the service is in business to do and what we may require them to do so that they can be in that business.

So yes, I mean privacy/proxy is there to shield what they've got to do in order to provide the service is another issue.

Thomas Rickert: Having listened to all of the arguments, I'm not sure whether we will easily reach consensus on an approach. I think the question is who has to pick up what costs and what communication channel should be available.

I have a question for David and Steve. For the communication with the customer to fail, you know, we have this reference that was made to 3.18 of the RAA whereby domain name is suspended. And as far as my experience is concerned, whenever you suspend a customer, they will wake up, right.

So wouldn't that be good enough mechanism for you to open the communication channel and invoke that? Or do we have to take the bouncing rule. I mean we could lean on what's in the RAA already for that purpose.

Kathy Kleiman: You're saying if there's bouncing then you're going to suspend?

Thomas Rickert: Not instantly, but if the established communication from the registrar to the registrant fails, then at some point in time they will have to suspend the domain name. Holly.

Holly Raiche: To elaborate or to perhaps to explain, I think what Chris Pelling was getting out is under the 2013 RAA, there is a requirement for the registrar to deal with accuracy issues.

Now if the beneficial users contact are proving to be inaccurate, I think at that point you start to say, “Well, we need to verify.” And that’s not so much a part of this discussion but it is relevant in saying if you’re dealing with something that’s inaccurate, then in fact you have some responsibilities quite far from this working group. And I think that’s where that comes in; that’s where the RAA comes in.

Thomas Rickert: But if there’s something in existence already in terms of process, then we might not need to duplicate it.

David Hughes: There are a couple of concerns. The 3.18 takes two weeks? Fifteen days, okay, so there may be a time issue. But the obligation of the end customer to provide accurate information is the underlying principle of the privacy/proxy setup.

So another idea - I’ll just throw it out there - is that if they haven’t provided their proxy service with accurate data, and we have to mail something to them, maybe you have to bill the customer. And maybe that’s their incentive for keeping their data accurate and responding in a timely manner; I don't know.

Steve Metalitz: This is Steve. Only to add that I don't think - I agree, 3.18.1, and as we’ve transferred that into the privacy/proxy setting is important and could be helpful. But because of the timing and because - let’s not assume that an answer to this problem is perfect compliance with another provision.

Not everybody is going to do that. Some people will just send it, it bounces, nothing else will happen. As long as they get paid, I can see a lot of privacy/proxy service providers just letting it lie.

And we don't know that it’s bounced so we can't go to ICANN, for example, and put in a Whois complaint. Or a complaint under the accreditation program in saying that they’re failing to act on this.

So I think the idea that there should be - and I agree that it could be this cascade. We should be made aware of the inability to reach the customer through the designated address and we should be given options for other means to reach them. Thank you.

Thomas Rickert: Thanks Steve. David.

David Cake: I just wanted to - I know this point was made, you know, a few weeks ago when we discussed this. But I just wanted to remind everybody that knowing whether or not an email has bounced is not necessarily a trivial technical thing to do. Email, (SMTP), setups are extremely complicated with, you know, backup service that may hold email for awhile and optional bounce messages. It's not always possible.

So we can sort of try but it is difficult. I'm just going to say it's technically complicated.

Thomas Rickert: Well we have six minutes left before the lunch break. And what I'm hearing is that there's a desire for cascaded approach when establishing communication or having email delivered to the customer fails.

I hear that there are difficulties with the setup with mail service some of which simply don't provide bounce notices so you wouldn't know, so even the registrar doesn't have the intelligence. We heard from Graeme that in the wholesale business that you have difficulties providing that information.

So can we link your request to the feasibility at the registrar side? Or are we talking about the...

David Hughes: I'm sorry Thomas. Can you just rephrase the question. I'm sorry.

Thomas Rickert: My question is your request to have this cascaded approach, is that something, you know, given the technical concerns that have been voiced, is that something that can be addressed by the registrant? So maybe we're talking about, you know, something that would be desirable but that's not feasible in technical terms.

And if that were the case given the various replies, then we'd need to think about different approaches.

Now I see a lot of hands going up. I think James was first and then I have Steve. Kathy? No - good.

James Bladel: So just to answer your question as directly as possible, we encountered this quite frequently during the development of the 2013 RAA which is reconciling what we want in the perfect world, let's say, with the technology that we have.

And I think that's why you see phrases like if provider becomes aware or commercially reasonable, or something along those lines, to allow for the fact that some systems won't send a bounce message or they won't send it in real time; there will be some delay. Or that, you know, that registrars may, you know, may not - or privacy providers may not have the kind of intelligence at their fingertips that make them omniscient to these types of things.

I think that what we'd like to see is providers take reasonable steps to implement commercially reasonable and practical approaches to address these problems while leaving them, let's say, that their head is not on the chopping block for failures of technology or for future advances in malware and bad actors that have found ways to get around these systems.

And I think that's kind of where we landed with the RAA, and I know it's a source of a lot of frustration for some folks because they believe that it should do things that it doesn't.

But I think that's kind of the middle ground or the bridges that we've had to try to build.

Thomas Rickert: Steve.

Steve Metalitz: This is Steve Metalitz. Maybe I'm just a perennial optimist. But I didn't actually hear that much about insoluble technical problems here compared to a lot of the other things we've been talking about, for example, in the transfer area.

And I'm generally in agreement with what James said. I think there are ways to phrase this so you're not required to do the impossible.

But the principle ought to be that if you know, and you can configure a system in a way so that you will generally know if the attempt to communicate has not gotten through, tell us and give us an option, another way to try to reach this party.

It's not to the exclusion of 3.18.1 and steps there, it's not to the exclusion of anything else. Not to the exclusion of trying on your own to do it. But tell us and give us an option. I don't think those are technical infeasible. Thank you.

Thomas Rickert: Thanks Steve. Kathy.

Kathy Kleiman: One thing I think we can add to the consensus which hasn't been mentioned yet is that there is probably a joint agreement or (mind) agreement that what the requestor wants to get to the registrant, the registrant wants to get as well. If there's a complaint against the registrant, we want to see it too as long as it's not spam, as long as it's not harassment, as long as it's not the 1300th time you've tried to tell me.

But Thomas, I think you sent us into a cliff on the suspension; you certainly woke me up with that.

If there is a process of the proxy/privacy provider communicating with the registrar that there's an issue with the underlying data and the validation verification, that's fine. But I don't - we didn't build that in; you mentioned that. So let's keep that - so kick that off, do whatever is under the RAA.

But what we were talking about here is alternative ways to reach the registrant which one can assume we'll probably be successful.

Thomas Rickert: It was not my suggestion to make it more difficult, but just to include into our thinking the mechanisms that are already there. You know...

Kathy Kleiman: But that's not a mechanism yet of the accredited proxy/privacy provider, that's a mechanism of the registrar.

Thomas Rickert: Yes, but if it's elsewhere such as RTP or other mechanisms that we do have, then we can lean on those. But your point is well heard, I will remain silent on that one.

Kathy Kleiman: But there's nothing wrong with starting both ports, but the idea is to get the message as quickly as possible relayed I think.

Thomas Rickert: Understood.

We only have 30 seconds left in this session. I would like to suggest to you, Marika, and then Mary has started writing up a little summary of our discussion in the Chat which I will ask her to read out to us. Maybe we can take that with us as an interim result and maybe take a few minutes of the next session after the break to draw the line under this discussion.

Marika Konings: This is Marika. I don't necessarily want to open a can of worms in this last 30 seconds, but you know, to Kathy's point and as well to the point you raise on suspension, and that follows indeed as I understand from Chris the requirement in the 2013 RAA, we do recommend in one of our preliminary recommendations that the same validation requirements apply to privacy/proxy service providers as to registrars in 2013 RAA.

So that seems implicit that indeed, that suspension, that would also be part of those requirements as I understand it. So I think that's already something that's currently in our recommendations relating to, you know, validation or verification of privacy/proxy customers by privacy/proxy services as I understand it.

Thomas Rickert: Thanks Marika. Mary?

Mary Wong: Thanks Thomas. Mary Wong again from ICANN Staff for the record.

So in an attempt to not just summarize but to also provide this sort of food for thought that Thomas eluded too, also noting that there were certain caveats and cautions that were expressed, the sentence that I've written here in the notes part attempts to provide that summary and to provide some food-for-thoughts as I said. So I'll just read it for those who are not in Adobe.

A privacy or proxy service provider should be obliged to forward a hard copy or other alterative form of notice upon becoming aware that the original form of electronic communication was undeliverable only when there has been a certain minimum number of hard bounces within a certain specified timeframe - obviously TBD there.

The provider should have the ability to select the most appropriate means of forwarding including to account for issues of cost.

And the last part I put in square brackets because there still seems to be some discussion about it, and that last part is and to charge a reasonable fee.

Thomas Rickert: So I think we should take that with us. I don't want to cut into the lunch break. But I think some of the basic ideas are in there. I think we need to further refine the language but that will be maybe an incremental approach that we could further work on.

We have doors there that we can open, we have food there which we can take through the doors and eat outside. Okay?

So I'll see you all back at 14 hours to restart our conversation. Thanks.

END