ICANN Transcription
Privacy and Proxy Services Accreditation Issues PDP WG F2F meeting – Part 3
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: So just for everybody to note, since this is a closed session, we have two guests from the GDD, which have asked to join the session. And I've just heard that the recording is running so, Donna, I'm not sure whether you want to - no.

((Crosstalk))

Thomas Rickert: So I'm Thomas Rickert and I've been asked to facilitate today's session. And we kept the most interesting subject for this afternoon.

((Crosstalk))

Thomas Rickert: The Global Domains Division. So what we've been discussing before sort of was just the warm up to what we have on the plate right now. In preparation for this session we have agreed that it would be potentially of little value for Steve and others to present their proposals in great detail because we may easily get lost in detail and I think we cannot achieve more than hopefully agreeing on some basic principles on how to address the issue of reveal or to be more precise disclosure of publication.

And this is why we've asked Steve to give us a little summary of the very basic points with respect to reveal and the same would be true for registrars. And I think Graeme will - will you - will volunteer to maybe say something about the registrars' view on that?

Graeme Bunton: I might throw James Bladel under that...

((Crosstalk))

Thomas Rickert: Okay.

((Crosstalk))

Thomas Rickert: Okay so you will have a little bit - we'll get to that, yes. But let's kick it off with Steve. So, Steve, would you be kind to enlighten us.

Steve Metalitz: Thank you, Steve Metalitz for the transcript. The document that we circulated earlier this week really is an attempt to put a draft on the table for discussion and has already stimulated some discussion which is good. As you know both the IPC and the NCSG came forward with fairly detailed proposals on what we're now calling disclosure, the reveal issue.

But we've been waiting for the providers to come forward with something specific. So in order to try to help move that discussion forward we put this document on the table.

It basically gives a general policy statement of when the service providers should disclose to a complainant based on a prima facie evidence test. And then it provides an illustration of that for intellectual property. This is obviously the area that most of us in the Intellectual Property Constituency know and deal with everyday. It is only a small part of the world of other types of abuses that might trigger a request to disclose.

But we thought that since any general statement is inevitably going to be quite general, it was helpful to have a concrete illustration of how we thought that might play out in one area. And that's the bulk of this proposal; it's based on the domains by proxy policy that has been on the table for quite a few weeks in this group. It does make some changes there, add some additional requirements. And but that's kind of the basis for that illustrative example of the general principle.

And then I think it then goes on to set a policy for what - how the service provider should respond to having received a complaint either to disclose or to state its reasons not to disclose and have some review mechanism for dealing with that.

And then finally we felt it was important to say what the policy didn't cover or didn't rule out, kind of a savings clause if you will so that among other things you could have a trusted complainant policy, you could have a policy about when you notify your customers and how you deal with them and then you could have a policy about, you know, most of the providers seem to have a rule that if you breach their terms of service they can terminate the service or publish your data in Whois, which amounts to about the same thing.

And so we weren't trying to rule that out. That's the only place in this document where there's any reference to what we're calling publication; making the data - the contact information available to the world. Everything else here is making it available only to the complainant, only for stated purposes and so forth.

So that is our - is our basic proposal. I'm happy to provide our reaction to the text that Volker put forward. I don't know if Graeme wants to say anything before that or how you want to - how you want to handle that. But we have looked at it and I think there's, again, we're glad that he has responded to this

and I think it hopefully will help to kick off a constructive discussion. So that's the very brief summary of the proposal that we've put forward.

Thomas Rickert: This is me dying part two. James, would you like to step in?

James Bladel: So, yes, and just a word of advice, you will drown before you evolve gills, that's what I tell my children when they drink their soda too quickly.

So I read the proposal that Steve has outlined. And I definitely recognized a lot of our public procedures and policies in the proposal. And I think that there is, you know, I think in the interest of moving the discussion forward I think there's a lot to like in this proposal. I think there are some - certainly some issues that we need to iron out.

For, you know, as just a couple of examples, we did - I should mention that we did kick off an effort amongst the providers to develop, aside from Volker's response, a comprehensive - I would say our model that could be reconciled against this into some sort of hybrid or harmonized principle document.

Unfortunately, that's not ready despite my efforts and Graeme's efforts and I think Darcy and some others have also taken a shot at that but we're very close to that and we should have something here fairly soon.

But I can tell you that speaking for me personally and not on behalf of that document or other providers, there were just a couple of issues that we maybe should take a closer look at. For example, I think, Steve, your proposal indicated that all contact information would be shared. But our policy is that we only reveal the registrant contact data.

So other contacts and other information like billing and other things, nonpublic data, would not be shared. And I don't know that that's explicitly called out in this proposal and so that would have to be - that would have to

be addressed. I think it says customer - all customer contact data whereas we would leave that limited to just the registrant.

I think we have a general position, at least we seem to have a general agreement among providers, that there would be a separate process for law enforcement requests with a separate - with a distinctly different threshold that had to be crossed and particularly if we, you know, felt like the jurisdiction was questionable, whether or not it was applicable in that case. So I think that is another thing.

I think that it's good to see that the proposal included the idea of a trusted complainant system. I think that my personal preference, and I haven't surveyed the other providers on this, is that we move to that model as a default so that complainants or requests for reveal are all authenticated and known to the providers so that we can expedite those requests for folks who have a good track record and if someone has a bad track record that we can start to limit or revoke their access to these mechanisms. I think those are some other things we'd like to discuss.

And I think there was one other thing. Volker raised this - and I'm hesitant to go down this path but, heck, you know, we all got on planes, that's why we're here. Is this idea of - and this comes up a lot, okay, this comes up a lot in the context of this working group and other working groups, is we have to ensure that when a - we can't build into a policy a guaranteed outcome.

We have to have some - a little, a lot, moderate, I don't know what the right amount is - some degree of provider discretion or determination of - and I think you used the term prima facie, which is a nice legal term. We might have to boil that down to blatant or obvious or clear cases of infringement.

Because in those cases where, you know, maybe we're stepping into a gray area I think there provider has to make the determination of whether or not the risk that would be assumed of taking action like a reveal or canceling a

terms of service, would be offset. Because it's their neck that's on the line if this thing goes south and it turns out that it was, you know, either an error or false positive or whatever.

So I think that we need to make sure we're preserving a sufficient degree of provider discretion in making that determination of whether or not this is on - which side of that line of clear cut and blatant infringement.

And I think there were a couple of other - the one that I threw out, and, again, I'm not sure the other registrars and providers are on board with this is some notion that the relay process did not - was used and failed so that the - which kind of sets what I believe we're headed which is that this is an escalation path from the relay of communication that reveal is what you do when relay doesn't work or doesn't get the desired result.

So in general, I mean, that's me shooting from the hip here. And I don't see other registrars or providers grumbling too much but I think that we're kind of beginning to land on a provider consensus position that there really isn't in a different, you know, area code from what you guys put out it's - there are some key points here that need to be reconciled. Thanks.

Thomas Rickert: Thanks, James. Don.

Don Blumenthal: I just want to broaden the discussion a bit because there are other areas where reveal plays in they're not involved with intellectual property. And there are some very different issues. You know, in my past I've dealt with IP - with reveal more in the context of law enforcement, anti abuse, just trying to help consumers get redress.

So I'm just going to toss some ideas out there and keep in mind as we get into trying to come up with a general policy, if that's even possible, I think it's safe to say that we've certainly taken the approach that reveal is an escalation of relay but I think in some cases the consumer - I think in the

three areas that I mentioned that's not necessarily going to be the case because in investigations relay doesn't accomplish the purpose.

You need the information to step forward. And let me point out that the target is not always the bad guy. Very often reveal is done just as - people want to know the beneficial registrant; I'll put it that way, in the interest of further evidence-gathering. To link one registrant to another to see if there's a connection between one registrant and the particular bad guy; find somebody to interview, whatever. So those areas things are a little bit different.

The typical consumer, and we can probably - I know that people think that that doesn't happen - who wants to use Whois doesn't want his information (unintelligible) he wants to get his money back - her money back. Again, that's a reveal situation. You know, it's just the way - it's a real world operation.

Now I'm focusing here obviously on voluntary. I mean, I think we've already agreed that compulsory process is another issue that's going to trump what we do, you know, whether it comes from law enforcement or it comes from, for example, Microsoft's antifraud team - digital crimes group. And as a registry I can tell you that sometimes we get paper from a judge at their request, it's not just from a Department of Justice or - we haven't gotten them from some - law enforcement from other countries.

So, again, and I'm happy to go into details ad nauseam because that's what I did for many years in law enforcement and that's what I do now in anti abuse work. There are going to be different models that we're going to confront as we go forward.

And I'll leave it at that and we can - I'll inject myself as appropriate channeling my ex-law enforcement days until the day we can get some people who do it now. I think what I say is, no, I'm confident what I'll say is accurate but sometimes it's nice to have a fresh voice.

Thomas Rickert: Thanks, Don. I'd like to hear whether there's anybody else in the room who would like to make an introductory statement on this. Kathy? Holly? Who wants to go first?

Kathy Kleiman: Great. First, thank you for Steve for presenting a draft and to Volker for editing it. I'm going to put the draft aside for a second because I think what I'd love to extract from the draft is the principles of what you're looking for. And so at the outset let's talk - because we haven't done enough of this, let's maybe talk about some of the principles that customers might be looking for, registrants, you know, the customers, the underlying customer.

One would be a recognition of the gravity of the situation that a reveal means something; there's a reason they're behind the proxy. I know we have scenarios of the bad guys but there are lots of good guys and, you know, a lot of us work with the human rights groups. And we know there's gravity in the revealing, it's not just a mere procedural thing.

People, you know, there's issues here, also for small businesses, home-based businesses, nonprofit organizations, individuals. So how can we protect there customer? That's one of the keys here. What kinds of principles can we adopt for that. And so I'll repeat the phrase and then I'll try to stop saying it, the idea of the mere allegation. A prima facie case is still an allegation.

So presenting it is great but what else can we add to it that would add due process? And so we need due process. We need the customer to be able to respond if they want to. Maybe there's something else going on; maybe there are harassment purposes really underlying the allegations even if they're intellectual property allegations.

And lots and lots of areas. There's the opportunity of a response. So we would like - we would very much like to see that as a principle is that the

customer is notified and has the opportunity to respond. And if it was your client you'd want the same thing. And as lawyers you're going to be offering them the same thing outside of this accredited process.

What we heard from a lot of the Tuesday discussions was that many of the proxy privacy providers work on a case by case basis, some dedicating immense amounts of time to looking at the reveal requests that come in to evaluating them against their national laws and against their terms of service. We want to preserve that right that they have.

So these are kind of the elements that we want to see. And, Don, I'm not sure this addresses all of your anti abuse issues or the law enforcement issues but specifically addressing some of the intellectual property issues that there really should be kind of a back and forth before a reveal comes through. Thank you.

Thomas Rickert: Holly.

Holly Raiche: (Unintelligible).

Thomas Rickert: Okay. Alex.

Alex Deacon: I guess - so I agree with that. I think what's important to remember is that with relay we hope to start that dialogue with the consumer, right. So when that dialogue doesn't happen for whatever reason, perhaps they don't want to respond, perhaps they're behind mailer that, you know, some black hole, that's when - that's one of the reasons why we would need to then escalate to a reveal.

Kathy Kleiman: But escalating with other protections perhaps. They may not be responding for legitimate reasons. Right? There's no obligation to respond.

Alex Deacon: No, I agree 100% with that.

Kathy Kleiman: Okay, thanks.

Thomas Rickert: Wendy.

Wendy Seltzer: Thanks. And in this I think we come to some of the distinctions that the information that's being asked to be revealed is sometimes sort of thought procedurally as evidence to help in a further investigation. But it's also often for the - the registrant a substantive interest to keep that information private whether it's against investigation or against a use of the - of that information.

So it's - and there's a balance to be set sort of how far we let the investigation go to root out the person who's trying to use privacy for illegitimate purposes. And part of the way I think at least the US legal tradition deals with that is through the adversarial process with the opportunity to respond with motions to quash a subpoena or to stay a request for information before that's revealed.

And so if we can put some of that back and forth into the process that that gives the - the registrant the opportunity to protect that substantive interest in privacy.

Thomas Rickert: Kristina.

(Kristine): I'm confused. And I think - I guess what I'm struggling with is - and I think I'm misunderstanding it but it would be helpful for me if Kathy and Wendy, you could maybe help me understand because where I'm - what I'm hearing, I think, is Kathy on the one hand saying that the proxy service customer has no obligation to respond; and Wendy saying that we have to build a system that gives them the opportunity to respond.

So if I'm hearing you both correctly I'm trying to kind of reconcile how that would be.

Kathy Kleiman: That's a good question. I don't see a contradiction but maybe it's - and I'd love to hear Wendy's response as well. But in response to the relay I don't think - just knowing that the request came through so there's a very - I mean, we've all seen, you know, great cease and desist letters, the Jack Daniels' letter was a really good one, a nice cease and desist letter. We've all seen really vile cease and desist letters. And I tell my clients probably not to respond to some of them. So it doesn't matter how many times you relay it to me, we may not respond.

But that in and of itself is not an excuse for reveal. And then you kick into the process when the reveal is requested that Wendy is suggesting whether it's a reveal coming, you know, through the relay process or directly we're hearing that it's going to come directly from other sources as well that that kicks into its own due process which is an opportunity for the customer to respond.

And in lots of other arenas there is a motion to quash, the opportunity for that motion to quash. Most customers probably won't take it but to have that opportunity to say wait a second, there's another side to this request. Wendy, does that make sense?

Wendy Seltzer: Yeah - yes, so I think the opportunity to respond that I was seeking is the opportunity for the person whose information is being requested to move through an intermediary or a lawyer to request that the information not be revealed. And it's - does that resolve the confusion?

(Kristina): Not really, but I (unintelligible) I'll come back to you guys if I still am not clear on it.

Thomas Rickert: Okay. Thanks, everybody, for sharing their - James.

James Bladel: I'm sorry, so, you know, I'm going to stand down. Thanks.

Thomas Rickert: Thanks. Now, some of you have taken the opportunity to make some initial remarks on what their needs are. Let me confront you with a couple of statements that I think I could extract from the discussion or the statements that we had so far. And I would really like to get some feedback from you either nodding or opposing whether these are true.

There is no one size fits all solution for reveal. There is no one size fits all solution for reveal. I think that's something that we can agree on, isn't it? We need due process. Is that something everybody - please do ask your questions. But, you know, I'm just trying to slice it a little bit.

Steve Metalitz: Can I go back to your first statement, Thomas? There's no one size fits all but the question is can there be a general policy that, you know, a measuring stick that you can use in all cases? How it gets applied obviously depends on the facts of the particular case. But I'm not prepared to abandon the attempt to try to have a general policy and just say it's all, you know, case by case and you can't come up with any generalization.

So I would - I agree with one size fits all but let's not lose the concept of size here and that there could be a general policy if we can get it right that would be - give a certain element of predictability and certainty to how this operates, not all ad hoc.

Thomas Rickert: Let me maybe - let me clarity. That was meant to establish, you know, for this group that law enforcement requests require different treatment than trademark related requests than copyright requests and what have you. So for different categories or types of requests we would need to - to need different approaches. But those certainly would need to follow certain standards.

Holly.

Holly Raiche: I'd say even more than that one thing that was really useful on the list was looking at how registrars - different registrars deal with issues. And almost always it's a case by case basis. Almost always it's we look at it, we will take it seriously and then essentially, I mean, prima facie, yes it's a legal term, it describes the fact that the registrars are actually looking at what is put before them, is it - does it describe something that is wrong?

Does it describe something well enough to be taken seriously that something might be done about it and I haven't got form of words but prima facie is a nice kind of way of summing that up. But to say more than they should be taken seriously and don't (unintelligible) depending on the resources available, depending on your own national laws, whatever, you can generalize to that point; after that I think you get in trouble, would be my way of summing that up.

Thomas Rickert: Thanks, Holly.

Woman: (Unintelligible).

Thomas Rickert: Let's put that on the record, he was nodding.

Don Blumenthal: Agreeing or sleeping?

Thomas Rickert: Don.

Don Blumenthal: Just a - I think when it comes to law enforcement or anti abuse we have to be aware of the differences in how things work. But I'm not sure that responses do law enforcement, for example, are necessarily going to be different. They will be if there's a subpoena, they will be if there's a court order. But if it's a voluntary request you'll find at least - I'm sure you'll find a broad range of the extent to which law enforcement voluntary requests get different treatment than anybody else's.

James Bladel: Hi. So I think going back two statements ago your original statement or principle should be that reveal will be used by different groups for different purposes and they may have different standards for the mechanism. I think to Steve's point, that doesn't mean that we can't strive for some standardized process flow of those requests. How they are structured, how they are submitted, how they are tracked and how they exit that process.

And then to my point I think is that in that box there will be some review by registrars who may use different - or I'm sorry - providers - who may use different standards depending on the category of abuse, depending on their jurisdiction, depending on whatever. And so I think that we can have - I don't think it's incompatible to say that there are different categories of uses for this but we can have some high level standards.

Thomas Rickert: And I'm - Michele.

Michele Neylon: Yeah, thanks Thomas. Michele for the record. A couple of things, first off, while I can appreciate the - the meta-principle of, what was the term, damn it, the term has left me now...

Kathy Kleiman: Due process.

Michele Neylon: ...due process - thank you, Kathy - of due process I would be wary of making that an overarching principle for one very simple reason; as far as I'm concerned if you're a criminal scumbag who's registered a domain name with us using stolen credit card details you don't get any due process as far as I'm concerned. I need to have the ability to take decisive action without having to get - go back into these things. Hold on, Kathy, I'll come to you in a second.

I mean, there's levels to this. I'm just - what I'd be very wary of is there has to be a way of wording this so that you get the due process where the due process is merited but at the same time I don't know, maybe it's a case of looking at say the - that section of the new Registry contract where it talks

about the registries have to deal with - it's like abuse of the DNS and various other things which kind of affect the stability and all that.

I don't know what way to do that and ultimately, look, there's a load of lawyers in the room; you can sort of it out. But I - the thing is that, you know, at a practical level you don't want a situation where you have a criminal who has got nothing better to do all day except argue with you who manages to keep a Website, a domain, a resource online simply by abusing the quote unquote due process aspect. The due process needs to exist for, you know, legitimate purposes.

I mean, we've had the situation where dealing with fake pharma stuff where we've ended up in these ridiculous arguments with people. We've even had people who I think used 45 different credit cards to attempt to pay for their hosting in the space of an hour, trying to argue that we should keep their stuff online. So, you know, just be wary of that.

In terms of the points that James raised around, you know, this kind of higher level principles and, you know, trying to get some something which we can agree on, some of you may be familiar - I know that Don is - with stopadware.org. There's an entire thing there which is like best practices for web hosting providers which deals with, you know, how providers should deal with abuse reports.

Which, you know, as a hosting company we don't have an issue with, we're actually signed up for it. But it basically addresses a lot of the issues that reporters have so that, you know, the abuse department, you know, receives a request, has to deal with it within X number of hours, etcetera, etcetera, etcetera, there's an entire thing laid out there which has been accepted and was worked by a lot of companies so it's not kind of pulled out of somebody's rear end.

There's also another thing as well which is a best practice for submitting reports. I mean, just as somebody who receives reports of various types of abuse having to spend 25 minutes reading the very, very long and fascinating list of the trademarks that the apparent victim has isn't particularly helpful when we actually really want to know is what's the actual infringement. You know, the fact that Bank of America has 150,000 bloody trademarks doesn't really interest us. Thanks.

Thomas Rickert: But a quick response, Michele, how you organize your abuse department and on what grounds you choose to terminate the service for your customer I think that's to be separated from the discussion that we have here. Talking about process for reveal is a different type of approach than you throwing out a customer that you believe does wrong things. Right?

So what I'm - and I'm sure you will have noticed by now, I'm really trying to slice this very complex thing to see where we...

((Crosstalk))

Michele Neylon: (Unintelligible).

Thomas Rickert: Well I better - I think you better say this now, maybe you will have changed your mind in an hour's time. But...

Michele Neylon: (Unintelligible).

Thomas Rickert: Lucky me. But I guess the wording that James suggested is a very good one. I'm not keen on keeping the wording due process. I think the notion is that we have different scenarios in which reveal is requested and that those need diverging responses in terms of process and outcome.

And I think if that's something that we can agree on then the next thing that I've heard you saying where I think might be common ground is that we might

need an authentication mechanism for requesters. Is that something that everybody likes so that there are no anonymous requests? And also that there is an opportunity for service providers to sanction vexatious requests. Is that something that everybody can agree to? Yeah?

No position. So can we agree on a authentication mechanism required for requesting parties? Kiran.

Kiran Malancharuvil: So in principle that's a great idea. Similarly to, I guess, how Mark Monitor feels about the accreditation procedure with the EWG. But that being said, there are a lot of kind of small actors, small firms, individuals that need to enforce in the same way that, you know, a Mark Monitor would, for example. It may be easy for us to get accreditation and not so much for individual users who don't, you know, retain counsel for, you know, financial reasons for example.

So in principle it's a nice idea to kind of gate it to make sure that there's a trusted user system but, you know, that would exclude a lot of people who have legitimate rights and enforcing against these types of individuals.

Thomas Rickert: I might have misunderstood James but I think he's not asking for more than the requesting party authenticating themselves.

James Bladel: If I could respond quickly? I don't think we said that this would be a fee service, that there would be a subscription or something. I think it's more a question of identifying yourself, providing contact mechanisms and having a login, you know, credentials similar to, I think, just about any free web service or app that you would set up to communicate with someone and establish that this request is coming from the person or party who they claim to be. I think that's just - I don't think that's an undue barrier to put on the person who's filing the reveal request.

Kiran Malancharuvil: Okay.

Thomas Rickert: Great. Paul.

Paul McGrady: With a slight tweak that whoever is - that self-authentication doesn't exclude representatives, right? So this is something that we experience all the time in the social media aspect. We're like, oh you're a big law firm and we can look you up on a search engine of your choice and you clearly are not somebody who's going to - you're not a fake person but we still want you to fill out a power of attorney form.

So as long as we're not heading down the path where if Company X wants to submit - wants their attorneys to submit something that we're not going to end up in a situation where, you know, we have extra paperwork to do to prove that we represent Company X or that kind of thing. If it's simply like yeah, my email address works, right? That's a different topic, that's fine.

Thomas Rickert: But as far as I've understood this the idea is not to put you out of business for this type of request. I guess the - the important thing is that the requestor gets authenticated and whether that's the legal representative authorizing themselves or the requesting party itself...

Paul McGrady: Right, just for the record I'm not worried about being put out of business, I'm worried about grandma who's getting phished.

Thomas Rickert: Sure. James and then Michele.

James Bladel: Yeah, just to respond, you know, honestly I don't think we have time to look in and - into all of those requests and figure out all those relationships. I think it's much more of a situation where we want to establish an account, we want to make sure that that account agrees to some provisions for using the service and for making the request and that they're not going to abuse that privilege and it's going to only help, I believe, expedite those requests as we start to build a track record.

And I think that, you know, our privacy service has that facility now probably with some folks in this room, you know, where we say, okay we've already got your check box that says you agree under penalty of perjury or, now borrowing the language from Steve's proposal, that this is a true statement to the best of your knowledge, etcetera.

I mean, if you agree to that once there's no reason why you should have to jump through that hoop every single time. You know, and then - but then understanding that if someone says, you know, this person isn't reacting the way I'm going to submit 1000 abuse complains or, I'm sorry, reveal complaints on the same domain name in a 12-hour period, then that would probably mean that you no longer have that, your account privileges have been suspended.

And I think that's just kind of a way of determining who's using the system in good faith and who's using it to harass others. And if it's free I guarantee you we will have both. So, you know, we just - we have to be able to draw that demarcation. Thanks.

Thomas Rickert: Thanks, James. I have Michele and then Kathy.

Michele Neylon: Yeah, thanks. Michele for the record. Just very, very briefly, this entire thing around authentication of reporters and all that, I mean, at the simplest level, you know, somebody purporting to represent Company X shouldn't be using a Gmail address to send in an abuse report. They should have proper contact details.

I mean, we get in reports from people about things and it's, you know, some random Gmail, Hotmail, Yahoo, or whatever address, there's no telephone number for them, there's no physical address, there's nothing.

Thomas Rickert: I understand the point but I guess that would be more on the implementation side.

((Crosstalk))

Thomas Rickert: I would like to establish some very basic principles and...

((Crosstalk))

Michele Neylon: The thing, Thomas, you know, I think that's what would be our concern. James has gone into it a little bit more detail. You know, I don't think any of us are asking reporters to give over their first born or blood samples or anything like that; I think it's just really a case of you know who the hell is reporting to you, you can actually get in touch with somebody and have some level of assurance that they who they say they are.

Whether they're the person who's directly affected by the purported issue or somebody acting on behalf of somebody, I mean, we get reports from, you know, a multitude of different companies for a multitude of other different companies and that's fine. But, you know, it's just, you know, the proper reporters will have no issue in giving you contact details.

Thomas Rickert: Understood. Thanks. Kathy.

Kathy Kleiman: Okay. Things I don't think we're dealing with: I don't think we're dealing with terms of service and violations under terms of service and actions registrars and proxy privacy providers might take.

To Paul's comment, I don't think we're dealing with phishing. I think there are other - that's an anti abuse that runs to terms of service that I think can get taken down pretty quickly. Perhaps it's the investigation behind the phishing I guess that you're talking about. Kind of who's behind it, is that...

Paul McGrady: Sure, I mean, you want it to stop so you got to figure out who they are to make them stop. Yeah.

Kathy Kleiman: Actually you can go directly to most registries and registrars they'll take it down.

Paul McGrady: Right, but that's taking it down, that's not the same thing as stopping them and, you know, putting together a case for the FBI, whatever.

Kathy Kleiman: Okay. But to me - and I - it wasn't my sense with apologies to James that Domains by Proxy was the - was the baseline that we were hearing on Tuesdays, was, I mean, you have your policies; we're hearing more comprehensive policies, frankly, out of Europe and countries that had data protection laws.

And that makes sense based on everything Stephanie has told us and the data protection commissioners have told us that a reveal has a higher standard in countries with data protection laws.

But let me go back to the due process. And you can call it anything you want but your allegation is that it have - or my client has infringed your trademark. Where is my opportunity to show you I've got a trademark in my country? This is the whole (unintelligible) problem. Where is my - if it's completely ex parte where is my opportunity to say no, it's actually my copyright and you're abusing it.

You know, where the fair use argument? How do I even get to respond before you find out who I am? How do I get to put on the table, no, it's actually all an allegation and it's really my ex husband who's behind it.

Thomas Rickert: Kathy. Can I please ask, we go into the specific scenarios in a moment, right? So for the time being I'd really like to establish some more basic principles. The other thing I heard is compulsory versus voluntary. So I think it can be

policy statement of this group to say that what we're dealing with is only the voluntary part of things so that the - that there are no rules, unless you chose to deal with that, on how to deal with compulsory reveal requests.

Steve.

Steve Metalitz: I'm just not clear on how you're - this is Steve Metalitz. I'm not clear on how you're using that terminology exactly. Are you drawing the distinction between requests that are, you know, like court orders and subpoenas on the one hand as compulsory and everything else is voluntary? Because is that the distinction you're drawing?

Thomas Rickert: Well the distinction is what I heard somebody from the floor say. But I would construe it in a way that a compulsory request is one from a competent law enforcement authority that you have to respond to and I think it's not for this group to prescribe how service providers should be responding to those. That would be subject to the applicable local law.

So if we could clarify that I think that would help a great deal because from what I read sometimes these jurisdictional things and law enforcement requests have been mingled with the private requesters concerns, right?

Steve Metalitz: Yeah, I mean, I'd agree with that, I mean, getting back to one of the first points that James raised; I think there might well be different standards for law enforcement requests. I was just questioning that terminology but I think I understand it now thank you.

Thomas Rickert: So we're talking about the voluntary part. And if I - if I'm not mistaken if it's voluntary then it's something that needs to be enshrined in contractual language.

Steve Metalitz: Excuse me, Thomas.

Thomas Rickert: Yeah.

Steve Metalitz: This is exactly why I raised this question, it is voluntary in the sense that it's not the result of compulsory process from a government official, a government...

Thomas Rickert: Yeah.

Steve Metalitz: ...or a court. But we're talking here about accreditation standards, what rules should you have to follow in order to be a privacy or proxy service provider with whom accredited registrars are allowed to do business. So it's not voluntary in that sense; we're trying to come up with rules that you would have to follow if you want to be accredited.

Thomas Rickert: Yes, and...

((Crosstalk))

Steve Metalitz: ...that adjective is a little bit misleading.

Thomas Rickert: Okay so I - I'm okay with that description we use for it. It would be everything other than compulsory law enforcement requests. What I'm trying to get to is that for the accreditation standards I think the processes that we might come up with, the procedures for different types of categories of requests, would need to be put into contract language by the privacy and proxy service providers because at least in the jurisdiction that I come from if there is no legal reason, legal ground for disclosure of personal data, then you need to have a contractual basis.

So we would need to hard code that into the contracts by the - or make it a requirement for privacy and proxy service providers to have those in the contracts with their customers.

To illustrate this, the accreditation framework could say, "You, in order to be an accredited privacy and proxy service provider, you need to have the right to disclose information upon - when certain scenarios are present." And then the customer knows exactly what he's up to and then you - as a service provider you would have a sufficient ground to disclose the public data - to disclose the personal data of the customer. Right.

So I think procedurally what we need to work on is putting something into the accreditation requirements that would go into the contract language with the customers. Isn't that right? Steve.

Steve Metalitz: Yeah, I think that's consistent with the preliminary conclusions we've already reached which are that - at least - it's - here it's the form of a recommendation, and maybe you're right that it should be stronger than that. But the working group recommends that accredited providers should indicate clearly in their terms of service the specific grounds upon which a customer's details may be disclosed or published, those are both defined terms, or service suspended or terminated.

So I think we're already there to say that whatever the rules are they should be spelled out in a contract in terms of service so that customers know what the rules are. I think that's what you're suggesting.

((Crosstalk))

Man: What were you reading from, she asked.

Steve Metalitz: I'm reading from the document that - the preliminary conclusions to date on Charter Category F. And it's in bold at the bottom of the third page.

Thomas Rickert: If it were for my liking I would make this stronger because I think, you know, again I'm trying to test the waters with the whole group whether that's a notion that you can all subscribe to. Kathy.

((Crosstalk))

Kathy Kleiman: Jumping into implementation. I'm not there yet. I thought we were on principles (unintelligible).

Thomas Rickert: But I guess we need to be clear about the mechanism that is to be applied. I think it's not good enough of a service provider to say okay I will disclose if Steve sends me a notification and if he puts this and that information into it. This is something that needs to be translated into the customer contract so that the service provider is protected legally. Otherwise there would be no ground for disclosure.

Kathy Kleiman: But (unintelligible) what it is we're agreeing to and then talking about how to implement it.

Thomas Rickert: And that's what we're getting to now because the - I think once we know what we're discussing and what we're not discussing, which I think we've reached some clarity on now, we should now go through the various use scenarios, i.e. trademark related reveal requests, copyright related reveal requests and whatever scenarios there might be.

I mean, it's just a proposal to the group to do it that way. But I just wanted to set the scene that at least in the jurisdiction that I come from it would not be good enough for the privacy or - and proxy service provider just to have something in their drawer as to how they should be dealing with things. This would need to be translated directly into the customer contract for - to protect the privacy and proxy service provider from doing unlawful disclosure of customers' credentials.

Holly.

Holly Raiche: But can we do that for a global document? I mean, I understand the need in Europe to do that given the European directive on privacy. I don't know that that's necessarily a requirement in Canada or with the US or Australia or whatever.

I also think if we kind of go back a ways somewhere in the deep dark past we tried to talk about all the kinds of abuses that might engender this kind of response and I don't think we could ever reach our final list and I don't think we will. I think we can talk about examples but I don't think any service provider can come up with a terms of service that says if you - I deal with trademarks this way, I deal with copyright this way, I deal with - and then have this long list of abuses and say this is how I'm going to do it.

I don't think, you know, that's moving from high level principle to real detail and I don't think we can do that here. I think particularly when each of the service providers in the list have said when I get a request to deal with something it's dealt with on a case by case basis.

So already we have got the understanding that if there's a matter that is raised that is serious it is usually dealt with individually and in accordance with whatever processes and, you know, what the size of - and makeup and skill of whatever service provider.

So I don't know that we can actually do what you want. I think what Europe wants is one thing; I think what we can do is something different and higher level.

((Crosstalk))

Steve Metalitz: I think - if I understand it I think the point Thomas was making was a little bit different which was that whatever the rules are and at whatever level of detail they can be spelled out they should be communicated to the customer in the terms of service.

I'm not sure whether that's - I'm sure that's not a legal requirement in every country but it's - I think it's a fair - it's a question of fairness to the customer as well, by the way, as to third parties.

I mean, we right now have a specification that basically says that a service provider that's affiliated with a registrar under the 2013 RAA has to - already has to disclose this. It's pretty general, the requirement and the way it's being implemented maybe is very general for some providers, but we already have that under the interim specification.

Holly Raiche: I'm not disputing that at all. But I think what I am saying is that Thomas was talking about a level of specificity that I don't think we can do. I think what James was talking about, which is a whole process, we can describe, that's fine. We can talk about examples and that's fine. But I don't know how, around this table, we can get really specific. I don't see it.

Steve Metalitz: I'm with you on that as, in our proposal we said here should be the general policy and here's some illustrative examples. I agree with you, we can't cover everything. Ideally we would cover more than what we've just listed because that's only a small part of the universe. And, you know, Michele suggested maybe stopbadwork.org has some principles that could be adapted, maybe, I don't know. But I agree with your point that you're not going to cover everything.

Thomas Rickert: Back to my original suggestion, this was primarily for transparency reasons and in my jurisdiction it would also help to protect the service provider. If you have other requirements in your local jurisdictions you certainly need to apply them.

But I think for this group, you know, as we're hopefully coming to a point soon when we're recommending policy, I think it would be appropriate to require the service provider to detail exactly to the customer what's going to be -

going to happen. That can certainly be abstract general, it doesn't have to be concrete for every thinkable instance of request.

But just to give you an example, I know privacy and proxy services terms and conditions that say, okay, if we are being notified of abuse or if we are confronted with reveal requests, this request has to be - has to specify the potential - or the alleged infringement in sufficient detail that allows for very fine whether the breach is present or not.

So if you just say I don't like what's on the Website, right, that wouldn't be sufficient but you need to - let's say it's a forum where information is allegedly taking place then you would need to specify which block post or which forum post is concerned, why this is infringing upon some third parties rights and what have you. So it needs to be sufficiently detailed.

Then you can have a rule whereby you notify the beneficiary owner of the domain name, give him like 48, 72 hours notice to respond to the request and if there is no response let's say then you would proceed one way or the other. You know, you can flesh out general approaches to how to deal with those things that might be applicable to all cases.

I'm not saying that we should agree on exactly that but I think we have to find one way or the other to specify or to narrow down how providers should be dealing with certain cases of allegations. Unless, Holly, you have an idea of how we can...

((Crosstalk))

Thomas Rickert: No, but I'd like to hear from you since you said that, you know, this all has to be dealt with on a case to case basis. I think if we leave it like that we will never get to policy recommendations.

Holly Raiche: What you were saying is individual providers can tell their customers what their policy is in relation to certain things. I - around this table the best we can probably do is say you should be reasonably clear about how you will deal with allegations, what has - that in fact there needs to be sufficient detail and some of those things. I don't think we can go any further than that.

And we're not going to - you know, I'd be surprised if any service provider could list all the kinds of abuses that will come across their table that they will deal with. It will be, from what I read on the list, it's a case by case decision making, things are certainly taken into account.

What I think Kathy was talking about and I was talking about is in some - in many situations, unless the criminality is blatant, that customers should be able to respond individually or through their representatives or whatever and maybe that's written in, in some fashion.

There are some high level principles but I think we're dangerous asking for more than high level principles. And I think it was a dangerous saying to the service provider, you must list what you are going to do in every circumstance because I don't think they can. But see, Graeme is very helpfully going no which tells me I'm on the right track and I can't see what James is doing but I suspect he's also going no.

James Bladel: Raising my hand.

((Crosstalk))

Thomas Rickert: Don first.

Don Blumenthal: Graeme.

Thomas Rickert: Graeme. Graeme, James and...

Graeme Bunton: Sorry, this is Graeme. I didn't have much add other than, yes, I agree, it would be extremely difficult to list our responses to the incredible variety of things that come into us.

Don Blumenthal: I generally agree with - I have troubles with the feasibility of saying anything more as a policy matter than you must list your terms concerning disclosure and concerning publication. But is it possible rather than suggesting we will do this for copyright, we'll do this for abuse, we'll do this for criminal activity, to suggest certain categories. And generally this is what we'll do with intellectual property, allow that to factor in Kathy's concerns, do something similar with other types of activity.

I'll be honest, I'm throwing this out as a possibility. I'm a little bit skeptical. But if we could find a middle - the thing I'm concerned about is if we just say you've got to lay out your terms and services certain protections will escape too easily.

Thomas Rickert: So I have a queue. James, Paul, Kathy and Steve.

James Bladel: Hi. So James speaking. So I got a solution for the terms problem that Don raised but you're not going to like it. And it reads something like, "Domains by Proxy, in its sole discretion, blah, blah, blah, blah, blah."

And let me put that out there because I am kind of being serious. And to respond to Kathy and Wendy's points and I think Holly's as well is I understand as a consumer that I shouldn't be subjected to these mechanisms simply based on a complaint; I should have some opportunity to respond or take some sort of corrective action.

But I also want to point out that we are a service provider; we are not delivering or designing a bullet proof service, you know, like you might see in some offshore, you know, we are ultimately going to have some reasonable limitations. I think that, for example, the process by which a respondent could

block us from revealing a name or, you know, something like that - that sounds like something I frankly don't want to manage.

I think that we can give them a choice which is you can cancel this Website or you can have your name revealed or you can find another service provider that feels differently about these things. I mean, we can lay these options out and give them a window to respond and say if, you know, if the name is still active on such and such a date we will follow through with this.

I feel like we're being dragged into an area that as a business we don't want to go, you know, which is - and particularly if we're dealing with law enforcement, especially if we're dealing with law enforcement where it's like either contribute to the crackdown of the secret policy of some state or hide a dissident or, you know, and the answer is we don't want any part of that, you know, we are commercial entities here; we're not, you know, we're not the Vatican Embassy, you know, where these folks can hide.

So I'm just putting this out that when we get into these situations and these scenarios I think that we can offer providers, I believe, are putting ourselves out there that we can offer reasonable protections and reasonable services for the vast majority of customers who simply want to operate with some reasonable degrees of privacy.

But it's not going to be bullet proof system that stands up to every conceivable legal maneuver, you know, pro or con and as a service provider we certainly don't want to be a party to that. Thanks.

Darcy Southwell: Darcy...

((Crosstalk))

Paul McGrady: Yeah, it was Darcy then me.

Darcy Southwell: Darcy Southwell. So a little bit to James's point but also to what Holly said, when you think about a high level global policy that we'd be looking at in the accreditation program one of my concerns, and this is just the best example off the top of my head is the laws between countries are very different.

And if you have a defamation claim that comes in, for example, and it's a US customer and we are a US-based company the defamation laws in the US are very specific. And we have no obligation to take it down and no liability to take it down because it's not assumed to be true. Ireland is exactly the opposite; it is assumed to be true.

So as a US provider - and we learned this the hard way - that our customer in Ireland brought us into that lawsuit because our customer had posted something online that was considered defamation under Irish law and we got pulled into the lawsuit and held liable for it because we were the service provider.

And that's where when we talk about a global policy for accreditation that's where I get concerned. I don't know how we can address that level of detail at a high level policy. Providers should definitely, I feel, have a plan of what they do in those scenarios and this goes back to the case by case basis that all of us responded to on the list when we gave details about how we handle cases. And that's one example of why it's case by case.

Paul McGrady: So I sort of feel like we're - everybody wants a set of custom clothes. But could we - maybe we should just sort of build one out, right, build out copyright or build out trademark or build out defamation or something.

And then, you know, get comfortable with the timeframes and the who does what and who says what back and all that rather than trying to put together a very unworkable global list of everything that could go wrong and we start down the road of, you know, actually stitching something together that might work for 90% of the situations that we encounter.

Thomas Rickert: Steve.

Steve Metalitz: Thank you. Steve Metalitz. I just want to pick up on something Darcy said which is, yes, in some cases the laws are extremely variable from country to country. In other cases the laws are rather uniform from country to country.

One hundred and sixty countries are members of the Bern Convention, which is the premier international copyright treaty. All of those countries are obligated to protect the copyrighted works of foreigners on the same basis that they protect the works of their own citizens at least as good a basis. And they have minimum standards for what types of rights need to be recognized and so forth.

So there are some areas that are fairly uniform and don't raise big jurisdictional problems in terms of figuring out what's illegal activity. So maybe Paul's right, we should build out a couple of - a couple of examples. But I just want to make it clear that - and I'm not sure if Don said this or somebody else, but this can't be limited just to requiring service providers to explain and disclose what their standards are and what their processes are. We have that already, it's called the Interim Specification.

And we want to move beyond that if we can and the goal from the perspective of copyright owners is so that a copyright owner who let's say sees her work thousands of copies of her work being made available on a Website, that's registered through a proxy or privacy service, can have some predictability and some expectation about what she needs to bring forward in order to find out who that person is and therefore find out what remedies she might have against that person or even just persuade the person not to continue this massive infringement.

So predictability and some level of consistency is important here. So it can't - I agree with James that you cannot take discretion out of this. And we

shouldn't be trying to do that. But on the other hand if we just leave it up to discretion then we don't have a satisfactory outcome and we're not one step farther ahead of where we are today. Thank you.

Thomas Rickert: Thanks, Steve. I have Wendy and then Kathy.

Wendy Seltzer: So I think we're - we are all looking to build a predictable process and I think we're also not looking to set a one-size fits all business model. So the process and the accreditation rules should permit different registrars and different proxy and privacy service providers to adopt different levels of protection for customers who might well pay different prices for those services and see different options and choose among privacy and proxy providers based on what sorts of guarantees they offer for, you know, levels of response based on the complaints and the registrant's preference to respond or move to quash or have names removed.

So I think we can look for baselines that offer the opportunities to protect those interests and set out procedures by which there's a predictable set of escalation steps depending on what regime the customer and privacy and proxy provider have set up.

Thomas Rickert: Thanks, Wendy. Kathy.

Kathy Kleiman:: I agree with what Wendy said. And so the predictability, the escalation, that's what a number of people in the room are looking for. And what James said that there are scenarios - or it should be part of the process, and we're not talking law enforcement here, let's take law enforcement and abuse out, requests from third - by third parties for reveal.

So if I understood what James said correctly that providers go to their customers and ask, you know, there's a reveal request, you know, do you want to, you know, we're going to reveal an X number of days. Do you want

to take it down? Do you have a response for us? Is there some kind of court action?

I'm not sure I understood that correctly but that's the idea of the opportunity of a response. And, by the way, you guys know what happens when, you know, registrants and customers are given the chance to respond to UDRPs, they don't. So that time for response I don't think nullifies in any way what you're trying to do.

But it does add that layer for those who choose to respond to say look, I've got a trademark in Holland and, you know, or, you know, in Eastern Europe that you might not know about so that exercising rights under the treaty to let you know that there are conflicting rights.

Thomas Rickert: We are - we've already...

James Bladel: Can I just respond really quickly?

Thomas Rickert: Yeah.

James Bladel: I think my - one of my central points, Kathy, was that we don't want to manage that back and forth respond, not respond, whatever. I think as a provider we want to say we've received a request to reveal your contact information and we believe it's legit and we're going to comply on this date if this site is still active.

So now the customer has a choice, and I believe if they believe they have a valid competing trademark then they say go ahead, publish - tell them who I am and I'll tell them who I am and I'll tell them what my trademark is and where it is.

And if they believe that it's part of a persecution and it may be a threat and, you know, then maybe they say well, you know, maybe this is more law

enforcement than copyright, they say, okay, then I'll cancel it. But the choice is back - I really - this third option of they get to send something back and then they send a motion and we are kind of the, you know, monkey in the middle passing these things back and forth between these different courts, I don't want the providers - as a provider I don't think we want any part of that.

Kathy Kleiman:: But if the court is literally a court, I mean, I rather than a tennis, you know, tennis court; if we're saying someone files a motion to quash and you get a court order that says, you know, there are not grounds for this right now, then you're - then you're completely supported...

((Crosstalk))

James Bladel: We follow court orders if they are in our appropriate jurisdiction.

Thomas Rickert: Unfortunately time is up already. I was surprised to look at the - at my watch, time flies if you have fun isn't it?

((Crosstalk))

Thomas Rickert: Nonetheless, you know, I'm allowing myself to cut a little bit into the break because we started a few minutes late. I think the - nobody would object to the service provider doing things that they need to do to limit their liability risk, right so the information in Ireland question, I think was an issue where you didn't suspend the side, it was not related to reveal. Is that correct?

Darcy Southwell: There were a number of issues.

Thomas Rickert: But I think that needs to be taken out at the equation in so far as certainly if there is illegal content on the Website then other parts of the terms and conditions whereby the service provider can suspend a domain name would be applicable, right? So for - is that something that everybody would agree to?

So what I'm hearing from what you said is that we would need some sort of process whereby if an allegation is made the beneficiary owner gets an opportunity to respond. And that is notwithstanding the right to maybe suspend the domain name in the meantime.

You first and then James.

Alex Deacon: Hi, so it's Alex. So again I just want to - at the risk of repeating myself, which I know we agreed not to do that, I think that the opportunity for the domain name owner to reply it's to say that they have a trademark claim in some other jurisdiction would be during the relay conversation which doesn't - which doesn't involve the service provider, it's this one on one conversation that we wish to have with the person on the other end of the proxy service.

So my - maybe I'm being optimistic here but my hope would be that we wouldn't get to the point where we have this ping pong during the reveal phase if information like that was made available to the complainant earlier on during relay.

Thomas Rickert: So do you think it's common sense that relay must have taken place prior to reveal?

Alex Deacon: No.

Thomas Rickert: Because that would - the assumption if...

Alex Deacon: Well I would let Don answer that.

Thomas Rickert: So I have James and then Don.

James Bladel: So I just want to mention - and I think it's going back to the exchange Kathy and I were having is that the status quo today is that when we receive a

complaint like that we cancel the service, so it's publication not reveal, and it's immediate.

And I'm thinking that the giving a 7-day window, I'm just throwing a number out there - a 7-day window to make a choice, as Wendy was saying, to prioritize what do you value more, your content, your website, your domain, your privacy, you know, make a choice, something - if you want to throw something overboard.

I think that is a huge step up from where we are today which is publication - immediate publication versus delayed reveal to a single complaining party.

Thomas Rickert: Don.

Don Blumenthal: Yeah, I think we have to decide here if we're going to do the categories I suggested or not because the fact is this discussion is about 95% premised on intellectual property issues and maybe reveal is necessary.

But the unequivocal answer to what Thomas just said here in the views of law enforcement situation is no, reveal cannot be a precondition to a - relay cannot be a precondition to disclosure publication. Yeah. Voluntary or not if you put in a relay request the target will be gone. There's just no purpose to the relay request.

Thomas Rickert: But, Don, just for me to - I thought we had focused our discussion on everything that's not law enforcement related, right?

Don Blumenthal: But this is - but let's make two distinctions here, abuse is not law enforcement. Abuse is the anti-phishing working group, it's Spamhaus, it's the Internet - a company called Internet Identity, it's private organizations who are fighting abuse on the Internet. It's law enforcement coming in with a voluntary request. And there's no legal compulsion to respond, it's help us out here.

Thomas Rickert: But then - am I correct in assuming that there is no consensus on a relay requirement prior to reveal? I mean, there could be a statement. And I think that...

Alex Deacon: We have to divide it.

Steve Metalitz: I mean, we - in fact on the screen right now in deciding - this is our preliminary recommendation it would not be that you would require reveal. Deciding whether or not to comply with the disclosure or publication requests providers not mandate that the requester must first have made a relay request.

I think it's really going to - that may vary depending on the type of complaint and - so at this point what this body preliminarily decided several months ago was no, it's not necessarily an escalation situation. We could revisit that but that's where we are now I think.

Thomas Rickert: But I guess that having listened to this discussion I think there's no momentum for revisiting that is it? James, very briefly because...

((Crosstalk))

James Bladel: I wouldn't say momentum, but I think I'd like to understand, you know, I mean, I wouldn't say it's a prereq but I think that if we're going to hold this out as reveal is a more drastic measure then we need to understand what the relationship is to a failed relay attempt.

Thomas Rickert: It's a good thought. I think we should break for 10 minutes and then reconvene with the presentation on the accreditation framework. Thanks, everybody.

END