

**ICANN Transcription  
Privacy and Proxy Services Accreditation Issues PDP WG  
Tuesday 15 April 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 April 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-20140415-en.mp3>

On page:  
<http://gnso.icann.org/calendar/#apr>

Attendees:

Luc Seufer - RrSG  
Graeme Bunton – RrSG  
Tim Ruiz – RrSG  
Steve Metalitz - IPC  
Kathy Kleiman – RySG  
Darcy Southwell - RrSG  
Libby Baney - BC  
Roy Balleste – NCUC  
Susan Prosser – RrSG  
Justin Macy – BC  
Jim Bikoff – IPC  
David Heasley – IPC  
Michele Neylon – RrSG  
Osvaldo Novoa – ISPCP  
Jennifer Standiford – RrSG  
James Bladel – RrSG  
Volker Greimann – RrSG  
Tatiana Khramtsova – RrSG  
Carlton Samuels – ALAC  
Maria Farrell – NCUC  
Paul McGrady – IPC  
Tobias Sattler – RrSG  
Phil Marano – IPC  
Christain Dawson – ISPCP  
Laura Jedeed – BC  
Don Blumenthal – RySG  
Griffin Barnett – IPC  
Gema Campillos – GAC  
Stephanie Perrin – NCSG  
Valeriya Sherman – IPC  
Frank Michlick - RrSG

Apologies:

Kristina Rosette – IPC  
Sarah Wyld – RrSG  
Holly Raiche – ALAC  
Marie-Laure Lemineur – NPOC  
Amr Elsadr – NCUC  
Joe Catapano -Staff

ICANN staff:

Mary Wong  
Amy Bivins  
Mike Zupke  
Terri Agnew

Tim Ruiz: ...is now being recorded.

(Terri Agnew): Thank you, Tim. Good morning, good afternoon and good evening. This is the PPSAI working group call on the 15th of April, 2014. On the call today we have Justin Macy, Laura Jedeed, James Bladel, Michele Neylon, Tatyana Khramtsova, Christian Dawson, Steve Metalitz, Osvalda Novoa, Darcy Southwell, Don Blumenthal, Libby Baney, Paul McGrady, Roy Balleste, Tom Lam, Carlton Samuels, Graeme Bunton, Griffin Barnett, David Heasley, Jim Bikoff, Kathy Kleiman, and Frank Michlick.

We have apologies from Sarah Wyld, Kristina Rosette and Amr Elasd, as well as Joe Catapano. From staff, we have Mary Wong, Amy Bivins, Mike Zupke and myself, Terri Agnew. I'd like to remind all participants to please state your name before speaking for transcription purposes. Thank you very much and over to you.

Don Blumenthal: Hi. Appreciate it. Thanks. Just jumping back to the right screen. Well, first, since I wasn't on the call last week, I just wanted to note in general, it's good to see some people that I had not met before.

It's one of the best things, some might suggest, one of the few good things about ICANN meetings. We've been (in this little world) in conference calls and Adobe but it's nice to actually put faces to lines in the chat room or email - is really valuable.

Why don't we jump right into this session? James has offered, was drafted, however you want to put it - I wasn't there - to discuss the whole issue of the gTLD transfers. So I will step back and listen.

James Bladel: Thanks, Don. This is James speaking. Did you want me to just go ahead because I had difficulty hearing you there at the end.

Don Blumenthal: Yes, please. Might as well get started.

James Bladel: Okay. Oh, that's much better. Thanks. Okay, so this is James speaking for the transfer and - or for the transcript and (saying) today I volunteered to present an overview of how transfers work in gTLDs.

This is in the context of discussing how transfers and other policies might interact with privacy proxy accreditation services and in order to delve into those questions, I think it was determined that we needed a better synchronized understanding of how the transfers work.

This slide deck, I would love for you guys to think that I would just, you know, kind of banged this out here in the last week but, in fact, is from one of our IRTP PDP's. I think Marika and staff - Mary can probably help me.

This is going back now probably to late 2012. So it is a little dated. I will try to highlight any areas where I think that the information in the slide is, you know, perhaps been overtaken by events but I think that - I did go through it over the weekend and it looks fairly current.

So I'll try to go through this quickly. I'll try to make it interesting. I'll try to leave ample time for Q&A and - but certainly interrupt me if you feel like we're going too fast.

So next slide please. So here's the purpose of transfers. And, in general, the transfers, while not the most exciting thing in the world, are critical to supporting a competitive marketplace because it allows the registrars to leave - I'm sorry - registrants to leave and move their business to another service provider if they're unhappy, if they see a better price or if they just want to, you know, want a change of scenery.

We're just - registrants or transfers of registration are very - are varied and implemented differently at different registrars. So the purpose of this transfer policy is to establish some standardization so that different service providers can interoperate in a compatible manner.

The transfers are often used in conjunction with the change of control so that is where a domain name not only changes registrars but also changes registrants, typically in the case where a domain name has been sold on an aftermarket or perhaps, you know, in the enforcement of a UDRP or a type of decision like that. And that was something that this particular working group addressed as well.

Next slide. So here's a couple of diagrams that are going to outline the sequence for a transfer when everything goes right. And it is meant to

be broad brush strokes. I'm sure that registrar colleagues on the phone will point out a number of details that are sometimes implemented inconsistently but in general, this is how the process works.

The transfer process is initiated at the new registrar, so a registrant initiates - goes - opens an account with a new registrar and says something along the lines of, you know, I want to move my domain name to my new account and my new registrar.

And the new registrar will usually provide instructions or walk them through the process or even perhaps has a support team dedicated to this process. So the new registrar will essentially say, you know, to start the process, make sure your names are unlocked and retrieve your auth info codes.

Next slide. The new registrar also concurrently performs a Whois lookup to get the registrant of record, the email for the registrant and the admin email. This is - the registrant and the admin contacts are collectively called the transfer contact.

And this form of authorization for the transfer, which is required by the policy, is sent to the transfer contacts. The - so this is a critical part of essentially establishing the paper trail of authorization for the transfer.

Next slide. The registrant unlocks the domain name and in its current registrar says maybe the auth info code. The auth info code is a unique ID number. You can think of it as a password or the domain name or a key that is shared by the registrar and is on record at the registry.

The registrant accepts that form or authorization, sends that and the auth info code back to the new registrar. The new registrar then contacts the registry and says, "Okay, I've got a completed and accepted form of authorization. Can I have a valid auth info code?" And then it sends that up to the gTLD registry and requests that the transfer sponsorship of the domain name move to the new registrar. Next slide please.

Don Blumenthal: Yes, James.

James Bladel: Oh, sorry.

Don Blumenthal: Yes, Steve's got his hand up there. Do you want to jump in?

James Bladel: Okay, sorry. Not paying attention to the queue. Jump in, Steve.

Steve Metalitz: Yes, I'm sorry. If you can - I'm trying to, again, figure out how this would fit in with the proxy service situation. So if you go back to your - I think it's your second slide on a pristine transfer, so it's - yes. Yes, that one I think.

So that's the point it seems to me, at which the new registrar performs a Whois lookup and in the case of a service, of a proxy service, they will have the contact information for the proxy service basically. That will be the one to whom they send the form or authorization.

So that, I think, is the point at which this system - it's hard to fit this system into the proxy service system because we have to assume that the service provider is going to communicate to the customer who is what I could call the register here. Or is that mistaken? Would the ser-

would the customer have to go first to the service provider and say,  
“Hey, I want you to initiate this process since you’re the...?”

((Crosstalk))

James Bladel: That’s a good question, Steve. So if I could take a swing at addressing that, Don.

Don Blumenthal: Certainly.

James Bladel: Okay, thank you. So essentially the registrant icon in this scenario, in the context of this PDP would be representing the proxy privacy service, and the form of authorization and all communications from any registrar would, in fact, be going to the service.

However, I think as we noted from our previous presentations, a number of these services will generate a unique email and that will be used for relay purposes for this type of communication, you know, critical communication.

However, as we discussed in our last call, a number of proxy services because, you know, because when they’re in the role of the current registrar will, in fact, reject transfer request as a security feature and will ask registrants or the - their privacy proxy customers to deactivate the proxy service prior to initiating the transfer, so going all the way back to Slide 1. Does that help, Steve? I’m sorry...

Steve Metalitz: Yes, I think it helps, especially because since we’re on the question of what the rights and responsibilities of the service provider would be, I

suppose this suggests that one responsibility is to cooperate in this transfer process.

Obviously that could take different routes. And in the case of a provider that generates this unique email address, then is that email address - is that immediately accessible to the customer or is that simply an email address that's maintained by the service provider and the customer doesn't necessarily receive that?

James Bladel: Probably best described as an email alias that would be posted in Whois and a relay, an automated relay, would occur if, A, the service were structured to do that and, B, if the, you know, in our case, we allow the registrar - or the customer of the privacy proxy service to select what kinds of emails they will and will not receive. So if that were to fail, for example, then the transfer would not be considered authorized and it would be rejected and I believe it times out after five days.

Steve Metalitz: Okay, thank you.

Don Blumenthal: Kathy?

Kathy Kleinman: Yes, following up on Steve's question - good morning everybody and James, thank you for the presentation. This is very helpful. Following up on Steve's question, could we try two scenarios? One is if you're transferring within a proxy privacy service provider, so if I'm transferring to someone else in domains by proxy - I don't know if we want to pick a specific one to - does - how does - does that require an unveiling or a publication of the information?

And the other question would be -- and I'm not sure it's just to James -- how might we set up a system that doesn't require the relinquishing of the proxy privacy protections prior to a transfer between proxy privacy service providers? Is there a way that has a working group we can think about ways to keep that protection up? Two questions. Thank you.

James Bladel: Those are, I think, very key questions, Kathy, and I can tell you that for domains by proxy and I believe this is true for (two cows) and also, I'm looking down the list, other registrars like (Black Knight).

In any - in all cases, the privacy service must be deactivated prior to transfer so that the domain name arrives at the new registrar with the customer's - you know, the privacy proxy customer's contact information where they then would activate that registrar's privacy service.

So you're correct. There is this period of exposure and given that a number of services, and I know domain tools is represented on the call here, will archive Whois on a continuous basis. That means that that is, even for the brief moment, potentially being captured by these services.

So I think that would be an interesting - not just the policy question but an interesting technical question to solve, is how can a domain name change registrars with the pro- the privacy services in tact? And as part - to my knowledge, that's not possible currently.

Kathy Kleinman: Great. Thank you. I'd love to footnote that this is an area we should definitely be looking at. Don, if I might, this is a fascinating technical and policy area.

James Bladel: Can I make this even more complicated by noting that I think that some of that is an artifact of the thin Whois model and not having visibility to the other registrars (Whois) and perhaps having thick Whois universally implemented across all gTLDs might be, you know, one way that registrars could begin to address that problem.

Don Blumenthal: So we just ignore it for a few years and it'll go away, huh? Got a couple more people in the queue here. Michele.

Michele Neylon: Thanks. Michele speaking. Yes, James touched on an important thing. One of the key issues here is -- and with respect to thin registries -- in the case of a thick registry, you wouldn't need to rely solely on Whois to get back the details you need in order to do a transfer.

In the case of thin Whois, it's the only thing you can rely on, plus it's also the only way you have of (accessibility) of data. So hypothetically speaking, if you were to logically follow through what is possible and what isn't possible using EPP, one could, in theory, access the data needed to initiate transfers if the registry was thick.

In the case of a thin one, you can't. You have to use Whois. And, of course, the problem is that the - while you could potentially do a transfer with privacy proxy in place, nine times out of ten, it's going to fail.

I mean, this is based on our experience plus, you know, there's no relia- there's no way of knowing whether or not the email is actually functional. Thanks. Do you mind if I address Steve's...

Man: Okay.

Michele Neylon: Do you mind if I address Steve's thing on the chat because he's asking about the EPP thing here?

Don Blumenthal: Oh no. Actually because I was going to - I had a question here too, so perfect.

Michele Neylon: The - Steve, the EPP allows you to transfer data that isn't public. So if I - if you - if I, as the gaining registrar of a domain and I'm just talking about domains in general. It doesn't matter if they're ccTLDs or gTLDs because we're talking EPP as a protocol not as an ICANN exclusive concept.

Once I have a valid - once I, as the gaining registrar, have a valid key, I should be able to access data that's not in the public realm. So I could potentially access extra data. Somebody who's more familiar with EPP might be able to give more concrete examples, but that's what I'm referring to.

Whereas, in thin Whois, the valid key (for the) auth info code, Kathy, yes - in thin registries, the registry does not have the contact details. It only has a minimal set of information such as the domain create, domain expiry and very little else. Thanks.

Don Blumenthal: I appreciate that clarification. James, do you want to go - just go ahead and handle the queue since it's...

James Bladel: Sure. I can do that. I see a number of other registrars want to weigh in on this so Volker.

Volker Greimann: Yes, just two things about Kathy's question there about the reveal.

It's a bit of a conundrum, as you said, James. And in our case, when we get requests from the registrants that say, "How can we turn off the Whois privacy when we want to transfer if we do not want to have our details in the Whois," is that we usually recommend to the registrants to use a throw away email address for the underlying data and use the new privacy proxy services data already before initiating the transfer.

So when we deactivate the service, the new data will already be in place. The registrant will then transfer that email - that domain name with the throw away email address and the data and then he would, at the new registrar, again, update his Whois details.

This, of course, will be made impossible once the waiting periods that are coming out of IHPC are implemented which will complicate things even further.

But we've found no other workable solution at this time that allows the registrant to stay hidden during a domain transfer. Some registrants have tried transferring out domain names with the Whois privacy service intact.

That means that at the moment of the transfer, the email address is no longer working because we will not provide the forwarding service that they described a couple of sessions back.

And we will file - either file a Whois (inaccuracy) complaint with ICANN right away when we get notice of that or take other action against the incorrect Whois data because basically it's our liability when we are in

the Whois for domain name that we cannot remove ourselves from the Whois at a moment's notice.

James Bladel: Thank you Volker and I think that's correct. And I think that currently is the case for other privacy proxy services if we were to spot our contact data being used and domain name that's sponsored by another registrar that's usually a pretty good indicator that something is wrong and we would take action against that domain name. Tim, (you're up).

Tim Ruiz: Yes, I guess, you know, that I - what I don't understand is why reveal -- excuse me, rather relay -- isn't, you know, an opportunity to perhaps implement a transfer without revealing data.

You talk about using thick Whois and I think that might have some merit to a point but it relies a lot on, then you know, bringing registries into this process, you know, a whole - white a bit further. And then I think, you know, that would be an even bigger debate.

And I'm not even sure how many registries we have in this working group. We'd want to make sure that we've got good representation so we can see what they think about, you know, what it would increase in their responsibility as far as handling transfers.

But relay, you know, the only reason relay doesn't work is because nobody uses it for that purpose, but it certainly could. You know, if a proxy service receives a request, there's no reason why that couldn't be relayed on to the underlying beneficial users who would then reply in a particular way and the proxy service relays that reply onto the requesting registrar.

So there's certainly an opportunity in there to make that work. It's just - just hasn't been done but there isn't a reason why it couldn't be and somehow made to work. Now, it may not solve every situation such as the UDRPs, et cetera.

But then I think, you know, that's a situation where, you know, I might be prudent to use the registries perhaps in the thick Whois having a little bit more, you know, for that type of a thing. But for just normal transfers, it would seem to me that there's an opportunity to make relay work appropriate for that. Thanks.

James Bladel: Okay, thanks, Tim. Yes, I think you're right. And it just occurred to me that relay, in most cases, is a one-way transaction. There's no way for a registrant to respond to the relay address that might be assigned to them from the service. So that, I mean, it's an implementation issue but it seems to be the way it that those systems are structured now. Steve, you're up next.

Steve Metalitz: Yes, thank you. This has been a very informative discussion. I appreciate everybody's contributions to it. So just picking up on Tim's point then, it might be theoretically possible for this to be handled through relay but apparently no, or at least many, service providers, proxy service providers, that are affiliated with registrars are not doing it that way and I can understand the business reason not to.

But - and then it becomes - I mean, to some extent it's a disclosure issue and making sure that registrants or customers are aware of this. But it appreciate his comment that it is theoretically possible and maybe perhaps that's a best practice that one would want to encourage.

I do want to come back to this issue of the extent to which thick Whois addresses the problem. I get it that there could be non-public information as communicated through EPP but my understanding is that even in a thick registry situation, does the thick - does the registry - what's the basis for assuming that the registry actual has the underlying contact information of a proxy registrant?

In theory, even the registrar doesn't have that. It's their affiliated or, in some cases, non-affiliated, proxy service provider who has that information. Or is that information routine? In a thick registry environment, I'm not clear why that information would routinely be held by the registry.

I agree that if it were and EPP could then be used to communicate that way, that would be - that would solve the problem but I'm - I guess I'm puzzled - am I wrong in assuming that in my assumption that a thick registry would not ordinarily have the contact information of the proxy service provider, customer?

James Bladel: Thanks, Steve. You're correct. The thick registry would not have the underlying contact information. The reason to introduce that - and I agree that it would not necessarily solve this issue that was originally raised by Kathy but I think that it - maybe turning that around and saying the fact that there are thin registries and that registrars, you know, even in transfers that don't involve privacy proxy services today, are relying on the voracity of the Whois information contained by the other registrars, I think that that complicates this issue and necessitates why a registry or registrar would either (snatch) a transfer request for a privacy domain name or not accept a request for a

domain name to transfer in with another registrar's privacy proxy information.

So it's possible that a combination of transitioning to a thick registry model and establishing some sort of a trust mechanism based on the idea of accredited proxy services might someday address those two issues but I agree with you.

It's not just that we're counting on the registry to be a repository of the underlying privacy proxy information. It's more a question of do you have, you know, some third party information to confirm that it is privacy service in the Whois or are you just doing it blind? And I think in the thin - in the current model for thin registries, you're doing it blind.

Steve Metalitz: Okay, so it's partly a question of the level of confidence in the accuracy of the Whois data.

Michele Neylon: Is it me now since nobody seems to be managing the queue or maybe I've just lost the line? Hello?

James Bladel: Hello. Sorry, I just...

Michele Neylon: No, (unintelligible).

James Bladel: I just got bumped over onto mute. Sorry about that. So yes, Michele, go ahead.

Michele Neylon: Yes, sorry, just thinking about the reliability of the data in thick versus thin, I don't think this - this isn't really the issue operationally speaking. Operationally speaking, the biggest issue as a gaining registrar we run

into, it's not about what the data on the losing registrar side is. It's weather or not the losing registrar's Whois server is actually serving anything or that we can access it.

So I mean, if the losing registrar's Whois server is offline more than it's online or has crazy ass rate limits which means that one query and you get black listed, then it's very, very hard for us to do a transfer.

Also, as well, technically speaking, Whois servers, like any other software, will fall over. I was informed by our technical team earlier today that ours was misbehaving yesterday for a couple of hours.

You know, this kind of thing happens because in the case of a thin registry, it's not just what the data is. It's the actual, is there anything that you can access?

And it's not simply an enforcement issue because the problem is that a lot of the time it's, you know, the registrars themselves probably need to sort this stuff out. I mean, personally I couldn't give about the enforcement. All they do is transfer a domain between registrars.

The other thing, as well, with respect to data, underlying data and all this reveal and a reveal and relay thing is what I was tr- suggesting wasn't that that data was available now, but that hypothetically it could be available.

And, I mean, already at the moment, the EPP keys are held at the registry level, they're obviously not going to be public. And there's no reason why you couldn't add other bits of data somewhere else.

And I'm not saying that the underlying registrant contact or anything is going to end up being pushed to a registry but, you, if for example, let's say we were to go back to the - kind of the operational contact points concept that was bandied about several years ago, you know, you could have an email address that would be available for transfers only or something. I mean, there's a lot of different possibilities there. I'm just saying that in a thick registry, you have more options open to you. Thanks.

James Bladel: Thanks Michele. And Kathy, you're next. And then we should probably address some of the conversation going on in the queue.

Kathy Kleinman: Do you want me to wait while you're doing that, James?

James Bladel: Well, let's see here. I just - I want to see if there's anything that we're catching in the chat. Don, maybe if you could review that while Kathy's speaking and let us know what we need to address there.

Don Blumenthal: Yeah, I was just scrolling back up.

Kathy Kleinman: So I was wondering if the valid key that Michele was talking about or the auth information code that you were talking about, James, which I understand to be the same thing, might provide a way through some of the discussions that we're talking about.

Because if a registrant under proxy privacy - and I'm just throwing this out there because I don't know these systems nearly as well as you do. But if a registrant - so if the registrar provides the auth info code to a proxy privacy service provider that then passes it on to its registrant and then the registrant - even though they're under proxy privacy is

able to produce that code to enable and facilitate the transfer can the code itself be used as the proof of valid request for the transfer?

Because the registrant wouldn't have it if it hadn't passed through kind of a trusted network from the registrar to the proxy privacy service provider to the registrant. Can the code itself be the authenticity?

James Bladel: Thanks, Kathy. Interesting question. And this is something that touches on a little bit something that's currently being discussed in IRTP-D which is whether or not the auth info code has effectively replaced any other types of authorization and has become sort of the de facto, you know, transfer authorization for a domain name in all cases.

And I think that that, you know, without going into the weeks of discussions on that issue the working group is basically coming down on the idea that it has become that in most situations however there are certainly enough edge cases and/or situations where a customer's registrar account may have been compromised to prevent us from kind of endorsing that auth info code as a, you know, general purpose transfer key.

So I think - and I'm not sure if that directly addresses your question. I think could it be - could it be used or further employed to establish some degree of trust between a new registrar and a privacy proxy service customer from another registrar with whom they had no relationship I think that's possible.

But now I'm channeling Mikey O'Connor who likes to point out that the auth info code right now is overloaded and is used to check or to authenticate the registrant on just so many different types of

transactions that, you know, he considers it to be an overloaded piece of data.

But it is something interesting and I think that any approach that would eventually allow a domain name to transfer while maintaining private information would probably make use of that code in the way you describe.

Kathy Kleinman: And perhaps with some additional protection built around it to prevent some of the edge situations that are creating problems now which I don't fully understand but I recognize they're there.

James Bladel: Sure, why not. These are, I think, good points but they are a bit speculative in that, you know, the transfer process that is laid out in the slides is actually more of a model in reality and I think the other registrars will weigh in it actually frequently encounters problems not the least of which is what Michele was raising which is, you know, not having access to the other registrars Whois data and the whole thing breaks on the first step. So, but we'll jump to Tim next.

Kathy Kleinman: Yeah.

Don Blumenthal: Yeah and let's move on in the slide deck after Tim.

Tim Ruiz: Yeah, I was just going to mention that - or point out that, you know, there really isn't any 100% secure way to do transfers. Even where we're doing it now we have issues. And I'm not sure that it's necessarily has to do with - that by not relying on the auth code alone that we're actually, you know, have diminished transfers, you know, false transfers or whatever that much.

So I guess I would agree with Kathy that what we should do instead is take those identified edge cases and see if those aren't things that could be dealt with. And if, you know, if we see that that's a possibility then maybe this is one of the potential recommendations we could make even though I realize it probably require, you know, some work with the transfer process policy down the road.

James Bladel: Thanks, Tim. Is that the - is that an old hand, Kathy? Or did you want to respond?

Kathy Kleinman: I apologize, that's an old hand.

James Bladel: Okay. Okay so returning back to the slide deck - thanks, Don, for putting us back on track. And I actually think we're almost done. I think this is where we left off here. So once the form of authorization and the auth info code is presented to the new registrar it is relayed to the registry and the new registrar asks the registry to transfer sponsorship of the domain name.

Next slide. Registry takes a look, everything checks out. It notifies the current registrar, the registrar of record, that the domain name is transferring away. In some cases this may be the current registrar's first indication that the registrant is - that they are losing this particular customer.

The transfer - it does not occur right away. The current registrar has the ability to (nac) or block or object to the transfer which they can do within five days. After five days, however, the default timeout process is that the transfer would proceed.

Next slide please. Here are just a couple of reasons why this process might not work or may deviate from the model that we were just discussing if the FOA is not accepted, if the domain name is locked, if the auth info code isn't valid or if the losing registrar rejects the transfer. Next slide.

The losing registrar can't just reject transfer for whatever reason it likes. It has to do so based on some clear justification for why it denied the transfers. These are called reasons for denial and this I think has been updated since November 2011 so apologies for that; this is probably one of those slides that's a little dated.

But as you can see here that has to be reasons for this, rejection of a transfer, other registrars certainly are not shy about reporting - registrars are not shy about reporting each other to ICANN Compliance if they feel a transfer has been rejected for insufficient cause. And Compliance will routinely ask registrars why they've rejected a particular transfer and ask to see documentation of one of these events.

Next slide please.

Mary Wong: Actually I think that's it, James.

James Bladel: Okay great. So as a - as a service, a privacy proxy service will essentially - it's not necessarily rejecting the transfer at the registrar level in the service itself is - if we can go back one slide - the service itself is rejecting the FOA so that is where the privacy proxy service is

saying, "No, I do not authorize this transfer as the registrant of this domain name."

Now, you know, to Kathy's point, yes, that means that privacy services would need to be removed prior to initiating a transfer, at least that's how the industry solves this issue today.

To another point I think that, you know, it is at least amongst our customers and our service and I'm sure other registrars would agree that the privacy service provides an extra layer of security against unauthorized transfers. Because you essentially, you know, it's another form of lock that someone who is attempting to hijack or steal a domain name and move it to a new registrar would not have access to the privacy service and be able to cancel that service to allow the transfer to proceed.

So it is another hurdle that a bad guy would have to go through in order to hijack the domain name. So that was it. I think that we covered a lot of the meat of this issue in our discussions in some of the earlier slides. But would be happy to address any other questions or be looking to my registrar colleagues on the call if they want to weigh in on these issues as well.

Don Blumenthal: Tell you what, why don't we move - oh, Steve, go ahead.

Steve Metalitz: Yeah, this is Steve Metalitz.

((Crosstalk))

Steve Metalitz: Again I appreciate this presentation and all the input from the other registrars on the call too. I mean, my sense is that we kind of have two ways we could go here.

One is kind of the descriptive way based on the world as it is now and there in terms of rights and responsibilities of service providers it seems as though it's basically a disclosure requirement to make sure that registrants are - or their customers are aware that in order to effect a transfer to a different registrar you will generally need to step out of the service.

And that - and that that is also a protection against unauthorized transfer but it also is kind of a - perhaps an impediment to an authorized transfer. That's one route.

The other route is more prescriptive if we want to say that as a minimum accreditation standard the service provider should do what most of them are not now doing which is what I was having the dialogue with Tim about in the chat, you know, should they be required to cooperate, to facilitate a transfer whether it's through relay, a CCTS or in some other way to facilitate a transfer if their customer wants it.

So I think that's kind of - it looks - at least based on what I've heard today it sounds as though we would have to choose whether to take a descriptive approach in these minimum standards or a more prescriptive approach that says in order to be accredited you actually have to do things differently than most services are doing them today.

I don't know, I'd be interested in other's reactions to that but that just struck me that that's a little bit of a fork in the road that we're looking at

here as far as rights and - statements of rights and responsibilities for service providers. Thank you.

James Bladel: Don, did you want me to respond or just...

((Crosstalk))

Don Blumenthal: Yeah.

James Bladel: Sure. And I think other registrars - and I haven't been following the chat - may have already weighed on this. Steve, I think that you correctly identify the choice or the fork in the road, as you put it. My concern, just my initial reaction without having really put a whole lot of thought into how to address this problem, is that if we were to choose the fork that says, you know, fix this problem registrars, I think that we - we might be going down an interesting and possibly - and I'm trying to be careful here but a possibly technologically unworkable situation.

And my concern is just that that, you know, addressing that - if someone were to be able to reliably address that problem I think it would be pretty amazing and would have, in fact, a, you know, I think would have invented some really interesting and new to world type processes and technologies.

And so I think we have to be careful that we don't, you know, compel service providers to do that in policy. I think that that's my only concern is that we would, you know, require service providers to solve a problem that no one has yet to date. But I mean, I think it's an interesting idea and I think you have accurately captured the choice that we would have to make as a working group.

Don Blumenthal: Okay I made one exception when we - call on Stephanie and then we'll get something done on Category B Question 3. Stephanie. Stephanie. Stephanie, we're not hearing you.

Michele Neylon: Don, just move on if she's not on the call.

Don Blumenthal: Yeah, I was just going to say why don't we move on if you could just type what you have to say and we'll move on to the document.

Mary Wong: I'm sorry, I'm having trouble sharing the second document so just if you'll just give us a couple of minutes here.

Don Blumenthal: Okay. Maybe Stephanie will be back.

Steve Metalitz: Don, this is Steve Metalitz.

Don Blumenthal: Yes.

Steve Metalitz: If we're in a bit of a pause here to get another document up I - there are these questions on the right hand side of the screen and I would be interested in response - James or other's responses to them. Like the first question, this is in the expiration renewal situation rather than a transfer situation. But it seems as though it raises the same concern.

Registrars must notify the registered name holder of the expiration at least two times. So that would mean that the registrar is sending it to the service provider so then the question is should it be a requirement for the service provider to notify its customer that, you know, your registration is about to expire.

I just wonder what is the normal practice today and is this something that raises the same kinds of issues that we just talked about?

Stephanie Perrin: Hello. Hello?

Don Blumenthal: Yes?

Michele Neylon: Who's yelling at their phone?

Don Blumenthal: That's Stephanie.

Stephanie Perrin: That would be Stephanie. I just managed to get my mic working.  
Sorry to interrupt, Steve, I didn't mean to; I didn't think it would work.

Steve Metalitz: I finished asking my question so...

Stephanie Perrin: Jolly good. Well I typed out my question but basically when you say that Mikey is concerned about what's being loaded on that authorization code I too am concerned. Can someone explain to me what is loaded on that auth code? Because clearly - and we've been working in the EWG about all of this kind of stuff - if there's too much loaded on there and it creates a weak point where the bad guys can do something then that's a problem, right? As the non-geek here talking.

Don Blumenthal: Well does a geek or a quasi-geek want to answer that? Michele?

Michele Neylon: Oh sorry. I thought somebody was going to speak to Stephanie's point.

Don Blumenthal: Oh I saw your hand up, I thought maybe...

((Crosstalk))

Michele Neylon: Oh I was reacting to Mr. Metalitz because I feel somebody has to. A lot of the stuff around notifications and how registrants, account holders, etcetera, etcetera, etcetera, are notified with respect to upcoming expiries and everything was discussed to death during the Post Expiry Domain Name Recovery Working Group. I believe there are several survivors of that PDP on this call.

I'd have to check transcripts, which I'm not going to do because I really don't have time or the energy, but I'm sure we did look at privacy proxy stuff. I mean, like from a very practical point of view a lot of us - and I'm speaking - I'm not speaking for all registrars here - we send billing notices, in other words, renewal notices, to the billing contact detail we have on our internal billing system.

And what - the details I have for my clients and what my clients publish and what we publish for our clients are very, very different. So that's not really an issue. So if - for example, a domain name that is held that is on behind privacy or proxy with ourselves I'm not going to be relying on Whois details to be sending them renewal notices. Thanks.

Don Blumenthal: Tim, did you have a response to Stephanie's question?

Tim Ruiz: Yes I did. Tim again.

Don Blumenthal: Okay.

Tim Ruiz: Yeah, you know, I don't know about loading - what all is trying to be loaded onto the auth code. I don't think anyone suggested the auth code be used for anything other than transfers. You know, there was some discussion about possibly, you know, uploading or transferring additional information in addition to the auth code to thick registries so there was some discussion of that.

But I think the auth code has a specific purpose and I - and I agree I think that the reasons or the purposes it's used for should be minimal so that, you know, there isn't - the registrant doesn't have to keep this code memorized or known or written down on something forever and ever because they have to use it every time they turn around. So I think it should be used strictly for transfers.

And then just a quick note about Steve's question about that first question on the right because it's about renewals actually and I was just going to mention what Michele did there that it may not be that simple to just say, well, we're going to require the PP provider to notify it's beneficial user because at many registrars they have - their customer information is separate from Whois information.

And when they notify registrants of renewal often they'll be notifying both. However, I don't think there's any reason why you couldn't require the proxy privacy provider once notified by the registrar to notify via whatever method it has. You know, we have this discussion coming up about relay. Maybe - I'm beginning to wonder if we're going to find out that most PP providers never implemented relay. I would find that hard to believe. And so there must be some mechanism in place for PP providers to contact or have discourse with or whatever with their underlying users.

So I understand Michele's point to some degree. I also think that - I guess I'm beginning to wonder why PP providers can't communicate with their underlying user and find out and get things back like asking them oh we got a transfer request, here's the information. Do you want this to go through? And they respond. It seems like a simple thing to me.

So if it's more complicated the problems than that instead of just saying yeah there is I'd like to understand the specifics of what the problems or the road blocks are because they might be things we could overcome. Thanks.

Don Blumenthal: I appreciate it. We have five minutes to go. Note to self, next time I say let's move on, stick to my determination. At this point let's just continue this discussion. We will get to this document again next week. Stephanie and then James.

Steve Metalitz: I think Stephanie might be back on mute.

Don Blumenthal: Yeah. James, you want to jump in?

James Bladel: Okay. Yes and actually my question was - or my comment was to address Stephanie's question and I think Tim covered it mostly but just wanted to add that, you know, it certainly seems that there could be - first of all for overloading auth info codes we've had recommendations through other - or proposed recommendations through other PDPs that auth info codes be used for things such as inter registrar transfers, locking and unlocking domain names, updating or verifying Whois details.

And it was just kind of getting to this, you know, as Tim said with this kind of required password in order to conduct any sort of transaction related to your domain name including changing name servers. And it was becoming a universal key and then it would become then therefore vulnerable to being compromised. So that's to address Stephanie's question.

But I think Tim has the actual, you know, has captured the important element or takeaway from this whether we're talking about transfers or that we're talking about expiry notices that there should be some types or categories of email communications not only from let's say law enforcement or claims of, you know, abuse but also from the sponsoring registrar that a proxy privacy service must relay to its underlying customer.

And that it should not have the discretion to either block or withhold those messages. And I think that's kind of where in general where this is trending. And I think if there are services that aren't doing that I think we need to understand why because I don't know that there's a compelling reason why they shouldn't be required to relay certain critical - domain-critical messages. Thanks.

Don Blumenthal: Michele.

Michele Neylon: Thanks, Don. Just picking up on something from James - James's point. One of the reasons why people sign up for proxy privacy services is so that they don't get emails. This is something that Stephanie, myself and Carlton have been - what's the polite way of

describing this - vigorously discussing within the EWG over the last couple of months.

So okay, yeah, but from the registrar, yes, sorry okay so James has put in the there but from the registrar. So I think if you worded it along the lines of, you know, the proxy privacy service would need to relay all messages from their registrar then, yeah, that's absolutely fine.

Just kind of a blanket must relay everything concept would be one of the reasons why people didn't want the stuff in the first place. I mean, I did a check on a system earlier today just to see the amount of emails being directed at domain names using a particular privacy service and from a very small sampling - totally unscientific - of, you know, a snapshot of, I don't know, a week on a small number of domains I'd say 90 plus percent were coming from mail servers who were black-holed and blacklisted by Spamhaus.

So, you know, the volume of actual legitimate email that can potentially be going to those domains is probably negligible. Thanks.

Don Blumenthal: Yeah, appreciate that, Michele. Interesting. Yeah, let's just start to wrap here. This is - as I said, it wasn't quite what we had in mind but this discussion has been outstanding for substance, for education, whatever term you want to use. Really appreciate your taking up, leading it, maybe getting more than you expected, James. But it's going to be very helpful as we go along.

We will revisit this question next week when we plan to talk to (unintelligible) hopefully move onto the next. Please take some time in the email list to follow up on any issues that came up today that you

still need clarification on. The list has been a little quiet recently. Far be it from me to be complain about less email but it really is useful sometimes.

So until then we will talk to you all next week.

Steve Metalitz: Thanks, Don.

Don Blumenthal: You can now stop the recording.

James Bladel: Thanks, Don.

Don Blumenthal: Bye.

Mary Wong: Thanks, Don. Thanks, James. Thanks, everybody.

Man: Thank you.

END