# WHOIS Working Group
# Teleconference
# TRANSCRIPTION
# Wednesday 6 June 2007
# 13:30 UTC

**Note:** The following is the output of transcribing from an audio recording of the WHOIS Working Group teleconference on June 6, 2007, at 13:30 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/whois-wg-20070606.mp3
http://gnso.icann.org/calendar/#jun

Attendance:
Philip Sheppard - WHOIS wg chair
Yaovi Atohoun - observer
Carole Bird - observer
Patrick Cain - observer
Andrew Denholm for Leo Longauer - observer
Avri Doria - Nom Com appointee to Council
Wout de Natris - observer
Christopher Gibson - observer
Lynn Goodendorf - observer
Palmer Hamilton - CBUC
Doug Isenberg - IPC
Susan Kawaguchi - CBUC
Tom Keller - registrar
Dan Krimm - NCUC
Steve Metalitz - IPC
Milton Mueller NCUC chair - wg chair
Margie Milam - Registrar/IPC
Kari Moeller - observer
Lane Mortensen - observer
Jon Nevett - registrar
Richard Padilla - observer
Kristina Rosette - IPC
Melissa Rotunno - observer
Adam Scoville - observer
Suzanne Sene - observer
Ken Stubbs - registry constituency
Michael Warnecke - observer
Shaundra Watson - observer

ICANN Staff:
Maria Farrell - GNSO Policy Officer
Glen de Saint Géry - GNSO Secretariat

absent apologies:
Jon Bing - Nom Com appointee to Council, chair sub group C

Maria Farrell: Right. Someone sent us out an agenda yesterday. Maybe we might go through the agenda before we start.

Philip Sheppard: Yes, I can happily do that once we're ready to start.

Maria Farrell: Right.

Philip Sheppard: And today is merely a planning and stitching together call. I think is how we can describe it.

Coordinator: Please (decease) instruction. (Unintelligible) joins. Thank you, Sir.

Philip Sheppard: Hello everybody and welcome and we're a group of about 30 or so at the moment and maybe some more people joining us as we go along. And it'll be noted in the record of discussion.

I have circulated a brief agenda for today and what I was really sort of planning on doing overall is doing sort of more of planning and sort of quoting session, really and looking at how we sort of perhaps stitch together the three reports that we have from our subgroups.

And hope that in that process we can make perhaps some elegant patchwork quote from this subgroup reports and have some structure and form to it. And I hope we won't end up stitching together something that just like with Frankenstein monster.

In the second, I think, for the agenda, I was planning on having just each of the subgroup chairs or their substitutes giving an overview in terms of whether subgroups have got to - not a full treaties and the written reports - just about five minute each, on each of the subgroup reports A, B and C - just a brief discussion of some sort of parallel or tangential issues that have come out of some those discussions and relate to some of the overlap issues. And then looking at some ideas of going forward and how we start to structure putting these three things together in ways that are going to be digestible for us going forward.

So, that’s the plan to do with the agenda. We should be on for about an hour. So, and if I may, and first of all, I like to thank all of our three subgroup chairmen very much for the work they put in and while the short period of time, I think we achieved some excellent results. So, thank you very much to Steve, Milton and to (Jon).

And perhaps, on that, so take it in order, (Steve), if you could give us a quick sort of, you know, summary of where your group got to in its deliberations in about sort of speaking for it right about five minutes, I think.

Steve Metalitz: Okay. Thank you, Philip. I think subgroup A has made some progress as far as we got. I think we left a number of issues that we hadn’t discussed in great detail. We at least have framework for further discussion.

We identified the – our task of finding roles, responsibilities and requirements back to the OPAC since we were talking within the context of the OPAC proposal. It really broke down into four major questions, who the OPAC is, what issues the OPAC is required to handle and what it's required to do, when must the OPAC act and how would these responsibilities be enforced. And what happens if they're not built.

And we had two main proposals that we drew from, one, from Steve DelBianco, one from Christopher Gibson. And it quickly became clear we're talking about three basic functions which we defined in the report at least to some degree, the real life function, a reveal function and a remedy function.

So, the first one communicating back and forth to the registrant via the OPAC, the second is, the circumstances under which the – someone who makes a request is provided with the contact information on the registered name holder that's not part – no longer be part of the publicly accessible list.

And the third, is remedying the problem which could involve suspending the registration, making a site domain name resolves go dark or other changes to remedy a problem then applied.

Philip Sheppard: Right.

Steve Metalitz: So, that was the basic framework that we used. I think we got farthest on the first couple of question about who the OPAC would be, what capabilities it would have to have, in other words capabilities to carry out these functions…

Man: (Match). Sorry.

Philip Sheppard: Carry on, Steve.

Steve Metalitz: Okay, what relationships it would have to have both to the registered name holder, to the registrar, to ICANN. There were some discussion about whether OPAC should be accredited or whether by ICANN or whether simply the registrar would have some responsibilities to make sure that the OPAC listed was somebody who can carry out these functions.

And then the "what question" of age five over the…

Glen de Saint Gery: (Gary Moore) now joins.

Steve Metalitz: …really helps to spell out the circumstances in which these different functions would be actuated - the relay function, reveal function. I think the remedy function is probably the one we talked least about beyond some level of agreement that it would be reserved only for really serious cases such as a phishing situation.

And we had some discussion about the timeframes, how fast the OPAC would have to act. I don't think we reached any clear agreement on that but the framework that we talked about on our last call is laid out in the report. And another proposal was received after our last call. And that is we have a link to that in the report.

And finally, on enforcement, I think the general idea was there will need to be some type of backup if the OPAC failed to carry out its job. And likely, that backup would (reach) through the registrar. But there obviously could be some role for ICANN as an enforcer of last resort.

There was also some discussion about overlap of what we did with both the other subgroups. First, the overlap with regard to the reveal functions with the work of subgroup two. And second, the overlap with regard to enforcement with the discussion in subgroup C regarding who really would be within the OPAC system would a registrant who was not a natural person or who was carrying out commercial activities even in designating an OPAC.

And if that were the rule, then you would need to have some enforcement mechanism for registrants who improperly designated an OPAC rather than making their contact information available in WHOIS.

So, within the time constraints, that's a brief summary of a rather somewhat rambling report. But I think we did make progress in some areas. There clearly are a number of areas that need further discussion.

Philip Sheppard: Steve, no thank you very much, I mean, I – I surely – I think that report actually made some very good progress particularly in the way that you categorized it. That was helpful for us and certainly identifying the overlap issue is of particular use for my work going forward.

Milton, subgroup B.

Milton Mueller: Okay. Our subgroup was concerned again with which legitimate third parties may access registration data that might be shielded by the OPAC. We first developed a template so that people could make the sort of proposals as to how they wanted that problem to be solved. And we received ultimately 11 proposals and those are all included along with our report.

Basically, the discussion mostly ended up focusing on how to define or recognize legitimate third parties and on the question of what type of access those parties might receive.

In terms of eligible third parties, we started out with the pretty firm, I think, and well agreed distinction between public law enforcement agencies and others. We define what we mean by those in the report. But we thought that there was – in terms of the categorical distinction that that was the most fundamental one.

And there was pretty good agreement that law enforcement agencies should be granted access to the data elements although variation in views about how restrictive those conditions might be. There was no, I think, fundamental or principled objection to that.

And we also felt that there might be some kind of basic institutional framework in place for identifying who would be qualified to be classified as a public law enforcement agency although that would need to be explored and examined in greater detail. And there was mention of Interpol in the financial agency…

Coordinator: Adam Scoville now joins.

Milton Mueller: …that interface with the Interpol in that regard.

Now, when it came private parties of course, as you might expect there was a lot more divergence of opinion. I think in some ways we were sidetracked a little bit by talking about who the private parties might be and people listing categories of private parties rather than what kinds of legitimate needs they might have and that would justify access and how those needs would be vetted or identified.

Anyway, we didn’t make much progress on that. Most of the proposals from business constituencies proposed some form of self certification and affidavit with some kind of exposed threat that that access would be withdrawn if there was an abuse of the access privileges. But there was no agreement on the merits of relying on self certification.

And this discussion of private parties was complicated by the fact that we had a couple of advocates of special sectoral approach in particular, banks. There was certainly support for the idea that the phishing that target banks is a problem that requires origin detention.

There was report for the view that the working group however should not necessarily devote its time to a sector specific bank proposal. The good thing about the bank proposal is that it's possible to reliably certify what is a bank at least within the US legal framework and probably in Europe and most developed countries as well.

But most people thought that the solution that would encompass all legitimate private party users would be preferable. However, there was an ultimate view that a proposal narrowly focused on banks could be used as a model or test case.

I did not make good progress in terms of identifying the different degrees of access that might be granted. And here's where the overlap takes place with potentially with subgroup A.

But we identified three basic kinds of access - four if you include indirect access through government. What we call type one access is restricted and incident based. You – access is limited to the record of a particular domain and/or registrant causing problems. A specific request is made to a gatekeeper for those domains.

We note that this can't be provided by port 43 and this type of access could incorporate a two tiered process in which a manual review gets certain entities access to an automated query screening process.

Type two access, we considered – in which you have query based access to any domain but you are somehow contractually or legally restricted to making queries to the records of particularly domains or registrants needed to support a specific investigation. And this would require some kind of auditing regarding which queries are made by users.

And we recognize that there are special cases in which law enforcement agencies - the auditing rights have to be limited because of say, national security or something like that.

Type three access, we classified as what we have now. And what we called type four access which could be considered a special case of type one is indirect access by means of governments where private parties obtain access to the shielded information through their governments or some kind of agency designated by their governments under national law.

And after discussing these types of access, we agreed that law enforcement agencies at the very least, should be granted type one access, the support for granting them type two access and that ultimate view that they be granted type three access.

With respect to private parties, the business users made it very clear that they favor the status quo in WHOIS but it's going to go with the recommendation. There's agreement that private parties should not be granted type three access.

And there was a basically equal division between participants who support giving private parties some kind of type one access while others support giving them type two access.

Now, note that type one access could be provided to what subgroup A calls a reveal mechanism. In other words, you're basically making a request of the OPAC and OPAC is then giving you the shielded contact detail.

Also, I noticed in your agenda Phil, that you mentioned tiered access as possibly a separate agenda item. I would think that most of what we were talking about in this subgroup would classify as various flavors of – or variance of tiered access. And I…

Philip Sheppard: Yeah, No. If I try – it was already overlap issues of tiered access are coming to there so, I think on some of those indeed (they are) identified.

Milton Mueller: Okay. So, the tiered access group gave us a report very late in our deliberations and I submitted it to the group but it's not really - wasn't discussed by us. Tiered access group is maybe something you want to explain later. Or do you want me to explain who that is now.

Philip Sheppard: (Unintelligible) who that is, why not.

Milton Mueller: That was a group formed around the initiative I think of VeriSign and some registries but included most other stakeholders except perhaps for the privacy advocates. And they discussed the mechanisms and the practical issues associated with delivering tiered access.

They didn't reach any conclusions either but they have a report with a pretty good sort of description of the landscape of the problem. So, I forwarded it to our group but we didn't really discuss it. I think that's all.

Philip Sheppard: Okay. Thank you very much for that. Now, subgroup C. I think (Jon) is not with us because he's traveling if I recall correctly.

Glen de Saint Gery: (Unintelligible).

Philip Sheppard: Yup, okay. So, then let me do my best to sum up where he got into some extent, he had one of the easier jobs in it - sort of scoping the issue.

And I think came up with a couple of interesting conclusion. I mean, C was charged with a question should the distinction be made between the registration contact information published based either on the nature of the registered name holder or the use of the domain name.

And I think going down that road, they made some useful distinction between the concept of natural or legal person, and natural being real people, legal persons typically being organizations of some form.

And commercial or non-commercial activities, distinction there of course was that a natural legal person is a historic fact about the nature of the registrant. Where the second distinction dealing with commercial/non-commercial activities for example is more difficult because it relates to things like the future intent of use of the domain name and therefore, already assuming that there will be a website based on that domain name.

On the basis of their discussions, it was generally agreed, I think, by the group that certainly making the distinction between natural and legal person had much greater simplicity and areas of ease of verification. And had a certain sense in that there was a connection to - between legal person or actually natural persons and data protection legislation typically found in many legislations who are called data protection legislation is normally focused on legal person or real people and therefore privacy of data is typically focused on that area.

And on that basis, they came up with one option which I think had produced reasonable agreement within the group which was I think in the case of legal person or an organization, there should be full disclosure of the data as we have today and only in the case of natural persons should there be the concept of retain the disclosure of data.

The group then also discussed if it was possible to make such distinctions with commercial/non-commercial activities. So prior to that, they had also recognized this – the simplest way for distinction to be made should be by self declaration by the registrant to the time of registration. So there was a trust issue in terms of how the registrant was declaring.

So, on the second item, now looking at the idea of whether or not a distinction can be made between commercial/non-commercial activities. And there was a list of various things that could be used to help define whether or not commercial activities taking place such as offer of sale of goods or services, (unintelligible) of extra money, marketing activities and so forth.

And on that basis, there was a - they've agreed to produce which was still linking back to the concept of legal persons and natural persons as well. And then saying, and what happens if those people are engaged in either commercial activities or non-commercial activities and (unintelligible) come after that in terms of how disclosure of WHOIS data set should look.

But it has to be said that there was recognition on the group that this was much problematic in terms of describing, verifying and also recognizing that - even if it's true, one day it may well change to the next.

And finally, I think the group recognized that in the case of data that was either declared and that was inaccurate through either good intent and inefficiency or bad intent and there should be some sort of challenge procedure and they recognize that link back to that sort of activity that was happening in working group A.

So, again, my thanks to (Jon) for doing this. What I want to talk about now, and just ask some questions to the group as a whole is relating to some of the sort of side issues that have come up from that. So I just listed on the agenda three things that I thought that had come up that have some relevance which are proxies - what would be the future fate of the admin and tech contact and the linkage in particular of - between subgroups A and B in relating to ad hoc requests for full WHOIS data.

Perhaps it may be useful to state that in reverse order and if it was possibly logical from the reports you've just heard. And I just wanted to air the fourth that as we tried to put all these three ideas together. Would it make sense to always think about integrating the four ad hoc requests as one off request for data, integrating the work that came out of the subgroup B on tiered access with the mechanisms that were being discussed for those with the queries within subgroup A.

My feeling was this sort of yes, that seemed to make sense, whereas access to bulk data sort of either the whole data set or limited part of it as Milton described seemed to have a different flavor to it and therefore a different process could be structured for that.

So those, does that fourth make sense, your comments on that?

Milton Mueller: Phil, I guess I'll take up the government.

Philip Sheppard: Okay. Milton, let me just take a list of those who want to talk, who else?

Steve Metalitz: This is Steve. Could I get in the queue?

Philip Sheppard: Steve, yup. Who else?

Okay, gentlemen. Begin Milton.

Milton Mueller: Yeah, I think there's a natural intersection here that is the operational point of contact ideally should be somebody who's in a good position to reveal the shielded data. And that the issues that we ran into again, and to which there is no easy solution to is how does person determine (unintelligible) thus would be dissatisfied with the system in which the OPAC simply gets a request and says, “oh, here's the so-called private data.”

And then other people, you know, who are constantly trying to fight lawbreakers are going to be concerned about a situation which makes that into a month long process. We need to have a clear criterion. But clearly, since Port 43 does not provide any authentication mechanism that a manual process that works through the OPAC and is, you know, sufficiently guided and protected so that it only reveals the data under the proper circumstances I think is one of the big solutions to providing type one access.

Philip Sheppard: Okay. Thank you for that. Steve.

Steve Metalitz: Yeah, I think – just picking up on what not was the last comment, I think this is kind of the type one access that was discussed in subgroup B. We made a stub in subgroup A at kind of sharpening this to identify what types of activity we were talking about. And we borrowed from the registrar accreditation agreement that user phrase that at every quest about one of these issues would have to be accompanied by reasonable evidence of run for registration user activity.

This is all in the definition that was actually in Chris Gibson's proposal about request raising legal issues, what that means. And so, presumably there would be some request that didn't qualify. And those would not have - at least not right away – at least they reveal (for you).

But those that did qualify the OPAC would make that determination and reveal the data. Again, this is based on something in the registrar accreditation agreement now that's applicable to well…

Milton Mueller: Steve, you're fading in and out. Are you moving away from your phone or something?

Steve Metalitz: No, I'm not. But I'll try to keep my voice up. Just to say that this – we borrowed that phrase "reasonable evidence" of actionable harm is the phrase that's now on the registrar accreditation agreement. I think it was kind of flag and falls to (Horu's) must made document that he circulated to this working group even before the subgroups were started.

Philip Sheppard: Okay, that's helpful. And the other quick question I had also was would it be reasonable to have a different test or different reaction to an individual inquiry that's concerning the accuracy of the WHOIS data that's displayed that is alleged legal activity on the website under that help was also perhaps in the mechanisms there.

Milton Mueller: Well, I thought we were just talking about access to the shielded WHOIS, the contact information on the address. But I thought…

Philip Sheppard: Yes, but it's a reason – so my question (unintelligible). It was a reason behind asking access for that. And if it was simply saying, “Hey look, the WHOIS data hinge backward. I'm sure this person is really a company” for instance. Or and I just it seem that address doesn’t seem to be correct versus I didn’t like what they do on their website and should the test that you like call the mechanism be different.

Milton Mueller: Well, I thought we already had a mechanism for challenging the accuracy of WHOIS data?

Philip Sheppard: Yes we do, an existing mechanism. Yes, I mean, perhaps the question is (unintelligible) of them should there be any change to that merely – that process would go there a little (part) in the future. That’s the way things turn out.

Steve Metalitz: Milton, could I get in the queue on that?

Milton Mueller: Yes, Steve, indeed. Yeah, anybody else also? Okay, I think there's two.

Steve Metalitz: I think in the OPAC environment, that issue of challenging the accuracy of WHOIS data becomes somewhat irrelevant because there isn’t much WHOIS data that’s made publicly accessible.

I guess the two areas where you might still need to be concerned about that are first if subgroup C’s approach is taken and you have someone who should be revealing their full WHOIS data – full data in

WHOIS but who's falsely claiming to be a non-commercial natural person registrant. You need to have some mechanism for challenging that.

And I guess the other thing is if you have a someone listed as an OPAC and their contact data is incomplete or, you know, they don't list an email address or something or if you have a system of accrediting OPAC's and it's an accredited entity that's listed as the OPAC, that would be – you would need a sub-procedure for challenging that.

I think both of those are really – I don't think anybody would be challenging these just on the basis of inaccuracy alone. Their reason for challenging it would be that in order to facilitate their access to the shielded datas…

Philip Sheppard: Mm-hm.

Steve Metalitz: …as Milton has referred to it.

Philip Sheppard: Yup.

Steve Metalitz: So – but I think these are two – might be two cases in which you would need to have some type of challenge procedure, I suppose.

Philip Sheppard: Mm-hm.

Milton Mueller: I'm still a little bit puzzled by this. Now, let's assume for the moment that we are in fact only dealing with natural persons. Forget about non-commercial. I don't think there's any consensus on that. But natural person takes a huge load off of this whole problem, right? Because that means that 75% of registrations are going to be - supposed to have full unshielded WHOIS data, right?

They're going to be illegal persons and there's no reason for them not to reveal that. And I think I can get, you know, everybody that I know behind that as opposed to the non-commercial distinction which is a more ass in the swamp.

But again, assuming that the natural persons are the only ones that are shielded, then if you're challenging the status of someone as a natural person, that is indeed a challenge for the accuracy of the WHOIS record, isn’t it? There's some little box on there that says this is a natural person and you're challenging that. So, why couldn't the existing procedure be use?

If the – I don’t agree with you, Steve, that the shielded OPAC WHOIS contains not enough information that concern with accuracy. I think that the name and jurisdictions, state and country are going to be critical things and if the name, you know, turns out to be something that is clearly unrelated to the domain in some way, I think that’s the basis for challengers.

The OPAC is some made up address which, you know, if they make up their own address, they’ll do that with the OPAC too if there's some kind of fraudulent registrant.

So, I think there's plenty to go with and I don't think we want to be creating new procedures unless we really, really have to. I mean life is complicated enough.

Philip Sheppard: Mm-hm. Okay. I think they're useful. Let's just move on to one of the (unintelligible) as I mentioned which is "proxies". And sort of the first open question that is shall we revolve it about proxies. And the reasons that you might be would be that's supposing we do have a world following subgroup C suggestion.

Now if you're a legal person and you want to have shielded the display of your data, you would opt for a proxy service. But if we're now loading an OPAC in terms of a certain set of responsibilities in terms of how they would react, do we need to have a more formal specification of who a proxy could be.

At the moment I'm assigning a proxy can be the registrar or the seller or indeed sometimes somebody even further remote. And would it make sense for that proxy to be only an ICANN accredited registrar for instance. Comments on that?

(Tom): I would like to have comments for that.

Milton Mueller: Who's (that)?

(Tom): It's (Tom), Sorry.

Milton Mueller: (Tom), who else?

Andrew Denholm: Andrew Denholm.

Milton Mueller: Could you say your name again, sorry.

Andrew Denholm: Andrew, Andrew Denholm.

Milton Mueller: Andrew. Who else? Okay, (Tom), (unintelligible).

(Tom): Okay, thank you. One thing in regard to proxies, I want to mention that we have two different types of experience right now in terms of proxy services. One is proxy services are being off with the registrars in the big scale which certainly could be dealt with some one way or another.

Other thing I see is that for example, solicitors or as a business people taking on the role as a proxy for a customer who doesn't want to reveal who they are. And I guess, this is a type of business that we cannot regulate however hardly tried. I think it would even be…

Milton Mueller: Right, because that's outside of ICANN's capability essentially because if you're choosing to have your solicitors putting that name down for you, then, yeah (unintelligible).

(Tom): Right, so I kind of question on…

Milton Mueller: Okay.

(Tom): …you know, whether you could regulate any kind of business conducting these methods, you know, even if they're related to a registrant. So, you might be able to impose something registrant which I hope we won't do.

But just imagine that some new company has owned it and registrar have trust referring to them, you know. I don't think that we have as ICANN haven't measured with the policies to tackle that at all. So, I think the whole discussion about where we wanted or why not is pretty mute.

Milton Mueller: Okay. Andrew.

Andrew Denholm: If I ought to say, (side's time) if we need to point somebody who gotten appropriate IT material on there or something like that. Isn't that just adding extra hurdle? That's going to be difficult (to I become).

Milton Mueller: I'm sorry. I missed the first part of that comment.

Andrew Denholm: I'll tell you, I'm looking at this from the point of view of the bank. So, if we want to try to have info intellectual property removed or something like that. Isn't proxy going to make it just add an extra hurdle that's kind of make it much more difficult to get behind whoever is got a (unintelligible) might.

Philip Sheppard: Oh, is this? But I mean, the status quo as a proxy exist today. And there was nothing in the existing OPAC proposal to say that they should go away. So, my question is there's a whole existence of proxies drive a, you know, a truck through the things we're trying to set up in terms of the responsibilities, the OPAC is sort of behind that earlier question.

Andrew Denholm: Oh okay, apologies.

Man: No, no…

Philip Sheppard: Yeah. I think you're raising the same issue in a separate way. Where (Tom) was saying, it's going to happen anyway so…

Andrew Denholm: Mm-hm.

Philip Sheppard: …there's not much you can do about it.

Steve Metalitz: Milton, this is Steve, could I get in the queue please.

Milton Mueller: Steve, anyone else from the queue?

Adam Scoville: Adam Scoville.

Susan Kawaguchi: This is Susan.

Milton Mueller: Adam and sorry, who else beside Adam?

Susan Kawaguchi: Susan, Susan Kawaguchi.

Milton Mueller: Susan. Okay…

Margie Milam: And Margie Milam.

Milton Mueller: And Margie, anybody else?

Ken Stubbs: That’s Ken Stubbs, please go on.

Milton Mueller: And Ken. Okay. Oh just a moment Steve, off we go.

Steve Metalitz: Just to say that this was discussed to some extent in subgroup A. There were some took the view that they're with the OPAC system nearly it wasn’t anymore role for proxy services. I think we looked at the, again, at the must made document that were circulated which seem to indicate that the registrant could be a proxy service. That could be the registered name holder. And then you have to go through another step as Andrew was saying.

And there was another view I guess that if proxy services continued to exist, there needs to be some way to get at the identity of the actual registrant if you will. And I would point out that one thing that we looked out in the OPAC capabilities was that the OPAC would have to have the actual current contact data of the registrant.

And of course, sometimes proxy services may or may not have that. Certainly, registrars may or may not have that. And therefore, that – but that was an important point whether it was done by a proxy or done by the OPAC, there had to be some reliable way to pass on a request. And if necessary or under the appropriate circumstances, reveal accurate contact data.

Milton Mueller: Okay. Adam.

Adam Scoville: Yeah. I just wanted to make sort of a – in some way the technical kind of – in responding to the first comment or sort of query as to whether ICANN could venture in to regulate proxies particularly in the situation where say, the - it's a less formal proxy service such as I own a domain and I have my sister be my proxy.

You know, we currently do that in the registrar accreditation agreement of course, section 3.7.7.3, you know, says that if a registered holder intends to in the word of the REA license use the domains with third party, it's nonetheless, the registered name holder and have to put its own information in.

And it also says that the registered name holder licensing use of the registered name according to this provision shall accept liabilities for harm caused by wrongful use of the registered name unless it promptly discloses the identity of the licensee to a party providing the registered name holder reasonable evidence of actionable harm.

So, you know, in essence…

Philip Sheppard: So, I…

Adam Scoville: …even in that ad hoc sort of situation, the – someone who's holding a domain for me still has an obligation to give up my information when presented with a reasonable evidence of actual harm.

Philip Sheppard: Right. So, the first part of 3.7.7.3 you said was that – could you like…

Adam Scoville: Yeah (unintelligible).

Philip Sheppard: …say that again.

Adam Scoville: Any registered name holder that intends the license use of a domain name to a third party…

Philip Sheppard: Mm-hm.

Adam Scoville: …is nonetheless the registered name holder of record and is responsible for providing its own full contact information and for providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of any problems that arise in connection with the registered name.

Philip Sheppard: But what does that mean in terms of the way the WHOIS record should look today, then, if you're…

Adam Scoville: It well – if you – as I understand this, if you – if a proxy service put its own name in the WHOIS, it is considered the registered name holder. And there maybe a beneficial holder that by analogy, it's almost as if the proxy is the trustee and the real owner so to speak is the beneficiary of that trust like relationship.

In any event, the title owner to that domain is the proxy. It has to put its own information and it has certain obligations for its ability to facilitate timely resolution of problems.

Philip Sheppard: All right. Okay. So, either that the operator prompt you today, I mean, either the maybe questions about the application of that particular article or questions in terms of ownership. Is that…

Adam Scoville: Yeah. And that ownership may have consequences under national law. And…

Philip Sheppard: Yeah.

Adam Scoville: …this is a good mechanism in that it's sort of the first things to national law. If national law says, you know, the person who owns the domain name, you know, is going to be responsible for what the content is, then that we let national make that decision. And is this just sort of the first to that.

But it says, whoever is in the WHOIS is for these purposes be considered the owner or the registered name holder of the domain.

Philip Sheppard: Okay, thanks for that. Susan.

Susan Kawaguchi: Well, I'm probably just going to be echoing Steve and Adam's comments. But from our perspective, we need a standardized process for all proxy services as follows because if you're tying to get someone, you know, that registered name owner to, you know, the proxy service to reveal the information to be able to contact somebody a bad player, then each and every proxy service seems to do it a little differently…

Philip Sheppard: Mm-hm.

Susan Kawaguchi: …which takes a lot of time on our part. So if there was – if ICANN sort of establish a standardized process or revealing that information or at least contacting the actual owner, then – and they - these proxy services will bound to abide by that process, then that would make everybody a little bit happier, I think (unintelligible)…

Philip Sheppard: Okay. And if we're asking ICANN to do that, given that ICANN's relationship at certainly in this case with the registrars, would that imply that your preference would be that the – it's really proxy services and operation than it is the accredited registrars information has appearing a lot WHOIS record.

Susan Kawaguchi: Right.

Philip Sheppard: Yeah, okay. Margie.

Margie Milam: Yeah. One of the comments I wanted to make was regarding the whole register (client) situation. And I think that's kind of highlighted a lot of the problems related to proxies and being able to get information behind the proxy. So, I believe that there are number of registrars that do things to maybe a role or four some sort of rules or regulations related to proxies. At least the proxies that are the company is offering the service.

I believe, (unintelligible), I don't know if he's not on the line right now, has made comments for this fact that, you know, it probably makes sense to take a look at that, that registrar-client situation in particular something to highlight the need for looking at that.

Philip Sheppard: Mm-hm. Okay, thank you. Thank you for that. Ken.

Ken Stubbs.

Ken Stubbs: I apologize. Couple of issues, (Philip), first of all, I don't think it's possible for ICANN to regulate proxy services that are not – that are being offered outside of those under the registrar accreditation agreement. And I'm afraid what we may end up doing is creating a process that puts more of these types of companies in the business.

Number two is if you read 3.7.7.3 closely, you have the last sentence which basically you have to provide reasonable evidence of actionable harm. And from a legal standpoint -- I'm not a lawyer -- but first of all you've got words like reasonable and number two, actionable by who.

So, I think what you're creating as a process here that if any of this thing may cause a further delay because one might argue that either the evidence is not reasonable or the harm, the person who's claiming the actual harm is – doesn't necessarily have legitimate standing other than their own representation.

Philip Sheppard: Mm-hm.

Ken Stubbs: So, I'm just saying that from a practical standpoint, we need to try to provide a process here where the end result is one that's manageable within a reasonable timeframe once it's determined that the person who is requesting the information in fact has the right to it, that sort of things.

Philip Sheppard: So, Ken, so, I mean, would you – I mean, given – I mean, suppose we have a world in which legal person's data was not fully displayed. There was text in there. I mean, would you be comfortable of the idea that proxies - the role of proxies therefore was redundant and didn't need to continue? Is that what you're saying in terms of clarity and simplicity or not?

Ken Stubbs: No. What I'm saying is that if you're not careful, you're going to end up in the situation where people are going to start forming companies to provide the…

Philip Sheppard: Right.

Ken Stubbs: …pre-registration process so that a registrar will have let say, one client who was 200,000, 300,00, 400,000 names in which they're listed as the proxy for those names. And if I was the registrar, I'd look you in the eye and say, the information I have is accurate.

Philip Sheppard: Okay.

Ken Stubbs: And I won't have to go to this proxy. And you're just injecting another entity into the process and you're right back where you started.

Philip Sheppard: Right. So – hang on. So, the other side of the calling in of the tightening up the responsibilities of an OPAC would be a business opportunity for massive proxy services if people didn't like the OPAC who still wanted things to be hidden.

Ken Stubbs: Yeah, that's right. Now, I think what I'm saying is you had to offer people incentives that encourage them to provide legitimate information at the level closest for practicality. If you make the process too difficult, they'll just, you know, we're dealing with very creative people and that at space, we all know that. So, I'm just trying to avoid that.

Philip Sheppard: Okay. Thanks for that. We've just got less than five – ten minutes left. Let's just touch on the other outstanding tangential issue which is admin and tech contacts. This was being raised on one or other (just) coming which now. And it also just struck me looking at sort of what a future data set may look like if we're adding on OPAC data.

Largely, the role of admin and tech could – or one option would be for that to be sub-fumed by the OPAC for simplicity and indeed there always the possibility for having more than one OPAC. And, are there any concerns against that? I think it seems to be about the possibility of – for the whole new system not working and wanting to role back to the past.

But other views on the future necessity of admin and tech. It just struck me that the administering of database in which you might have up to five out to five that were contact for domain name and as a user having to put all that information in as a supply having to keep all that data struck me as a burden we can probably do without. But that may just mean me in my simple way. Comments on that issue?

Steve Metalitz: This is Steve Metalitz, can I get in the queue?

Philip Sheppard: Steve, who else?

Milton Mueller: Milton.

Philip Sheppard: Milton, who else?

Wout de Natris: Wout.

Philip Sheppard: Wout, who else?

Okay. I do this. Wout, let me take you first (unintelligible) yet.

Wout de Natris: Okay, thank you. I'll keep this very brief. And that I won't go into details. But this – it's information that we as LEA used and it also works for us to help find spammers. I think that would be as brief as possible.

Philip Sheppard: Okay. But that’s today. I mean, assuming that tomorrow we would have an OPAC contact there instead and maybe with certain responsibilities in terms of we're acting to your request. Would that not do the job?

Wout de Natris: We don’t know. That’s the problem. We know if we have. It's that simple.

Philip Sheppard: Anyway, it's practical. Yeah, okay. Steve.

Steve Metalitz: I would echo his by the last point A, this is today. Important information for contacting registrant, sometimes a registrant information which is not that detailed anyway…

Philip Sheppard: Mm-hm.

Steve Metalitz: …is insufficient to accomplish the task. So we would not want to want to see that eliminated at least without pretty secure guarantees about what the OPAC would do instead.

Philip Sheppard: Right, okay. So, it's conditional upon as Wout was saying, conditional upon what OPAC could end up looking like (unintelligible) going to do. All right, Milton.

Milton Mueller: Yeah, I thought that the whole point or one of the whole points that OPAC was to be a consolidation of the administrative and technical contact. And that the reason we proposed doing that was that people were completely confused about what the difference between the two was…

Philip Sheppard: Mm-hm.

Milton Mueller: …and did not systematically differentiate between the two factors. It's really almost no – I know in the case for example of my registration of the convergence centers domain. I just sort of didn't know what the put to the administrative contact or the technical contact. So, for the technical contact, I put our IT department. That's probably from – this guy probably knows nothing about what's going on in our domain most of the time.

And the admin tech I put myself but the universities addressed. I mean…

Philip Sheppard: Mm-hm.

Milton Mueller: It's not clear what you do in the OPAC because that's to be a consolidated simpler mechanism of doing that. So, I'm not sure why anybody would want to retain admin and tech. I think it would make things a lot clearer if OPAC was – what you put in there.

Philip Sheppard: Mm-hm. Okay. So, (unintelligible). (Well, I want to know) how this may is under items three and four of the agenda which are two sides of the same idea really, is just to propose a work item which is going to be work item from Maria as ICANN staff in terms of putting all the works going to subgroups together.

And my first opts were maybe a way to look at what are likely to be areas of agreement and also for understanding in terms of how things would work would be to sort of structure it as to, you know, how might A opposed to OPAC will look like. Assuming everything work as intended, so there's good face in terms of declaration, declared data by the registrant, the deficiency in terms of the way that system is operating, and how would that look first.

And then as a second stage to say, “Well okay,” Now, with the “what if” questions. “What if indeed is this bad face? What if there's inefficiency? What if there's mistakes?” And then how do we start to handle those as queries in the sort of way that subgroup A’s Ace task came in.

So, just your immediate thoughts if there's any downside to structuring things in that way. It may – my feeling is it might allow us just to see a thread through of system of how that would all look like. And then allow us to address some of those areas and identify the (do a gap) analysis, identifying those areas that still need to be answered.

People are generally comfortable with that as an approach for the next drop we see putting this free port together?

(Dan): Philip, this is (Dan). Can I…

Philip Sheppard: Mm-hm. I got (Dan), anybody else? Okay. (Dan), off we go.

(Dan): When I read this for the first time, the first thing that occurred to me was that without some very good incentives, we have to assume in the bad fate situation because there's enough bad actors out there that we're going to have deal with it. And, you know, if everyone acted in good faith, I think we wouldn't have a whole lot of problems in the world.

Philip Sheppard: Mm-hm.

(Dan): And so - and also, I think there's a certain circularity in the sense that if there are incentives for good faith then you're more likely to have it and therefore depending on what the actual structure is of what we would propose that would have an effect on the balance of what we have seen in terms of good faith and bad faith in reality.

Philip Sheppard: Yup. And I think it's probably true. How about other folks on that before we close?

Yup, Okay. What I propose to do is I will - based on our discussion today which has been very, very helpful, work with Maria and see what we can come up with in terms of first step at integrating these reports. And using what we already got areas – suggested areas of the (port) in agreement with it with the language and the to some of these issues and identifying clearly those areas whether is ideas that are not supported or indeed whether ideas that need to be further discussed in order for (a filling) to be made.

So, we will try to have that done. I guess in a week so we have something to look at for next week’s call. If that – would that – does that make sense in terms of timetable for you Maria?

Maria Farrell: It certainly does. At least they we can have a very a solid working draft.

Philip Sheppard: Yup, okay. I think before the – all we would need going on to that would those – already the best but we understand it, you know, the first attempt to that is going to be the most difficult probably. And then we'll be refining that as we go on.

Man: Philip, can I…

Philip Sheppard: Mm-hm.

Man: …is the call going to be at the same time next Wednesday?

Philip Sheppard: Probably. Just looking at sort of timescale across the globe. I hope this is about the best balance for most time zones. And that's a bit early West Coast, USA but then it's a bit late in the Fareast and Australasia. So, it's probably going to be about the same time.

Man: Well, I guess two points, one – I'm not sure there's a – who on the call is here from the Fareast and Australasia but it is very early for the West Coast people and I salute those of them who've got up very early for this.

And second, whatever the time is, let's try to get that, you know, sent out as a notice as soon as possible so we can plan our schedules. And I hope we'll have, you know, sometime to review Maria's work product…

Philip Sheppard: Mm-hm.

Man: …before the call.

Philip Sheppard: All right. Okay, well then I think…

Adam Scoville: Philip one question on that. This is Adam. Just- has…

Philip Sheppard: Okay.

Adam Scoville: …there been any attempts of sort of pull what our distribution in fact is? I'm not sure that I've heard anyone who I know all of hand is coming from Australasia. You know, if we don't have whole lot of folks who are interested in that then perhaps we could shift that. Even an hour would probably be helpful or an hour or an hour and a half would be helpful for the folks on the West Coast.

Philip Sheppard: Okay. I'll get staff to look at with this and (unintelligible) the work that's there. You never quite know how these things are working. With the fact the there people along from the Fareast and Australasia because they think it's all too bloody late anyway. And anyway, in bed…

Man: (Unintelligible).

Philip Sheppard: …or opposed – I supposed to lack of interest. And that they are upset by not being accommodated. And so we obviously need to look at that as well because clearly we are making decisions with a global impacts and the point is it will be taken.

So, all that note. I'll close the call today and thank you all very much for your contributions.

Man: Thank you.

Man: Bye-bye. Thank you.

END