ICANN Transcription
Privacy and Proxy Services Accreditation Issues PDP WG
Tuesday 15 July 2014 at 1400 UTC

Note: The following is the output of transcribing from an audio recording of Privacy and Proxy Services Accreditation Issues PDP WG call on the Tuesday 15 July 2014 at 14:00 UTC. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record.
The audio is also available at:
http://audio.icann.org/gnso/gnso-ppsa-20140715-en.mp3
On page:
http://gnso.icann.org/calendar/#july

Attendees:
Steve Metalitz - IPC
Justin Macy – BC
Sarah Wyld - RrSG
Chris Pelling – RrSG
Darcy Southwell - RrSG
Graeme Bunton – RrSG
Don Blumenthal – RySG
Val Sherman – IPC
Griffin Barnett – IPC
Susan Kawaguchi – BC
Kathy Kleiman – NCUC
Stephanie Perrin – NCSG
James Bladel – RrSG
David Hea sley – IPC
Alex Deacon - IPC
Jim Bikoff – IPC
Osvaldo Novoa – ISPCP
Kristina Rosette – IPC
Paul McGrady – IPC
Carlton Samuels – ALAC
Todd Williams – IPC
Dan Burke – Individual
Laura Jedeed – BC
Chris Chaplow – BC
Libby Baney – BC
Tim Ruiz - RrSG
Christian Dawson - ISPCP

Apologies:
Susan Prosser- RrSG
Michele Neylon – RrSG
Holly Raiche - ALAC

ICANN staff:
Marika Konings
Mary Wong
Nathalie Peregrine

Nathalie Peregrine: Thank you very much (Andre). Good morning, good afternoon, good evening everybody and welcome to the PPSAI Working Group Call on the 15th of July, 2014.

On the call today we have Steve Metalitz, Griffin Barnett, Chris Pelling, Dan Burke, Laura Jedeed, Darcy Southwell, Graeme Bunton, James Bladel, Todd Williams, Don Blumenthal, Justin Macy, Kathy Kleinman, Sarah Wylde, Libby Baney, Kristina Rosette, Jim Bikoff, Tim Ruiz,, and (Val Sherman). We received apologies from Michele Neylon, Holly Raiche and Susan Prosser. From staff we have Marika Konings, Mary Wong and myself, Nathalie Peregrine.

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

Don Blumenthal: I appreciate it Nathalie. I just heard from Michele. He's in Madrid airport and he doesn't want to end his vacation on a PPSAI call.

Okay. We decided to at least start with D4. I'm not sure how much we still have to talk about there, but I've been feeling that at least something was still hanging the last time, maybe a little bit undefinable. You know, we had hoped to be a little more (unintelligible) on the email list about that or anything else. I hope it's not just post-ICANN doldrums (unintelligible) we've gotten a lot of good work done on the email list. Steve?

Steve Metalitz: Yes this is Steve. I think you had asked - someone - you or the staff had asked on the list if anybody had specific items that they thought were essential elements of any abuse notice and I don't think anybody responded to that. So it may be that we can deal with these as we get into relay and reveal. Thanks.

Don Blumenthal: Thanks. Kathy?

Kathy Kleinman: This is Kathy. I don't...

Don Blumenthal: Before you start can I ask that people who aren't speaking go on mute please? Your turn.

Kathy Kleinman: Good idea. I don't think it's post-ICANN doldrums. I think it's post-ICANN catching up with everything else. But I think we should - we're probably ready to move on, you know, my personal opinion is we're probably ready to move on from this one. There may be a few small edits that people send, including me, things that I had offered in the past but didn't have a chance to send out already. I think we're pretty close here. So thank you.

Don Blumenthal: Okay. Yes that's a good point: post-ICANN catch up or in some cases including mine post-ICANN vacation catch up which has been really ugly this time.

Okay then why don't we move on to E. We're getting into relay and reveal starting with relay. And we've set aside a few weeks for this because I think it's - no I don't think, I know there's going to be a lot of discussion in both areas, both templates.

We're going to start with E1. I would be surprised if we get through it today but if we do E2 is keyed up and I know that it was sent out. We have a couple of models - well not models but we have a couple of things to work with as we go along. We - or to get started with. In E3 we had some discussion about our forwarding messages - any messages under requirements of the RAA or development processes.

The EWG report has some interesting thoughts. Now obviously the EWG is not a mandate because who knows what's going to happen with it as the process is continued. But the fact is there's some good ideas that we could adopt regardless of whether the paper itself proceeds.

Given that - well let me just ask right off. Since we did develop the text in B3, if I can ask any of the folks who are familiar with the registrar (unintelligible) if there's anything in there that might apply to relay in the context that we're discussing it here.

Okay? I guess not. We'll send that language around this week for review. And - actually maybe I can just read it quickly. There's not much to it. So it was, "All privacy proxy services must relay any notices required on the RAA or ICANN consensus policy. All registration agreements must state customer's rights and responsibilities and the provider's services obligations in managing those rights and responsibilities."

You know, there's a qualifier there that specifically just comes up in the context that they - domain name transfer. But I guess we could work with this language for our purposes as we go along. Steve?

Steve Metalitz: Yes this is Steve Metalitz. I think one thing that's useful input here and that was included in this template that's on the screen now is the sample of the terms and conditions of current privacy and proxy services as collected by the staff. I think we asked them to do this back in the spring I think.

And if you look through that it seems like there's three main areas again dealing with relaying emails. Some relay all emails to the customer either because there's an actual relay or there's an email address that's affiliated with the - or associated with the customer that appears in Whois.

Some do some type of spam filtering or filtering of unsolicited communications. The wording varies. And then some give the customer the option of whether they want to be - to have everything forwarded, to have some filtered forwarding, or to have nothing forwarded which I thought that last option was kind of unusual.

Those seem to be the three basic approaches and, you know, the IPC as you know from our provisional responses thinks that any bona fide queries that come in should be forwarded. But I'm kind of interested to know how registrars that do some type of filtering, you know, how they do that because we've noted that there may need to be some safeguards against abuse like a CAPTCHA requirement or something.

So there obviously is a risk that if you forward everything it becomes very burdensome for the customer and in fact bona fide queries, bona fide issues could get lost in that. So I'm interested to know how those registrars that say that they do filter what they forward how they do so. And I think looking through this GoDaddy is one domains by proxy. Domain Discreet seems to be one. This used to be a filtering option in some of the others.

So anyway I'd be - I think that may be a worthwhile point to pursue but in the absence of that again our position is that everything, you know, that there should be an automatic relay. Thanks.

Don Blumenthal: Yes. And as (Tim) points out in the chat, you know, there's going to be certain policies that apply (unintelligible) registrar in general and what we - my suggestion's necessary, you know, proxy privacy setting and we may also look at existing proxy privacy practices and suggest that some of them really aren't acceptable once we come to mandatory requirements.

You know, I'm kind of following the chat. Wish people would step up to the mic.

(Graham Buntan): I'll step up there briefly then. This is (Graham) for the transcript.

Don Blumenthal: Okay.

(Graham Buntan): Contact privacy which is the (unintelligible) affiliated service doesn't do any filtering. But what we do do is force people who want to communicate with our customers that they have to use a Web form by the contact privacy Web site and that has a CAPTCHA on it. And I think that is a - so far a reasonable mechanism that we found to reduce the sort of spam and other crap that goes through there.

Don Blumenthal: And I appreciate it. Hear from one of your competitors here. James?

James Bladel: Hi Don. James speaking for the transcript. And probably not as familiar with the specifics of how our filtering would work. I know that it is somewhat customizable. But speaking just in the abstract of a proxy service that is affiliated with a registrar I think there's a number of ways that you can approach this. And I think one way is to design the service and the terms of service around what will and will not be relayed and what sorts of communications or operations on the domain name that the proxy service will take on behalf of the customer.

So for example if the proxy service by design rejects transfer requests then it would never relay a transfer request form of authorization because that is defined in the proxy service as one of the benefits of the service is that it protects against, you know, unsolicited transfer requests.

And I think you could possibly say the same thing about renewals which is another ICANN required message. If renewals are provided on behalf of registrar that it will automatically renew then the renewal notifications are not relayed because they are received by the proxy service and then the renewal is executed. So that's, I mean, that's another way to approach it.

I don't know - and I should just again caution the idea that I have to take a closer look at exactly what we do and what is customizable, if you can set or unset these services. I’m not really clear on that part. But I just am speaking more in the generic sense here that that could be part of the service offerings.

Don Blumenthal: Kathy?

Kathy Kleinman: Sorry. Coming off mute. So lots - this is really interesting to hear from (Graham) and James. Let me throw out some of the questions that I have. Kind of outside the proxy privacy world occasionally I’ll get six phone calls that come into my home phone. And it’s somebody - it could be a mistake, it could be real but somebody thinks they want something from me and they call once a day, twice a day, five times a day and, you know, getting rid of them is hard.

When that kind of abuse happens how is that handled by proxy privacy service providers currently and how do we think it should be handled? Kind of what are the boundaries that as a community we think? Do we pass on everything? Do we pass on things up to, you know, five times or ten times?

The other question I have is domain name sales: somebody really wants to buy my domain name and it’s proxied (sic). Do all proxy privacy service providers pass on that inquiry and how many times? Will you pass it on 500 times? So all sorts of questions about boundaries and when things go too far. Thanks.

Don Blumenthal: Okay and before going to Steve I want to point out Carlton’s question in the chat. As we’re discussing this keep in mind that, you know, I think sometimes this gets lost in the - when we talk generally or just look at the templates. The specific question that we’re asking in E relates to relay of complaints. So just keeping that in mind as we focus our discussion because as Carlton said, you know, are we talking about legal proceedings and the extent to which the judgment of the privacy proxy provider has? End of discussion and do they have limits on judgment or not?

I hope that came out out clearly. I'm doing a realigned and I'm not quite sure. Steve?

Steve Metalitz: Yes. This is Steve. I don't have answers to the questions that Kathy posed. So I'll defer to James who may have answers to some of them.

But I think your - I agree with your point Don, that the focus here is on when there are complaints about the types of abuse that we have an, you know, we have kind of an indicative list of abuses. I think all those should be forwarded. I'm certainly comfortable with the idea that there would be some safeguards in place as Graham said for, you know, a CAPTCHA or as a, you know, some type of spam filtering. In principle I don't have a problem with that.

But any time there's actually a complaint relating to the types of activities that are subject to abuse reporting then I think that really needs to be forwarded very promptly. I think it's only in fairness to the customer as well as to the complainant to note if there's that issue there. Thank you.

Don Blumenthal: Okay. Sorry. I was making a note to myself. James?

James Bladel: Thanks Don. James speaking and just kind of building on the comments made by Steve and by Kathy. You know, I think that we - and I think this is what Kathy was getting at as far as boundaries or, you know, categories of, you know, I think that the answer is is it's very difficult to say in a general case as part of an accreditation program is there going to be this black and white line of, you know, what is relayed and what isn't? I mean, certainly you don't want to relay everything. That defeats the purpose of having this service to begin with.

And so then the question becomes what types of - what is the nature of the complaint and who is raising the complaint? Certain if the complaint is that somebody won't buy my product or give me a job or sell me the domain name then I would want the privacy service to block that. If it's a spurious or harassing complaint, you know, there should be some mechanism, you know, as we're talking about the potential for abuse and there should be some mechanism to discriminate against those types of complaints versus legitimate, you know, complaints that are either originating from law enforcement - appropriate law enforcement I should say or something like the UDRP or other proceeding.

I don't think that we should - I think it's going to be - I think this is harder than it seems. I don't know that we can bake in the degree of certainty that I think some may want to see out of this. It may end up saying something like, you know, the services require to relay well founded complaints from legitimate authorities or something, you know, squishy language like that because I think there's just so many avenues for creating gray areas there that would be abuse.

Don Blumenthal: Again we don't say on the call what I agree with or don't agree with but I'm not sure I ever thought this was going to be easy. (Susan)?

(Susan): Hi. So I send probably 100 to 150 enforcement emails a month to proxy registration. So our practice is to not ask for a reveal just because they've registered a domain name and/or may be using it. But we go ahead and we send the enforcement. So when somebody's registered something with Facebook in it, you know, after we've made the decision that this is infringing, it's not fair use then we send it directly to the email address of record on the domain registration.

So, you know, 125, 150 emails a month you would think the proxy service provider wouldn't want to get in the middle of that and have to, you know, review or distinguish, you know, what - this email from a spam email. There's great spam filters out there. So, you know, with our own domain@sd.com then it - which I use for all of the - or most of the Facebook portfolio, you know, I respond to it where - I get about 500 emails a day which I review every day. But we have spam filters in place. So there’s a lot of things that are not - that don’t come through but we make sure that all the registry and all the renewals and all the, you know, that type of important emails do come through.

So back to the 150 emails a month just from one company, I would think, you know, for - if it wasn’t a sensitive automatic system that goes straight to the - well the licensee I guess is truly the term for it. And then that puts a bigger burden on the proxy service who’s providing - could be providing the service for free or they’re usually extremely low cost for what you get.

So I think there should be some freedom in allowing the proxy service just to go ahead and send that all through. I do not think a licensee should say, “I don’t want any emails.”

And on the flip side of that I probably request a reveal - we may be - it varies but I don’t think I’ve requested a reveal of contact information from more than like 25 domain names in a month. This month it was one so far. And just to note GoDaddy’s the only - or (unintelligible) by proxy is the only reliable source that I have at a least to get that contact information. So and - but it’s a prescribed procedure and you have to attest to the trademark and, you know, there’s a lot involved in it.

So I think we shouldn’t, you know, blame spam and all these unusual circumstances. Those can be blocked. The industry has figured that out. But we do have a responsibility to receive emails as admin contact for a domain registration. But then waive that on the burden that it puts on a proxy service and what you’re paying for the proxy service.

Don Blumenthal: Thanks. That leads to a number of follow-up questions. The first of which: what kind of a bitcoin transfer happened in the background before your statement about GoDaddy?

(Susan): Oh no. This is true.

Don Blumenthal: Okay. Fair enough. I just saw James' reaction in the chat.

I do have two follow ups though that was interesting from the reveal requester perspective. I mean, to what extent - somebody mentioned that part of the fact they're in and looking at request for reveal is who's asking that. So one question would be how much of that did you recognize to - is going to help lessen the burden, lessen the review burden on a provider? And the other one is, you know, in general is is the question we're looking at deals with processes rather than the specifics.

What are the difficulties - no. What problems do we raise if for example you're using a spam filter and you miss a legitimate complaint because of false positives? Should there be any limits on even using spam filters or some limits in our processes concerning requirements to check to scan filters to make sure that legitimate reveal requests don't get missed? (Unintelligible)...

(Susan): Yes if you're asking - oh okay. Go ahead.

Don Blumenthal: Oh no. Go ahead. Go ahead please.

(Susan): Yes I, you know, in my experience of managing large corporate portfolios, you know, our spam filters - as long as I work very closely with my team - and yes I have a lot of resources. But as long as I work very closely with the team I don't miss things. I can't even think of an instance where we lost a domain per renewal or something.

Now there's other mechanisms involved. I have a registrar and I have outside counsel. I'm saying I have a lot of resources. I'm not saying that every registrant that uses the proxy has that. But they probably only have a few domain names and simply log in to your registrar account and check things. That's your responsibility as a domain registrar.

So, you know, my experience is that the spam filters work well. It weeds things out. When I get those 500 emails from the same source then I just put them on the no, you know, I put them in the junk folder and then they go away and it adds to the spam filter. So I think the spam filters work well today. Did they work really well ten years ago? No I don't think so.

And so I think there's other mechanisms. And I'm not saying that every registrant or a licensee should be, you know, just inundated with email. But I think there's lots of ways of preventing that nowadays and getting those important legal notices, it should be something that's allowed and it should not be allowed that a proxy service provider is not forwarded anything. I think that in my opinion it would take them to the level of yes they truly are the registrant and they are accepting all responsibility for what's the content of the Web site then.

Don Blumenthal: Okay. Well for what it's worth our spam filter once blocked something to me from Steve Crocker. So I'm not just saying (unintelligible). (David)?

(David): Yes. This, I mean, I think this question about the spam filter really brings up that I find this issue quite odd in that where there's no way proxy or privacy accreditors consider it or not that we can guarantee anyone will read anything or will have any control over how they filter or, you know, with their comment we can sort of say that if they, you know, we send something to someone and it falls in their spam filter and they don't read it that then that is, you know, their problem.

But we seem to be wanting to control something in the proxy privacy accreditation that we can't actually control otherwise. So I'm, I mean I think whatever recommendation we make it will be - it seems a little redundant - I find it very - I mean I find it - I am sympathetic with the general point that of course you don't want proxy privacy passing on - not passing on their consent to that but they would not pass on things that are important but, yes, there is no guarantee that AMON Systems generally will not hide it from people in some way.

So it is how much can - how much should we be trying to even control this inside proxy and privacy (accredities) when we can't control it in the general case is the real question and that is all, thanks.

Don Blumenthal: Okay, fair enough and James.

James Bladel: Hi, Don, James speaking and I find myself agreeing fairly enthusiastically, not only with what (David) is saying but what (Susan) is saying as well. I think that, you know, a responsible service provider cannot take a position that they will relay nothing and that we should start perhaps by putting some boundaries around this issue with, you know, those - as I believe we have with those notifications that are required or mandated as part of ICANN processes.

So if a registrar is required to send those messages to the registrant as part of the RAA or consensus policy then the service provider should be required to relay those. And I think that, you know, beyond that - and that includes UDRP and legal law enforcement - I mean all of that space into the RAA and so that would extend - that umbrella would extend out to the service provider.

And I think that beyond that then the service provider as (Susan) noted, you know should be free to innovate as far as coming up with spam filters and captious and anything to cut down on spurious or abuses or just overall spamming type communications.

And then, just to, you know, hit on what (David) said once again, you know, we also address this issue not only in the RAA but also in a number of policy development efforts is that e-mail is not a perfect system, it is not reliable. You can guarantee that something was sent but you cannot guarantee it was read - received, read or acted upon. There is just way to many variables that could, you know, interfere in that.

So I would caution against any work in this group that tries to, you know, control outcomes of sending emails and really focus more on did the service provider do their - perform under their obligations by transmitting these notifications and messages and relay and not necessarily put them on the hook for what comes after that because as (David) said, this is not something that we figured out how to control outside of ICANN policy so it is certainly not something that can be solved inside of it.

And, you know, I think the goal here overall is to make sure that the responsible actors continue to act responsibly and perhaps, you know, in a more uniform manner and that the irresponsible actors either clean up their acts or get out of this space and I think that, you know, that should be the goal here rather than attempting to prescriptively define every possible type of - or category and every outcome scenario. I think we should just put some basic guidelines in place like we have in the RAA consensus policies. Thanks.

(Griffin): Hi Don this is (Griffin) can I get in the queue?

Don Blumenthal: Well there is nobody there right now so sure.

(Griffin): I am not in front of my computer so I can’t see if there is somebody with their hand up.

Don Blumenthal: (Unintelligible) on.

(Griffin): I just want to...

Don Blumenthal: No, no, I appreciate that and nobody does, no - go ahead.

(Griffin): I just to agree with a lot of the points that James just made and just to say I think we don't want to lose sight of the point that the basic goal here is to protect the customer's identity from being revealed and who is and I think spam - well I think it is an important sort of secondary privacy aspect, it is maybe not the primary one and I would agree that there should probably be some type of presumption that all communication is forwarded for exactly the reasons James sort of just laid out and I think one way of doing that, as I think (Graham) mentioned earlier is to use sort of a Web form with some sort of CAPTCHA or something like that to at least help prevent sort of basic spam from getting through. Thanks.

Don Blumenthal: Appreciate it. Any other thoughts on the strings we have been going? Okay, I think except for the concept of the Web form what we have been looking at as potential bad ideas and don't think my throwing something out is - meaning I think it was a good idea. Those - I generally agree with the statements about the spam thought or spam - sorry that - about that or whether (unintelligible) what a provider can do with (unintelligible) spam system make any sense or not.

What I would like to look at (unintelligible) I will finish this thought. What I would like to look at is what kind of processes can we require - again this is a question as at a minimum? Steve.

Steve Metalitz: Yes, thank you - this is Steven. I think what I have to say fits right in with what you just said. These are - what we are after here are minimum standards. Obviously a provider could choose to do more and your point about, you know, whether you take into account the source of the complaint that could certainly be factored in here but as far as a minim standard beyond the question of should the presumption be that it will be forwarded and I feel strongly that it should be subject to reasonable safeguards, including spam filter.

There are some other issues that we probably ought to talk about in terms of possible minimum standards. One is the timing, how quickly should the material - should the complaint - again our focus here is on complaints of abuse - how quickly should it be required to have the complaint relayed and recognizing that, you know, we do not have any ability to control whether the customer will ever read the relayed message, should there be some requirement in terms of the number of complaints. If the complaint about an abuse is relayed 'X" number of times and there has been no response is that a basis for moving to reveal or to requesting a reveal.

So that would be another aspect of I think what we are being asked to look at here with regard to relay - one is the timing and the other is what is the impact of repetitive requests that are not responded to or not acknowledged - thanks.

Don Blumenthal: Let me just toss something out that is a sub-point maybe that is (unintelligible) should there be any obligation in the privacy of (unintelligible) to follow up if there is no response - question, not necessarily a statement of support.

And then as Chris points out how does whole - how do automatic relay systems - we should keep automatic relay systems in mind as we discuss these processes?

Steve Metalitz: Well this is Steve - I could just respond...

Don Blumenthal: (Unintelligible).

Steve Metalitz: ...that kind of mutes the question of the timing because it is forwarded automatically but obviously not every - not - it is not necessarily the case that every provider will do that so that is where a time frame might come in.

Don Blumenthal: Okay, appreciate it. Who is that - no, is somebody trying to jump in or? Okay, I guess not.

When we are talking about the standardized relay process how much should we be focusing on, say intake as to out - as opposed to output? Should we have some kind of minimum requirements concerning how information should be gathered? What information should be - I will just continue even though I see the hole in what I am saying. What kind of information should be gathered, how - what kind of system should be there in terms of data entry, if any - what kind of system should be there in - for forwarding - should we require any kind of - again, where it is standardized - what are we going to mandate or not mandate - Kathy?

Kathy Kleinman: Good questions Don. I am concerned about requiring answers and I am concerned about talking about reveal based on the number of relayed messages that get passed to a registrant or to a licensee.

From a human rights perspective let's - I just wanted to share from the perspective of human rights organizations that might be receiving some of these things. Just because there are a number of allegations of illegality, no, you are not allowed to be posting that prodemocracy material certainly does not lead to the conclusion that whoever is behind that human rights group should be revealed just because the Chinese government has sent 500 inquiries. That doesn't follow - I mean that is a complete break of logic to me. I can see it in some situations but there is a lot of situations that will raise concerns then.

The other is the concept of requiring an answer. Certainly as a lawyer I get inquiries on behalf of my clients. Let just deal with the trademark cease and desist letters and when I get those cease and desist letters and they come in paper, and they come on letterhead we have three choices. We can, you know, we can respond, we cannot respond and actually two choices, we can respond or not respond and when we respond we can say we agree or we can say, no, you are completely crazy but that ability to not respond - if it is completely frivolous or it is a waste of our time or it is kind of a crazy allegation and certainly that is an option that many lawyers do on behalf of their clients, they just don't respond.

So I think we, you know, so from the registrant perspective I raise some of these concerns - thanks.

Don Blumenthal: I appreciate it - (Susan).

(Susan): So I completely agree with Kathy. I don't think you have a burden as a registrant to respond. I think you have a burden to receive an email but if I was to respond to those 500 emails a day that I receive for Facebook, you know, I would be spending a good portion of my day responding. Most, you know 99% I don't respond and we don't take action on and, you know, I do if it is a DNCA allegation then that gets forwarded to somebody else for response.

I don't think it would be harmful to allow someone requesting a reveal to say these are my, you know, - this is my trademark or this is the reason I am asking for the actual contact information of the licensee and I, you know, I have attempted to contact them on ten occasions, you know, here are the dates, here is copies of the email and they haven't responded but to make the burden of a response or even tracking that response the proxy provider is just - I mean what do you want for $9.99 a year, you know, I mean that is a lot to ask.

So, you know, I completely agree that the response should not be factored in on the proxy. The relay that, you know that I am not even sure you could confirm somebody got in the email. You definitely cannot confirm that they have read the email but knowing it has been relayed and you have sort of put them on notice is in my mind is what is important.

Don Blumenthal: Okay, all right, nobody is in the queue I am going to ask two more questions. Steve, I think - somebody said something about repeated failures to respond, however that is documented might need to reveal and I just want to log that for consideration during the (unintelligible). Are we going to have some reveal requirements later where it is a penalty for not acting as opposed to something that is really necessary in terms of what the relay request was?

Okay, now it is time to vamp for the second one.

Woman: So Don I would just want to interject something there. I would not be comfortable with making it the - making it a requirement to actually contact the licensee or attempt to contact the licensee prior to being able to ask for a reveal because there is so many situations where we need that contact information and we do not want to contact them first. You know, we do not want to give them a heads up that we are looking at them and a lot of times that - because it is, you know, some sort of a malware issue that isn't clearly something that we could have, you know, report to their hosting provider, some ad ask where they are collecting log-in information and so to make the - make it is part of the reveal request that you have to attempt to contact them I would be uncomfortable with.

I think it is a good practice - why bother the proxy service if you don't have to but I don't - I would be really uncomfortable with it being part of the actual process.

Don Blumenthal: Okay, thanks. When we keep focusing on emails should we talk about other forms of - the kinds of process for reveal or is, you know, somebody calls in the PIR for example - I mean not a practicing but some - what if somebody tries to call (unintelligible) abuse and reaches us by phone should that -

should we even act on that or should the proxy privacy provider say, “Send it to us in email?” Okay - now - yes, it is a relay question. What if I get a - something that should be relayed but it comes in by phone instead of email? Is that something we want to even want to address?

Okay, I am seeing in the chat the overwhelming response is no. Nobody wants to speak up. Okay - (Todd).

(Todd): Yes, I certainly agree with (Susan) that there ought to be a process for reveal that does not require having gone through relay first and I think we are getting a little ahead of ourselves obviously and we will talk about that when we get to reveal. That said, I also think it is relatively fair to say that when we do get to reveal having made, you know, attempted - multiple attempts to contact the licensee through a relay that did not lead to any kind of a result is relevant to the reveal calculus and I think maybe if we just tag it at that for now and then we can debate later when we get to reveal how relevant is maybe the best way to go about doing that but I would be curious what everybody thinks.

Don Blumenthal: Thanks, and, you know, precisely I wanted to capture the thought but not necessarily to resolve until we do talk about relay reveal. Kathy.

Kathy Kleinman: Don going to the question you raised which is of course a really good question. So let me throw out a few variations of it. One is that PIR - well just using PIR if that is okay. PIR gets a phone call from law enforcement or from an attorney making an allegation and demanding that it be relayed to the registrant, to the proxy privacy licensee.

The other one and it happened a lot in the old days but we may see it happening again as we go in to new countries that haven’t had as much domain name work with the new gTLD’s is hard copies where the - a hard copy letter would be sent to the registry or to the registrar, again demanding something about a proxy privacy or demanding that a complaint be relayed, although they probably wouldn’t use those right words at all.

So let me throw those two things out - phone calls and hard copy letters - what should a proxy privacy provider do with those two types of communications? Should we be asking that they scan the letter in and send it on - that is a lot of work, you know, should there be any obligation to even respond to the requestor and say, “Look, you need to send this through email,” but different variations - thanks, bye.

Don Blumenthal: Thanks for flushing that out - (Chris).

(Chris Pelling): Well just a bit of few - this is (Chris Pelling) for the transcript - put some meat on the bones of my rather blunt, no comment.

Essentially if somebody rings you up and says, I am the police from the UK or I am the Met Office of - or rep. sorry, if I am the Met Police from the UK, you as the registrar, PP for service provider have no recourse to prove that and, you know, we even get emails from what could be a (unintelligible) stating what they are and if there is no change of evidence thinking from a logistic point of view that we can prove where something comes from to then pass it on to the registrant, aka, somebody doing something ROAM or whatever, then all it makes us is look stupid.

No obviously on stop of that if it comes down to the fact that we have got to then start accepting calls from anybody and therefore can’t prove it we are then going to lock those tools and record them which, you know, is just a way out of the bounds of the simplistic route this should be able to take. I - like we do and also if you can either email us on a (unintelligible) that goes straight to whichever contact you require. The point earlier was made with regards to how can you prove that something has been relayed or you have a (unintelligible) logs, you as the person that receives the email to send it on can only get those logs together (unintelligible) once an email has been delivered.

From the point of view of how an email comes in we don't relay all emails. As an example, I think Tim pointed this one out - I could be wrong, it might be James, sorry, with regards to FOA emails - we don't do that, purely for the fact at the end of the day if you send an email to the main dot com or IDCprivacy.com you get an also responder that tells you how to then create your second email, to which contact you want that email to go to. Once you then send that through we send you back a confirmation email and then you can send within 24 hours an email to the registrant. We don't release any of the information, we make up a totally spurious address and we can confirm back that the mail was delivered.

Just a couple of interesting points there - certainly from the point of view accepting any form of phone call from anybody over the phone that says who they are, who they think they are or what they feel they are doing.

Don Blumenthal: Appreciate and those are real useful - real world perspectives that are looking to critical as to because we - so we don't make things up without any contact with real rules.

Now, welcome (Dan).

(Dan Burk): Hey, thanks very much. I am new to the group so I was just sort of trying to listen for a little background.

I guess I sort of represent the law enforcement perspective on what the Office of Criminal Investigation for the Food and Drug Administration and I do make a lot of inquires pursuant to our criminal investigations.

So I guess just to add I understand completely some of the frustrations, particularly, you know, overseas - I mean there is tens of thousands of law enforcement agencies in the United States and so, you know, (unintelligible) exactly who is who probably can be very problematic.

I guess from my perspective I appreciate, you know, like if they will put in, you know, a phone number or an email or whatever. Some folks do some due diligence and call me and feel me out or call our main number to find out exactly who I am and once we sort of, you know, establish that trust then I think we can sort of move forward but I can appreciate the fact that, you know, there are lots of law enforcement agencies making inquiries.

But that said, a number, you know, usually when I am reaching out to make an inquiry it is something that is vetted - at least well vetted internally and, you know, we find it as an immediate or a significant public health risk and we don't want to simply ignore it on the basis of the fact that they can't validate who I am based upon our email or, you know, sending a letter with our business card - I mean, you know, it is difficult from our end as well.

Don Blumenthal: Thanks, yes. Is the second had disappear there?

(Chris Pelling): Yes, sorry Don that was me, Chris.

Don Blumenthal: Okay, oh, I see all right.

(Chris Pelling): Never mind.

Don Blumenthal: Yes, and particularly welcome (Dan) we have been hoping to get some law person - law enforcement for some time here, among the members. It has been a long attempt so appreciate your involvement.

Any other - okay I am just looking at (Chad) here. I don't want to - I have a few other questions to ask here but we are just up at 10 minutes to the hour. What I would like to suggest is in the bid to spur thought but also for the involvement an email list is, you know, focusing on specific types of processes and using the wording, minimum standardized processes that we can realistically require. Whether that is how complaints - or not complaints, how requests for relay - things that should be relayed come in, any kind of formats, any kind of basics for forwarding and I think looking at the list in two (unintelligible) would be worthwhile in helping to define some of those things.

I know in looking at some of them I just, right of the top changed them - I think we know what the basic question is.

So with that, unless there are any other comments, why don't we wrap 30 seconds early.

Man: Thanks Don.

Man: (Woo-Hoo).

Woman: Okay, thanks - thanks Don.

Man: Thank you.

Man: Thanks Don.

Man: Thanks Don.

Man: Thank you.

Woman: Well thanks very much (unintelligible) and I will stop the recording.

END