ICANN SAN JUAN, PUERTO RICO
GNSO Working Group: WHOIS
Sunday, 24 June 2007
9:00 a.m.

>>PHILIP SHEPPARD: Well, good morning. Am I broadcasting? Yes, just.

Good morning, everybody, and welcome to a fun-filled Sunday here in Puerto Rico.

I'm very concerned about having ICANN meetings held in resort hotels where people seem to be going off enjoying themselves and having a real life while we go into darkened rooms, but nevertheless, that's our life, and we must make the most of it.

So welcome now to our first face-to-face meeting of the WHOIS working group.

Perhaps before I go any further, let's just do a series of introductions starting with Mr. Tony Holmes down on that corner.

>>TONY HOLMES: Thank you, Philip. Tony Holmes from the ISPCP.

>>MARILYN CADE: My name is Marilyn Cade. I am a member of the business constituency.

>> Michael Warnecke, Entertainment Software Association.

>>AVRI DORIA: Avri Doria, noncom appointee to the council, member of the working group.

>>JON BING: Jon Bing, noncom appointee to the council, member of the working group.

>>UTE DECKER: Ute Decker, IPC appointee to the council.

>>KRISTINA ROSETTE: Kristina Rosette, IPC council, member of the working group.

>>STEVEN METALITZ: Steve Metalitz from the IPC, member of the working group.

>>MAWAKI CHANGO: Mawaki Chango from the noncommercial user constituency working group.

>>GREG RUTH: Greg Ruth ISPCP rep to the council.

>> Stefan Lindquist, technical manager of dot SE.

>> Anette Hall from dot SE.

>>MARIA FARRELL: Maria Farrell, GNSO policy officer.

>>MILTON MUELLER: Milton Mueller, noncommercial users constituency.

>>CARY KARP: Cary Karp, registry constituency, council member, here as an observer.

>> Palmer Hamilton, business constituency.

>> Dan Krimm, noncommercial user's constituency.

>> Steve Delbianco, business constituency, and NetChoice.

>>BERTRAND DE LA CHAPELLE: Bertrand De La Chapelle, French representative in the GAC.

>>MARGIE MILAM: Margie Milam, registrars constituency and member of the working group.

>> Doug Isenberg, member of the IPC and the working group.

>> Kari Moeller with Turner Broadcasting System as a subsidiary of Time Warner. We are a member of the IP constituency as well.

>>BRUCE TONKIN: Bruce Tonkin from the registrars constituency.

>>PATRICK CAIN: Pat Cain from antiphishing working group. I am an observer.

>>JON NEVETT: Jon Nevett, registrars constituency.

>>NORBERT KLEIN: Norbert Klein from the noncommercial constituency and the GNSO council member.

>> Carlos de Imus from Microsoft.

>> Peter Stevenson from (inaudible).

>> Dan MaHarry from (inaudible).

>> Wolf-Ulrich Kuoben from (inaudible) telecom.

>> Scott Vowels from America Bank.

>>PHILIP SHEPPARD: Thank you very much. Today's agenda, as you can see, should be in front of you, you have some papers from today.

>>ADAM SCOVILLE: Phil, would you like introductions from those of us who are on the phone?

>>PHILIP SHEPPARD: Yes, indeed. And who is on the phone?

>>ADAM SCOVILLE: Adam Scoville.

>>PHILIP SHEPPARD: Adam, welcome. Is there anyone else on the phone?

>> At this time, there is not. Adam is the only one on the phone.

>>PHILIP SHEPPARD: Could you say that again, please.

>> At this time there is not. Adam is the only one on the phone.

>>PHILIP SHEPPARD: Thank you very much.

Today's agenda as you can see on the paper, on the screen, is pretty much four points which really struck me as being critical path tipping points in the discussion we've seen so far on the working group for which there had already been some assumptions that had flowed from them if you take one direction or the other.

So I thought it would be just quite useful to spend a little time on each of those to see where the group wanted to go in relation to each of those points: legal status, relationship between OPoC and proxies, the expectations in terms of OPoC being a communicator or an actor in terms of actions being taken, and the whole issue to do with determining the right to access by third parties, which has been discussed quite widely in one of the subgroups.

And then if we have time towards the end of the day we can certainly look at other aspects that have either arisen from those discussions or particular things we ought to take out of the current draft version of the report.

Later on today, we in theory have got a meeting with the whole of the council as a working lunch, and there's also going to be a briefing that I'm participating in to the GAC in which I shall just be giving them an outline of where we are and sort of where we will be going, including anything I can include from our discussions today.

So if all that is acceptable, we'll make a start with item 1. And legal status is something that you'll see in the current report, around about sort of lines 80 to 99 where there is mention in terms of what -- about the nature of the discussions we have had in terms of what status if any the OPoC should have. And there I think it's centered around discussions of should there be some sort of accreditation mechanism or should the relationship of the OPoC somehow be captured and perhaps relationship in the RAAs and subsequently in terms of the registrar/registrant agreement.

So perhaps it might be useful, that would have come out of discussion on your group, Steve, would it, primarily? When that was had?

>>STEVE METALITZ: Yes.

>>PHILIP SHEPPARD: Could you summarize that little bit of discussion you had there and that may lead us to debate around the table.

>>STEVE METALITZ: This came up -- sorry.

Got way too much paper here.

This came up in the -- The discussion about the capabilities of the OPoC and the relationship of the OPoC. The way we had broken it down in subgroup A, as I recall, is what capabilities did the OPoC have to have and then what relationships did it have to have, both with the way -- or, rather, potentially with three entities: the registrant, the registrar, and ICANN itself.

And we also talked about once the roles and responsibilities of the OPoC had been determined, what would be the method of enforcing that or of dealing with a failure of the OPoC to carry out those obligations.

And the feeling was there had to be some way for the registrar to step in and perform some of those responsibilities, such as relaying a request that had been made -- that had been sent to the OPoC but that for whatever reason hadn't been relayed to the registrant. And in those situations in which the OPoC's responsibility was to reveal the registrant's contact information, if the OPoC failed to do that, the registrar would be in a position to do that since the registrar, under the OPoC proposal, really collects the same contact information that it collects today.

So it has that information.

But how the registrar would step in to do that and what would be their obligation to do that and what would be the enforcement mechanism if the OPoC failed to carry out its responsibilities led to really two different models that we talked about, and there were some pros and cons on both sides.

One model was that perhaps the OPoC should be accredited by ICANN and, therefore, if the OPoC didn't perform or didn't perform on a regular basis or at some point -- first of all, an accreditation agreement would define the obligations of the OPoC and would make them a contractual obligation to ICANN.

Second, if the OPoC failed to perform, then not only could the contract provide for a different root for how those functions would be carried out, but also if the -- if the nonperformance rose to a certain level, the OPoC could be disaccredited and could no longer serve as an OPoC. So that was one model.

The other model would be simply to incorporate this into the Registrar Accreditation Agreement, for example saying if the registrar takes WHOIS information that includes contact data on an OPoC, it would have to be an OPoC that met certain capabilities, certain requirements, and that if the OPoC failed to do these things, the registrar would have to step in and the registrar would have a contractual obligation to ICANN not to accept an OPoC who couldn't do these things and so forth.

The advantage of that, of course, is this is an existing relationship contractually between ICANN and the registrar, so we wouldn't have to create this new relationship.

The disadvantage, I suppose, is that there's another step involved because the OPoC's nonperformance would only be -- would only be enforceable once the registrar learned about it and would have to step in.

So the OPoC accreditation model people seem to think -- and I welcome anyone in subgroup A to chime in or give me a different perspective on this. The OPoC accreditation might work if there really were a limited number of OPoCs. If there were some entities that went into the business of being OPoCs, perhaps they would be registrars or would be affiliated with registrars, perhaps not, and under that circumstance it might be feasible for ICANN to simply accredit these entities.

Obviously if there were to be many, many OPoCs, it might not be feasible to do that. In that case, the registrar route might be more feasible because there are 800 registrars and there's at least an accreditation system in place.

I hope that is helpful to provide the context of the two views.

>>PHILIP SHEPPARD: Yes, it is.

Discussion, then, on the merits of either of those options? I must say my instinct in terms of accreditation strikes me as problems with scalability, particularly if we are saying as we have elsewhere in the report that the OPoC could be the registry themselves or the registrar. The registrar is perhaps an easier issue.

But comments on either one of those models? I've got Bruce. Let me start a queue. Who else is going to jump in?

Dan. Who else?

Bruce.

>>BRUCE TONKIN: Just a comment. I guess the default today is the OPoC is actually the registrant. So I don't quite understand how you would be accrediting, or are you discrediting in the sense that if it's not the registrant?

>>STEVE METALITZ: If it's not the registrant. When we talked about the relationships, our proposal was that the registrant could choose to be his or her own OPoC.

>>BRUCE TONKIN: Okay, thanks.

>>PHILIP SHEPPARD: Dan.

>>DAN KRIMM: Yeah, it seems to me that the issue with accrediting the OPoC depends on what the OPoC's responsibilities are, and if the responsibilities don't go significantly beyond what, say, a current administrative contact might be, there might be no need for accreditation, particularly in the OPoC is not necessary in order to gain access to privilege to its data under legal circumstances.

>>PHILIP SHEPPARD: Okay.

Does anyone in this group think accreditation is a good route to go down?

That looks like an easy win.

>>MARILYN CADE: Philip, it's Marilyn Cade. I would like to ask a question about the concept.

One of the things I see increasingly happening at ICANN is the lack of relationship of any kind between ICANN and parties who are delivering services that are depended on by other parties in the value chain.

Did I understand the discussion about accreditation to be partly driven by a concern about accountability and making sure that there's an understanding of the functional role that that party's supposed to play?

So maybe if Steve could just say a couple more words about what the purpose of such accreditation would be.

Is it to establish a relationship between ICANN and a party who is delivering services that are -- is services that are being relied on by other parties?

Take out dash.

>>STEVE METALITZ: Yeah, this is Steve Metalitz again.

I'm sorry if I didn't make that career in my earlier presentation, but yeah. The idea was that there should be some type of relationship with ICANN so that the responsibilities of the OPoC -- and I agree with Dan, a lot of this term (inaudible) doesn't know what the responsibilities are -- there's some oversight that they're carried out or some mechanism for dealing with the situations where they are not carried out.

I think the accreditation system makes sense if the OPoC environment ends up looking kind of like the proxy system, the proxy service environment looks now, with many of the entities that insert themselves into the process being entities that either have a contractual relationship with ICANN or have a contractual relationship with a party that has a contractual relationship with ICANN; i.e., the registrar.

And then the idea of qualifying them with some minimum standards and having some enforcement mechanism makes sense.

If the OPoC looks more like the administrative contact does today perhaps, then maybe it's not as feasible to accredit those.

And then I think the alternative we talked about was this model where the registrar would, in effect -- I mean, we didn't use this verb, but in effect the registrar would accredit the OPoC. The registrar would have the standards for the OPoCs that could be listed in its WHOIS. Those standards would be spelled out to some degree in its agreement, in the registrar's agreement, with ICANN.

>>PHILIP SHEPPARD: Okay. Steve.

>>STEVE DELBIANCO: Steve Delbianco.

As we look about for contractual relationships on which to hook certain responsibilities or capabilities, I have a question, and that is if anyone can characterize the nature of the relationship between registrars and registrants. What are the terms of use or contractual responsibilities the registrant takes on when they avail themselves of a registrar's services. And in that respect the proxy would care that and the administrative and technical contacts as well.

Because if the OPoC is going to become not necessarily a legal agent, certainly a representative of the registrant, they would take on the same responsibilities that a registrant agrees to today.

So I would look for anyone to sort of characterize whether that is also a potential hook, Steve, in a contractual way.

What are the responsibilities of a registrant when they take on the services of a registrar?

>>PHILIP SHEPPARD: Anybody care to respond to that?

Bruce.

>>BRUCE TONKIN: It's probably something to be taken off-line, but in the registrar contract with ICANN, it actually sets minimum provisions that need to be in the agreement between the registrar and registrant. There's a whole section, I can point it out to you on the ICANN Web site if you like, they're public documents, that specify minimum conditions.

In addition to those minimum conditions, each registrar has it's own terms and conditions which are unique to the registrar. So in effect when you are taking a domain name registration service, you are actually entering into a different agreement with each registrar. Each registrar has it's own set of terms and conditions there.

That's the contracting party, if you like, being the registrar. The admin and technical contact, they are not bound contractually to the registrar in any way.

So I don't know if that answers the question but I can accepted you a link for the information you are seeking.

>>PHILIP SHEPPARD: Do you see any particular problems in amending the RAA to include in what we end up agreeing in terms of the OPoC responsibilities and that then flowing on in terms of the registrar/registrant agreement at the time of registration as the way that that is passed down to the OPoC?

>>BRUCE TONKIN: So I think the question is, is the OPoC contracted to the registrant or to the registrar?

>>PHILIP SHEPPARD: Yes.

>>BRUCE TONKIN: You can contract it so that it's the registrant's responsibility in appointing an OPoC that the registrant is still ultimately responsible for whatever those responsibilities are, and that's probably the better way to do it from the chain point of view rather than trying to link the OPoC into the registrar. Because anybody can appoint an agent. That's essentially what they are doing. If I have a trademark or something, I appoint a lawyer to be my agent. That sort of relationship is between me and that agent, essentially.

>>PHILIP SHEPPARD: Yeah.

>>STEVE METALITZ: And the point of bringing that up and asking that question, thank you, Bruce, is to explore this as an alternative to the accreditation. If the accreditation has warts all over it, that might be another place to turn.

>>PHILIP SHEPPARD: Okay. So happy with that concept and probably the preferred route, indeed, is regarding the OPoC in a similar relationship as you would another agent. And therefore the relationship is between the registrant and your agent -- in this case, the OPoC -- as a further way forward.

Margie, did you want to say something?

>>MARGIE MILAM: Yes, I wanted to say something. I still see a problem in the sense that what if someone puts in an OPoC who didn't agree to be an OPoC? What if they put my name in and I have no idea I have been appointed as an OPoC? Shouldn't there be some acceptance of that? Otherwise, you may be carrying on some liability you never expected.

>>PHILIP SHEPPARD: You uniquely put us into bullet point 2 on the agenda which we can happily address. But let me just see if we got closure on the first point.

Probably the preferred route, subject to us getting bullet point 2 right, is as I just outlined, yeah? So we're looking at sort of the same legal relationship you have with other agents.

>>Can I get in the queue on that?

>>PHILIP SHEPPARD: We have Steve. Who else wanted to be in the queue.

>> Adam.

>>PHILIP SHEPPARD: Steve, off you go. I'm sorry. Adam, off you go.

>>ADAM SCOVILLE: The issue that I struggle with here, whether it's accreditation or some sort of agreement with the registrar, we need some sort of chain back into someone who can in a meaningful way impose contractual conditions on the OPoC.

And let me just set out why I don't think that that is the registrant.

And this is that let's take the sort of worst-case scenario where you have a registrant who is a bad actor and they are doing something, I'm not sure we necessarily need to say what it is at this stage.

We have -- Presumably we have had some sort of condition in the registration agreement, and I suppose that that condition has been dictated by ICANN in the RAA that says, as Bruce said, those sort of minimum set of things that you have to put in your registration agreement, and then it was in the registration agreement and so the registrant agreed to it in that sense and said I will only appoint an OPoC who has these capabilities or these qualities.

And say we have a registrant who is a bad actor. And ultimately, the purpose of all this is so we can have some sort of enforceability, some way of getting to the registrant. If the registrant doesn't include those terms in its agreement with the OPoC or, as -- I can't remember if it was Margie just said, what if there is, in fact, no agreement between the registrant and the OPoC, then the only way you would have of enforcing what the OPoC is supposed to do, the only guarantee that you have that the OPoC -- that any of this is meaningful, really, is that if the terms weren't included in that agreement between the registrant and the OPoC, then you'd have basis for the registrar to say, "Registrant, you violated those terms."

But the problem is that the registrant is the person that you can't find and you are trying to go after in the first place.

So you have a situation where we need the registrant in order to go after the OPoC, in order to go after the registrant.

So that's the point where I see it all come tumbling down. At that point, there's no realistic guarantee that whatever requirements you have dictated on the registrant with respect to who it appoints as an OPoC, there's no guarantee that that's actually going to happen.

And it's probably not.

And that's the basis on which I say that we have to have some sort of link somewhere higher than in the chain than the registrant.

>>PHILIP SHEPPARD: Okay. All that understood. I think what you are saying is what happens if there's a failure of whatever responsibilities we imbue upon the OPoC, which I think falls into a another category discussion that we have already had, which is then certain actions are taken, at which point the relationship becomes no longer between whoever is wishing to make a complaint or get action happening, but then there's communication directly with the registrar.

I think it's slightly definitions. There's only so much you can build in in terms of safeguards, but perhaps we can flesh out those issues later.

Anyway, I have a queue at the moment, and Steve Metalitz is next.

>>STEVE METALITZ: Just to pick up on what Adam said, I think if the only relationship that's required is a relationship between the registrant and the OPoC, then we're talking about WHOIS here. There is a third party involved -- or fourth party which is the requester. How could the requester -- the requester is not a third-party beneficiary of that agreement. There has to be

some mechanism for the requester to get the information if there is -- even if there is an agency agreement that has the appropriate provisions between the registrant and the OPoC.

>>PHILIP SHEPPARD: Okay. Next is Milton.

>>MILTON MUELLER: I'm going to pass right now. I want this to be -- I think the registrars need to talk more about this, but I may want to get in later.

>>PHILIP SHEPPARD: Okay, Bruce.

>>BRUCE TONKIN: I was just going to comment that the issues people are talking about, yeah, the contractual structure today, is the registrant agrees to a set of contractual conditions and let's say you did have a contractual condition around OPoC, and then if the registrant violates those contractual conditions, that's grounds for deletion of the name as per the other reasons.

So your next point of contact as it is today is the registrar, which is a recorded record and then you lodge your formal complaint with the registrar and today, for example, that's how a lot of the issues are resolved. There is a WHOIS complaints process. The name can be deleted if the registrar is not meeting its obligations. That is contractually how it works today. That's the chain.

It goes up to the registrar, and the registrar in its agreement has a set of minimum conditions and allows it to take action if certain conditions are violated including not providing accurate contact information.

But you can also say if the OPoC is not performing its responsibilities, you wanted to add that, it would be similar, I guess, to the way we deal with a registrant providing false contact information.

>>PHILIP SHEPPARD: Yeah, or make an addition to an existing mechanism.

>>BRUCE TONKIN: That's right. The mechanism is there. And the comment Margie made, which is correct, that someone can put in someone else's name and details for OPoC, they do that for the registrant as well. In fact, that's quite common. It is third parties that are acting in bad faith often use a stolen credit card, and they use the identity information associated with that stolen credit card that they give to us as the WHOIS information.

Their name and address and phone numbers are stolen. The only thing that's usually real, in fact, is the e-mail address because it would be a Hotmail or something similar. The e-mail does actually reach the third party but it is obviously hard to work out who the third party is based on that free e-mail address.

>>PHILIP SHEPPARD: Let's address Margie's point that she raises in terms of the need, in the first place, for the OPoC to acknowledge nomination. That's something that strikes me that is probably necessary in terms of fulfilling the fact there is some sort of relationship there and pretty easy to automate in terms at the time of registration.

The registrant presumably is nominating the OPoC. There is an e-mail address provided, and that just kicks off an e-mail to go out there and then it has to come back at some point within a time frame for that to happen. That's pretty straightforward, isn't it?

>>MARGIE MILAM: yeah, that part I think would be -- if you are using the e-mail addresses as the acknowledgement, I think that's right. It would be pretty simple.

>>PHILIP SHEPPARD: Everybody comfortable with that?

>>STEVE METALITZ: In other words, registration would not take effect until the OPoC had agreed to carry out the responsibilities?

>>PHILIP SHEPPARD: I guess that would be the case. Otherwise, it would be a meaningless exercise, wouldn't it?

Was that Adam on the phone?

>>ADAM SCOVILLE: If you have the OPoC acknowledge or some sort of system where you have to get -- where the registrar has to get feedback from the OPoC, then, you know, it strikes me that at that point, why not have them -- have the OPoC

agree to a set of terms and conditions with the registrar. It's perfectly easy. You know, if it is a situation where you send an e-mail, the OPoC has got to click on a link and go to a Web page and that Web page, instead of saying yes, I'm here, says, you know, I agree to these terms and conditions.

>>PHILIP SHEPPARD: Any quick reaction to that? Bruce?

>>BRUCE TONKIN: I think we got to sort of separate who is the OPoC providing the service to. Is it the registrar or the registrant?

Now, there is probably getting confusion here between services that registrars offer themselves, which are -- I will call them generically private registration services where that third party may well be a service provider to the registrar and the registrar is providing a service to the registrant in some kind of privacy service. That's one model.

Then the other model is where the registrant chooses to appoint an agent and that's really nothing to do with the registrar. So I think they are two very different things. The idea that if you're sort of saying the registrant can't appoint somebody to be their contact, I have to get that contact to be accredited with the registrar. I think we are creating a whole accreditation structure that seems unwarranted.

Certainly, if the registrar is offering a private registration service, then the registrar would need to take on some obligations which would again be in its service agreement with the registrant for providing that private service.

And then, in turn, that registrar would have an agreement with this OPoC provider, whatever you want to call it, that's contractual as well. But that's one model. The other model is just simply a registrar chooses to appoint their best friend down the road to be their contact because he is the technical guy and he set the domain name up for them. I think it is registrar's responsibility to manage it. They are very different relationships there, I think.

>>PHILIP SHEPPARD: On some point, you would any way be describing what those relationships are. Presumably, that would be something on the Web site or whatever that the OPoC can go and find. You don't necessarily need to go through a whole process of acknowledgement to do that out of thought, as long as the OPoC says, I agree to be that and they need to be aware that as an agent there are certain responsibilities and it is up to them to confirm -- to check that they're happy about taking that on. That's the mechanism you are envisioning, I take it.

>>BRUCE TONKIN: I'm just saying the two models -- the bulk of the private registration services today are managed by the registrar for the registrant. That's pretty structured. But I'm saying OPoC itself, it is basically binding you to use only the service provider by the registrar. As a registrant, you don't have to, you can use any service you like, including your trademark lawyer, which is another common model.

Those trademark lawyers have no agreement with the registrar. Their agreement is with the registrant. So I just want to sort of separate those. I think there is confusion between those two models.

People seem to be mapping OPoC on private registrar services. I don't think that's a sound method. I think that is a example of how they're used but not the only way.

>>PHILIP SHEPPARD: Back to the queue.

>>BERTRAND DE LA CHAPELLE: Bertrand de La Chapelle. Just a quick comment on the notion of having a mail that is sent --

>>PHILIP SHEPPARD: Bertrand, can you talk directly into the microphone to help with the transcription?

>>BERTRAND DE LA CHAPELLE: The question of the acknowledgement by the OPoC, in many discussions we are addressing the discussion of bad faith. The problem with these issues, however long the chain of accountability you make, you can always cheat it in the end. If you take this case, if somebody wants to

designate me nominally as a OPoC and forge a Web address that is supposed to carry my name on a Yahoo mail or whatever, you can do it and then the mail will come to them. They will say, yes, I'm Bertrand de La Chapelle, and there is no problem.

I'm afraid in the whole discussion, we're taking a lot of time to try to corner all the possibilities of cheating the system, maybe we should devote a little bit more time on making a system that works to handle the main questions which is on the one hand the protection of the individual's privacy. On the secondhand, the use of proxy services which basically the OPoC is and the question is below, is it a way to basically replace or organize the proxy services.

And the third level is how do you handle the remedy function that was identified during the thing.

I think we can discuss endlessly how people will cheat, how we want to control. You can not make it 100% full-proof system. Credit card information will be much more valuable in the end if you really have the wrongdoing and you want to track down somebody.

>>PHILIP SHEPPARD: Sure. Jeff?

>>JEFF NEUMAN: I'm Jeff Neuman with Neustar, the registry constituency. I want to comment on the point because the way Philip raised it, is everybody okay with OPoC having to do a confirmation. I believe the words Steve used were "before the registration becomes effective." I just want to introduce, there is another word here, is the registry. We need to be careful with the terms we use.

If you mean that a registrar would register the name and the name is put on a registrar hold status, that's one thing. If you are talking about that the registry can't make it effective until the OPoC confirms, now you are talking about the registry relying on a party that's four parties removed from the registry. Let's be careful with the terminology.

Since we are talking about implementation, if we could do some sort of registrar status rather than something that the registry has to do, that would be something we need to consider.

>>PHILIP SHEPPARD: What would be your preference?

>>JEFF NEUMAN: Obviously, my preference would be for the registrar because, again, the OPoC is four parties removed from the registry, so, yeah, some sort of status that the registrar would put the registration in until the OPoC confirms.

>>PHILIP SHEPPARD: A hold status for a period of time?

>>JEFF NEUMAN: Until it is confirmed and then they would put it on active.

>>PHILIP SHEPPARD: Seems workable. Behind me?

>>SCOTT VOWELS: One of the themes that I'm hearing, I actually began to agree with you at the beginning of your comments, is that it seems as though the processes that we're putting in place, it's required that they assume bad acting. You know, I have domains registered as an individual and so privacy issues around that are important to me, but I really haven't experienced anything bad as a result of that. I don't like the fact that my information is available on the Internet that way, but I'm not really being impacted by that, that I can tell.

What I am experiencing on a daily basis is rampant misuse of the system. We are being gamed, and as a result of that, access to the information is extremely important. So one of the things that we've been talking about are the multiple layers of accountability and whatever you do, it's important again that the access and the processes you put in place are much more tactical. It sounds as if the way we're developing the system is I will send an e-mail and have to wait for the dispute process to meet itself out.

Whatever we do, I think you need to assume that people are going to game the system. The majority of my focus is on bad actors. I just wanted to make sure that that was raised because it sounded like they were starting to take a turn.

>>PHILIP SHEPPARD: Okay, that's good. Thanks.

Bertrand?

>>BERTRAND DE LA CHAPELLE: Just to come on to that, I fully agree and it allows me to raise a distinction that I think is useful. When I was talking about bad faith and good faith, I was mostly addressing what we're discussing here is the bad faith of the registrant. Somehow they are trying to cheat the system in order to have as many shields as possible.

What you're addressing as well is the bad faith or the bad use of the system and the conditions that can be put on the access to the data which is different -- it is the second dimension. And what I wanted to raise is that on both cases, I think the distinction is important, there is a regime for entering the system and the second element is how you access the data and, of course, what we're discussing here is the articulation between both, what you put in and how it can be retrieved and under what conditions.

And in both cases, there is a step that says this is how it should work for it to be, simple, fluid, efficient, facilitating stability when everybody is basically in good faith and, second, identifying the possible abuses on both cases to see how you can reduce the misuse, which is exactly as, a matter of fact, the balance that we've tried to raise in the GAC principles that facilitate good users and preventing bad users.

I like your distinction.

>> SCOTT VOWELS: Possible as well making the registrars more accountable. That's another thing -- that's another theme I have been hearing about, the issues around accountability. I can't tell you the number of times that we'll see obviously fraudulent information entered into a domain name. It's generally the same four or five registrars that are allowing that to happen. If I'm an expert at it by now, these folks must know this is going on.

And so whatever accountability you're building in, I don't know -- one of the things I was thinking about, is anybody policing that or even looking at it? It just does not seem that's going on.

>>PHILIP SHEPPARD: Feel free to name names.

[Laughter]

It is being transcribed.

>> SCOTT VOWELS: Over dinner later, perhaps. It is obvious this is going on.

>>MILTON MUELLER: Let's keep this in perspective. Number one, we are talking about OPoC applying to the 20% or so of registrants who declare themselves to be natural persons as opposed to legal persons. Number two, if you are a bad actor, consider the following option. You register as a legal person and you're not shielded through OPoC but you put in false administrative contact information or you declare yourself a natural person and that information is shielded but you have to invent a OPoC and somehow make that false. Now.

What's the advantage of one or the other? I mean, both cases, there is an option for somebody to game the system. At least for the 90% or 95%, depending on your level of optimism of human nature, the 99% of the registrants -- individual registrants who are not bad actors the OPoC system would work, it would do what we want it do.

So let's not -- there is a certain characteristic of lawyers to focus in on isolation of a particular problem and forget about all the ancillary and contextual factors. So let's not try to overburden this OPoC relationship with too much. Let's not be casual about the need -- the existence of bad actors and the need to deal with them.

I just don't see how tying all this stuff to the OPoC relationship really gets us that much traction. If you make it that difficult, the bad actors would put it false WHOIS information or find some other avenue for getting around it.

>>PHILIP SHEPPARD: Milton, when you started off, you mentioned a 20% figure?

>>MILTON MUELLER: I made that up.

[Laughter]

But what is it really? This is sort of a -- like in -- this is a common figure to get kicked around in the industry. I don't know where it comes from. But, I think, VeriSign did some studies several years ago about how many were actually private individuals, something like that.

>>MARILYN CADE: Philip, can I ask a question of our previous speaker from the banking industry? My name is Marilyn Cade. My experience in the exploitation is that very few of the phishing, pharming, DDOS attacks that the Tier 1 that I advise, AT&T, encounters are perpetrated by corporations. Almost in all cases, the investigations turn back to an individual. One of the challenges, I think, we face and many people here know that I've suggested that one of the things we need to do is to try to actually better understand what the characteristics of registrants are.

To Milton's point, we're hampered by a lack of understanding of whether the majority of registrants are, in fact, corporations, they're organizations, they're individuals, or even the purpose for which they're using the Web site, whether they are holding themselves out to communicate with the public, whether they're engaging -- I'm not talking about the content on the Web site but really the purpose of the Web site.

So it seems to me that what we are hampered with is, you know, what the percentages are of registrants that we are really trying to devise a different system for.

>> SCOTT VOWELS: Just as an example, on the first phish I worked on -- I am not a lawyer, by the way -- the name of the registrant was first initial A., middle name Sid, last name Trip. I was on the phone with the lawyers at the time and they were like, Wow, we got to get this Sid guy. You got to be kidding me, right?

One of the issues is it is many layers deep. It is not clear what it is that you are up against. It won't be -- it will be a company that's registered and there will be three different names on the registration information and we are running all over the place trying to track it down. Even the fraudulent information is valuable.

So I don't know. I'm not sure what we're dealing with. The information again -- access to whatever information is there and quickly being able to access it is important. So...

>>PHILIP SHEPPARD: Steve.

>>STEVE DELBIANCO: The discussion thus far risks trying -- it risks the belief that bad actors follow one track and good actors follow another. And I refer you to the anti-phishing working group, pat's publication. It has brought a little color to the ICANN world because he printed the header in green. It is only three case studies. We wouldn't want to make policy on case studies but the facts are persuasive. The anti-phishing working group case studies reveal in these instances when they went to address a phishing problem, the bad actor doing the phishing wasn't seeking where they were to get information. The first step was to take down the site that was hosting the phishing page. And what do you know, it wasn't a bad actor site that was hosting the phishing page. It was a good actor. It was an internal page in the subdomain of the bank, a good actor. Plenty of resources go after the bad actor, and we need to solve that issue, I understand that.

A good actor's Web site was messed up by a page that was implanted. And so the need for access now is to access the good actors' technical contacts in a way to take the page down. And if that good actor had availed themselves of certain proxy or OPoC registrations, we have delayed -- without attaching responsibility to the OPoC, we will delay by hours or even days, the period of time it takes to take down the offending page inside the site. So we should not try to separate the world into good actors and bad actors and track their behavior through the access to the system. In fact, they crossover each other and it may be the good actor seeking to protect their privacy who has erected a barrier to law enforcement and their own interest to take a page down.

>>PHILIP SHEPPARD: Okay. Others? Jeff.

>>JEFF NEUMAN: Can I just address that point? This is one of my issues with the anti-phishing working group, is that it is only focusing on WHOIS. As a registry, when we determine that there is phishing going on, we don't care what information is in the WHOIS. We take it down. I don't want to make it sound like -- you make it sound like failure to know or get access to the WHOIS is going to delay any action that's taken against the phisher or whoever is producing bots or malware, that's just not the case. When we determine there is phishing going on. There are certainly policies and procedures we have with the registrars and there are names taken down.

I understand --

>>STEVE DELBIANCO: I appreciate your perspective and when we can ensure that all registries will fact as efficiently and effectively as you, then we wouldn't need it.

>>JEFF NEUMAN: But that's not a WHOIS issue, right.

>>PHILIP SHEPPARD: Naming names.

Okay, I think we're broadly covered what we had under that agenda item. Other things we need to address that came up in any of the subgroups in terms of legal status? Anything we're missing so far? If I can summarize, I think, what we're saying is not accreditation but the similar relationship you have as an agent, there is a need for acknowledgement as a OPoC, that will be manifested. That could be automated and manifested in terms of the whole status by the registrar until the acknowledgement happens and handle at the registrar level. That's where we are I think so far. Steve?

>>STEVE METALITZ: I am not sure where in your summary you left the other alternative that we talked about in subgroup A besides ICANN accreditation which was a registrar -- provision in the RAA that says the registrar must obtain this acknowledgement or OPoC must meet certain standards.

>>PHILIP SHEPPARD: Yes, I include that. Good. If we're happy with that, Steve?

>>STEVE DELBIANCO: I wanted to add one thing. In subgroup A, at least I had advocated that the OPoC have the technical capability and the permission level to be able to remedy offending legal content or legal activity on a domain. I don't think it is necessary to build that into the accreditation or even to build that into some self-serving --

>>PHILIP SHEPPARD: That's coming later on the agenda. We can probably address that under item 3. It is a very valid point to talk about.

All right. Let's move on to OPoC and proxies. Discussion also came up in the subgroups on this. And I think there were basically two points of view which had -- both of which had support, both of which were somewhat contradictory, one of which there should be no more proxies and the other one which is we should have some sort of amended service that -- which, I think, could be summarized if the proxy services were to continue, then the proxy becomes the OPoC and, therefore, everything we're saying in terms of the rights of the OPoC simply becomes a proxy and that may just simply be a paid-for service done by registrars in whatever way they wish to do it.

Comments on either of those two options, either those who believe there should be no more proxies or an amendment to the proxy service in that way is something that is going to be workable.

Steve?

>>STEVE METALITZ: Steve Metalitz. Just to provide a little bit of context of the discussion in subgroup A, this is really stimulated by early in the work of the WHOIS working group, Paul Stahura provided a must-may document that worked

through the OPoC proposal and spelled out in a very useful fashion what must happen, may happen and so forth. He made the point that at least some proxy services, those that in effect establish a license relationship between the proxy services, the licensor and the true registrant as the licensee, the actual contact data of the registrant in that case is the proxy service. If the proxy service then nominated a OPoC, you would be adding another step but you would end up at exactly the same place which was you still didn't know who the true registrant was, you just knew who the proxy service was. As it stands right now, there is a provision in the registrar accreditation agreement that says the proxy service in that circumstance has to rev!
eal the contact data of the registrant when presented with reasonable evidence of actionable harm, a phrase that not everyone agrees on its application in a particular circumstance.

So the idea was that if a proxy service that's set newspaper that way is the registrant, then in effect you have a OPoC system already. Why put another layer on top of it, of another OPoC and another step you would have to go through before you achieve the goal of finding the true registrant.

>>PHILIP SHEPPARD: Any comment from registrars who wish to defend their revenue model of proxy services? Bruce?

[Laughter]

>>BRUCE TONKIN: I just want to point out in case it is not wildly known, there are two variants of proxy services in the market.

>>JON NEVETT: One is not a proxy service.

>>STEVE METALITZ: That's why I am saying in that circumstance.

>>PHILIP SHEPPARD: Can we have clarification on one type of proxy service that's not a proxy service. This is an interesting concept.

>>JON NEVETT: There are two types of privacy services that typically registrars provide. This is Jon Nevett from the registrar constituency. One is what you all are referring to as an proxy service that is the Go Daddy model. They have a domain by proxy where they become the registrant and enter into a license agreement with the beneficiary registrant, if you will.

The other service is more of a privacy service and that's the Network Solutions and Melbourne I.T. model. In that situation, essentially the registrant information is still in WHOIS and all it is is a privacy service where we where we provide a forwarding address -- mailing address and e-mail address where interested parties could contact the registrant that way. But it is not publicly available through the WHOIS process.

>>PHILIP SHEPPARD: So under model one, the Go Daddy model, if the registrar is basically taking full responsibility, in an agreement outside as a registrant, the registrar is a legal person. In our work here, that means full WHOIS data, as far as we're concerned for that registration, so we need not discuss it any more. Is that correct? I would like it to be.

>>BRUCE TONKIN: That proxy is taking full legal responsibility.

>>PHILIP SHEPPARD: But also in our work so far, we're saying as a legal entity, there will be full WHOIS data.

>>JON NEVETT: It will be WHOIS data for the registrant in the Go Daddy model would be Go Daddy.

>>BRUCE TONKIN: In the proxy where the name is the registrant, they are legally liable for that name. They are the registrant.

Now, they might say, hey, it wasn't me, it was him. But unless they can prove it's him or her, it's them. They are the registrant.

>>PHILIP SHEPPARD: If they are bad faith or whatever, the person alleging that or seeking action is going to be talking with a registrar and take action in whatever way.

>>BRUCE TONKIN: What I am saying is the domain names by proxy is legally responsible for whatever it happening to that name. The way those services typically operate is when someone attacks them at a legal level, they will step

out of the way and say actually it is not me, it is him. And they reveal the information. Which they are doing it so they're no longer taking responsibility for that name. I think, again, it is -- we are confusing a particular business model with WHOIS which is a separate issue.

That proxy, that's not a OPoC at all. They are the registrant. The registrant is domains by proxy. If domains by proxy registrant infringes a trademark, it is the domain proxy that is completely reliable.

>>PHILIP SHEPPARD: The phrase that we should capture in the report just to put that in parentheses is "domains by proxy," that type of service or is that one manifestation of it?

>>JON NEVETT: That's one example.

>>PHILIP SHEPPARD: Can you give us a generic phrase so we can capture that type of proxy service?

>>BRUCE TONKIN: Proxy service.

>>PHILIP SHEPPARD: I thought we said that wasn't the proxy service.

>>JON NEVETT: That is a proxy service.

>>PHILIP SHEPPARD: Other one is not a proxy service.

>>BRUCE TONKIN: OPoC is not the same thing. OPoC is not the registrant. Basically, the way I understand it, it is the admin contact. It just needs to be another name for the admin contact and you are giving it responsibilities and trying to define it because at the moment they are not really defined. I have sent the text from the current agreement. It just says you have to supply an admin contact and a technical contact sufficient to resolve problems in a timely manner. I can't remember the exact words. But that's what's in the agreement today. I guess what I understand the WHOIS group is doing is trying to flesh that out some more as to what its responsibilities are.

>>PHILIP SHEPPARD: Milton, you wand to say something.

>>MILTON MUELLER: So, Steve, based on that description of the proxy model, the proxy service model, the way I interpret that is in those cases, the registrars are voluntarily assuming, for the sake of making money, many of the responsibilities that you would like the OPoC to have.

And therefore, that we should not say that the OPoC should exclude this kind of proxy service as a -- as a business.

You would, in fact, actually you would prefer that to the OPoC model.

The OPoC is the bargain basement, free privacy service that people are supposed to have as a matter of right.

The proxy service is an extension of that, sort of dealing with the problem of responsibility. They could sell this to customers saying, you know, if you have a bad OPoC, you might get your domain lost because they didn't respond properly. So you want that option to still exist.

However, I agree with you that there's something strange about a proxy service appointing an OPoC. That doesn't smell very good. And could the OPoC be defined in a way that excludes that?

>>PHILIP SHEPPARD: Steve.

>>STEVE METALITZ: Well -- This is Steve Metalitz.

Remember, subgroup A was proceeding without any assumption about what subgroup C was doing.

So when we wrote up what we said about the OPoC roles and responsibilities, we weren't taking into account the point that Philip made which was that a legal person would not have an OPoC anyway. A legal person would simply put contact data in the WHOIS as today, as I understand it, anyway.

So that may help to resolve the problem of the proxy service in that model. The true proxy services as Jon and Bruce are using it.

It wouldn't have an OPoC, so maybe there isn't that issue there.

>>PHILIP SHEPPARD: Yeah, that's a brilliant assumption we need to come back to, but probably for reasons of simplicity rather than for reasons of solving this particular issue.

So where are we on that? Are we saying that we're happy with one model of proxy services whereby -- which is as we said already, in fact, that one option for being the OPoC would be the registrar. We're happy with that concept, and that could be a type of proxy service, if the registrar wanted to leverage it in that way, and we as a group are neutral to how that would happen as long as whatever we imbue in terms of the rights and responsibilities of the OPoC aren't unchanged by that mechanism. Would that be correct? Everybody happy with that?

>>ADAM SCOVILLE: Adam in the queue.

>>PHILIP SHEPPARD: Adam in the queue and I see Steve hovering. Adam first.

>>ADAM SCOVILLE: Just to ask the question. How would this all apply to the other kind of proxy service that Bruce is referring to, which if I understand it correctly, looks a lot like what the OPoC would be now.

This is where the so-called proxy service leaves the registrant's name in the WHOIS but substitutes all the contact information for, for instance, their own post office box and an anonymized e-mail address, et cetera. How would the dual-layer system work for those kinds of proxies.

>>PHILIP SHEPPARD: So are you saying in the case where the registrant's name appears as the registrar, they are basically taking that --

>>ADAM SCOVILLE: No, appears as the registrant. Continues to appear as the registrant. And Bruce certainly can correct me if I am describing this wrong, because I think that his registrar is I think one of the ones who uses this model. But all the contact information is replaced by the registrars or the proxy services address, be it a post office box or whatever. And there's usually some sort of anonymized e-mail address that says, for instance, bigbox.com@joe'sprivacyservice.com.

>> What's the question?

>>PHILIP SHEPPARD: I think we're struggling. Could you put the question in crystal clear terms? It's Sunday morning here and we are terribly slow.

>>ADAM SCOVILLE: Too much time on the beach there, I suppose. We talked about the fact that if the registrant is a legal entity in the first model of proxy services that Bruce mentioned, how the OPoC wouldn't apply to it under subgroup C's proposal and so forth.

My question is how it would work in this other kind of system.

And I think Milton might have attempted to answer that. I think, if I understand correctly, by saying that in this kind of circumstance, he would be a little uncomfortable with a proxy service appointing an OPoC.

But I just wanted to explore a little bit more in this model of proxy service whether we think an OPoC would be an acceptable thing or not.

>>PHILIP SHEPPARD: Comments to that? We're still struggling with the question, I think.

Let me put something which may be capturing that.

In the model where, if you like, there's fully veiled information and the registrar is putting themselves down as a registrant as part of a service, presumably under the circumstances the registrar's names appears under all fields in WHOIS. Is that correct? I am looking at registrars when I am saying this.

>>JON NEVETT: Put your question in crystal clear terms, please?

>>PHILIP SHEPPARD: I know. We will have a coffee break in a moment, I think.

>> The answer is yes.

>>PHILIP SHEPPARD: In the case of a fully veiled service, the Go Daddy type service, where you have the registrar's name appearing in WHOIS in place of the registrant, does the registrar's name also appear in every other WHOIS field typically?

>>BRUCE TONKIN: It's not the registrar's name. The registrar is Go Daddy.

>>PHILIP SHEPPARD: So it's a second party, yes.

>>BRUCE TONKIN: Yeah. And -- that's right.

>>PHILIP SHEPPARD: And does it appear in all spots of WHOIS, typically?

>>BRUCE TONKIN: Yes. Yeah, I believe so, isn't it?

>>JON NEVETT: Yes.

>>BRUCE TONKIN: So the WHOIS, if you are thinking about the registered name holder has the postal address, an e-mail address typically -- no, just postal address, then you have an admin contact, and then you have a technical contact, and in some cases people display billing contacts as well.

Normally with the -- what registrars generally have is a privacy service. They will generally replace the registrant and the admin contact, and quite often the technical contact is left as the ISP or whoever is often providing other services.

So they don't always replace the technical contact but they certainly always replace the registrant and the admin contact.

>>PHILIP SHEPPARD: And are we happy that in a new OPoC world that that second party who is down as a registrant would also be down as the OPoC, albeit that's one removed, so long as they still have the rights and responsibilities of the OPoC in terms of getting information? I'd have thought yes.

Anybody feel --

>>ADAM SCOVILLE: I thought you said the OPoC doesn't apply to that model.

>>PHILIP SHEPPARD: Well, yeah, yeah. That's a separate question we perhaps need to address in a second.

Steve was in the queue. Let's go to him.

>>STEVE METALITZ: If I understand the private registration service, the Melbourne IT, Network Solutions type service, an individual registrant who wanted to get two layers of shielding could do so because they would sign up with the private registration service and they would designate as their OPoC somebody else.

And so what would appear in the WHOIS is name of registrant, country, and the OPoC data.

So if you -- if the requester went to the OPoC under circumstances where there was a reveal requirement, the OPoC would reveal, "Here is the contact data," and it's now the private registration service data.

Again, the registrant's name is already out there. But it's private registration service data.

So then you would have to go through the next step of piercing the veil of the private registration service in order to find out the actual contact information for the registrant.

So this -- I think this -- although if subgroup C's recommendation is adopted, maybe the domains by proxy type model is not so much of a problem, because they wouldn't have an OPoC. Here there still is an OPoC. And getting through the OPoC level, you still don't know where the registrant is.

That's the problem, I think.

>>BRUCE TONKIN: (inaudible) know where the registrant was.

>>STEVE METALITZ: You don't know who the registrant was. You know who they are in the sense that -- as I understand it, their name appears on the OPoC proposal.

>>JON NEVETT: Their name appears in WHOIS, so you know who the registrant is. And I don't see this double layer that you do. If we sell the service, then we would put that information in. It's not going to be double layers, because the registrant won't be able to layer on top of that. Either you have our service or you don't.

>>STEVE METALITZ: So if you structure the service in a way to say if you take our service you can't designate anyone but us as the OPoC, that's right, then there's only one.

>>PHILIP SHEPPARD: That's very good, yes.

>>STEVE METALITZ: But that's not necessarily -- that would have to be --

>>PHILIP SHEPPARD: Is that workable?

>>BRUCE TONKIN: I don't imagine --

>>STEVE METALITZ: We would have to waive your OPoC.

>>BRUCE TONKIN: I guess this service hasn't been -- this whole OPoC policy is not in place yet, but if I had to state the way my understanding of the model is, essentially we would -- sorry, essentially just speaking on behalf of Melbourne IT, what we would do is those contact details, which are post office box, et cetera, would be going to the OPoC fields. But the registrant data that you are referring to as the next layer would be the registrant data. We wouldn't be separately offering that service.

So I'm kind of agreeing with Jon. I don't think we create two layers there.

>>STEVE METALITZ: But the point is that under the OPoC system, the registrant has the choice of who to designate as the OPoC.

>>BRUCE TONKIN: That's right, yeah.

>>STEVE METALITZ: And unless it's ruled out contractually, if Melbourne IT says if you want to be in our registration service, you have to designate us as the OPoC, or you can't designate anybody else as OPoC.

>>BRUCE TONKIN: If you want to be in our private registration service. That's correct, yeah.

>>STEVE METALITZ: But absent that provision, and let's assume an actor that might not be quite as scrupulous as your companies, they would say we will offer you a private registration service, it works like the Network Solutions and Melbourne IT one, and you can designate Margie as your OPoC, and there will be this two-step process. Even assuming Margie does her job as the OPoC, all she will be saying is, oh, the contact information is the private registration service.

>>JON NEVETT: What address would you use for Margie in your example?

>>STEVE METALITZ: Margie's true address. The Margie Milam OPoC service.

>>JON NEVETT: Then Margie is the OPoC and not us.

>>STEVE METALITZ: Yeah, but all she has is your data.

>>BRUCE TONKIN: You can provide a privacy service that's not actually OPoC related. I think this is the thing. It comes back to what Bertand is saying. There are so many thousands of ways you create business problems around these things. I think you have to start with the principles. I think what you are saying, Steve, you can get a registrar that just decide to hide the data full stop. We provide the registry service, we won't provide it to anybody unless we have the court order. That's totally separate from OPoC, though.

In other words, they are just saying we are going to protect everything, so even if the OPoC doesn't come through, we are still aren't going to give you the data. I think that's what you are saying.

>>STEVE METALITZ: That's a separate question from what are the circumstances under which a private registration service has --

>>BRUCE TONKIN: That's what I am saying.

>>STEVE METALITZ: But even before you get to that question you might have to go through two steps to get to that point.

>>BRUCE TONKIN: No, but I think what I am saying is if you are just talking about OPoC -- is that right? Which is the admin contact.

>>STEVE METALITZ: No, no, OPoC is not the admin contact, Bruce. OPoC is something that, in the OPoC proposal, the admin and tech contacts are no longer displayed. OPoC is listed instead.

>>BRUCE TONKIN: Right, but what I am saying is it is functionally, from a technical point of view --

>>JON NEVETT: It replaces that.

>>BRUCE TONKIN: -- it replaces that, yeah. In other words, there's a difference between the registrant and -- at the moment you have a registrant and an admin and technical contact. And I am not proposing OPoC, I am just explaining it as I understand it. Now we are talking about you have a registrant and OPoC.

>>STEVE METALITZ: Which needs to be displayed.

>>BRUCE TONKIN: So the easiest way of thinking about it in terms of the existing contractual framework is if you read where it says admin contact in the current contracts, it's fairly similar to, it seems from what people have been describing, as OPoC. And then you are saying at the moment there are no rules around admin or tech contacts, and you are saying if we go to this new model you want to create rules around this thing which we have relabeled called OPoC, just relabeling the same technical field, you are creating some rules around what that is used for, if I understand correctly.

But now you are saying what happens if you have got layers and layers, but you can have that anyway. I can have -- it's like unwrapping a parcel or something. I can have my contact data, and then I strip those off and I give the contact details of the person who is sitting next to me who says it's not me who strips off their contact details. It's completely hierarchical. We can have thousands of levels. But the reality comes back to what Jeff is saying. What are you trying to achieve? If it's a phishing attack, you go after the party hosting the website and take it down. If you are talk about finding the end party for taking legal action, we have that problem every day. We get people who use fraudulent cards. You try and go a few layers. It's generally multiple layers. And I think what you are saying is there can be multiple players. Yes, there can. It's not saying it's a service registrants are providing.

>>PHILIP SHEPPARD: I am going to take a question from Bertrand, I am going to pose a question and then have a coffee break.

>>BERTRAND DE LA CHAPELLE: I must say the discussion on the proxy services is a bit frustrating because some of the proxy services are going to provide exactly the kind of service that an OPoC -- as far as I understand, that an OPoC is actually providing to private people. But then the proxy services is actually providing the same kind of protection for non-natural entities, but then they are not in the framework of the OPoC discussion on WHOIS.

So it's a bit difficult to address, because it's basically the same kind of service.

One thing that I get out of the whole discussion in the working group, and that is becoming more and more important for me to see what the problem is, what kind of problem we're addressing, is the distinction between the relay, reveal, and remedy.

I think when this emerge in the discussion, it's sinking in right now for me as being very simple and interesting angle, at least for me to, to try understand the problems we have.

Because if we then start from the need, and those are very simple to understand needs, either you get a need to contact, and then what we need is to make sure that the chain goes all the way along, and then comes back in good faith situations and in bad faith situations that we were addressing, either because there is a bad faith registrant or a bad faith person who wants to access or to contact.

But this is just a relay chain. A lot can be automated. A lot can be structured with agreements that any actor in the chain has the obligation to relay in an appropriate manner, whatever.

The reveal is a different element, because there are cases where you might want to reveal something because of some wrongdoing for future legal action, but connecting with the discussion on the commercial, noncommercial, you could have a situation where without anything illegal happening, you might want that under certain conditions the identity is revealed because it's actually a commercial activity, for whatever reason.

And then the next layer, which is remedy, where you have a certain number of cases where what you want is to get to the good guy sometimes who is actually being himself attacked. And what you want is takedown procedures. It's what you have, for instance, in the legal system at the national level. In France it's called refere. It's when you need an absolute immediate action because there is a major infringement or major impact if it is not remedied immediately. So you go to a court in that case and you have a decision that can be taken, boom, immediately.

So the three layers and the three angles are actually things that are actually very different and very easy to understand.

The remedy is a very rapid, quick action. It can be the takedown, it can be other measures. And then you can draw the line of how it works.

The reveal, you can connect it with the conditions for access by third party. And the relay, you can automate in a certain way.

Interestingly enough, if you take this approach, the reveal function could even take into account the revealing of other types of information that are already in the possession of registrars.

Registrars have credit card information for people who actually bought the domains.

Maybe in the line of reveal, there are conditions where the infringement has been demonstrated in the due process, and you can get the real information that is not present in the WHOIS at the moment.

So I'm wondering whether the distinction, as a finishing point, whether the distinction between the relay, reveal, and remedy is not actually the good angle to take the whole problem, because it even allows to go beyond the present WHOIS system.

It goes to the proxy services and it also goes to the possibility of accessing different types of information and making the thing more secure.

Just a --

>>PHILIP SHEPPARD: Thank you. It makes a very good point. It leads us into the discussion we want to have under item 3 in terms of actor or communicator role for OPoC.

The question I wanted to just finish off on this item 2 is, given that as a group we're saying we have agreement of this concept of splitting between legal and natural persons and legal persons would be full of WHOIS data, given also that we have said, I believe that was also in the initial proposal that OPoC would replace admin and tech contacts as today, would it make sense in terms of simplification that, whoever you are, legal and actual person, you would anyway be appointing an OPoC, and is there any reason to make a distinction about that, even though the function may be slightly different or the use of that may be slightly different if that replacement of admin or tech is going to take place.

I don't want an answer. I'm going to have a coffee break, but if the question is clear, it's a good discussion point, unless you want to discuss the merits of Puerto Rican rum which may be much more interesting.

So 15 minutes.

(Coffee break).

>>PHILIP SHEPPARD: Side conversations over, please. Transcription get going, please. Let me try to summarize a question I asked before the coffee break and see if we can come to some conclusion on that.

If we are saying in agenda the OPoC will be replacing admin and tech assuming there is some continued meaning for admin and tech, if you are a company with full data, even in a post-OPoC world, we now need something in place for that role, so it makes sense, does it not, that it is there for the OPoC so if you're a legal person or natural person, you would still be having a OPoC. Indeed, the only real distinction we're saying is the nature of the data that is currently shown at which point we're also saying there are three functions in terms of our three Rs, the reveal and remedy and whatever the other one is, sorry, relay, reveal and remedy.

Once you've gone down the first two of those to relay and reveal, the -- you're basically on legal terms if you are a legal person or natural person in terms of the accessibility to that data from the party asking for us. Therefore, it seems to make sense, does it not, that to have a OPoC under the same sort of rules and could elect for those as they choose. That was a rather complicated question. I hope it was clear.

Do we all agree?

[Laughter]

>> What?

>>PHILIP SHEPPARD: Let's do it in stages. Are we all happy with the principle which, indeed was prior to us that OPoC replaces admin and tech functions? Steve, yeah?

>>STEVE METALITZ: I just want to put on the record that, the OPoC proposal that was before the WHOIS task force did not say that. It said admin and tech would continue to be collected but OPoC data would be collected and would be revealed to the public as part of the public accessible to WHOIS. I am not trying to defend that distinction, I am just pointing it out.

>>PHILIP SHEPPARD: Slightly different perspective. Thank you. Are we happy to go beyond that original concept to wrapping into OPoC those responsibilities that are currently admin and tech, which does have the advantage, of course, of not actually expanding your current WHOIS database to have an additional contact? Jeff.

>>JEFF NEUMAN: Actually, I join with Steve there. I think that data does need to be collected, at least from the registry level. There is a lot of functions. I can't remember if the OPoC addressed things like transfers. So I'm not sure the OPoC is ready to take on all the responsibilities that historically have been admin and technical contacts. So I do think that still needs to be collected, at least from the registry's perspective as well.

>>PHILIP SHEPPARD: Could it replace one rather than both?

>>JEFF NEUMAN: Again --

>>PHILIP SHEPPARD: Or do you want to expand the database?

>>JEFF NEUMAN: The way the OPoC was described is really for this one purpose of WHOIS and reveal and all that other stuff. If you want to throw on other functions like being responsibility for transfers and being responsible for technical questions involving the site, I guess it could but I'm not sure -- I think that would add a lot more to the OPoC and make it harder for anyone other than a registrar to be a OPoC.

>>PHILIP SHEPPARD: Is the balance of doing that, though, better than the additional cost which would be expanding your existing database with one -- with a whole new set of fields to have the OPoC data as well?

>>JEFF NEUMAN: Actually with respect to EPP for all the registries that have put that into place --

>>PHILIP SHEPPARD: EPP being?

>>JEFF NEUMAN: Extensible provisioning protocol that most of the registries and registrars operate. It was designed to add additional fields. So to add fields from a technical perspective is not a big deal at all. In fact, we do it in -- let's say, I'll switch hats for dot U.S. We have additional fields. And then there are other registries that collect additional information. Now, you are also talking about storing additional fields and that may affect speed of relaying the information. But as far as adding the fields itself, it is not a big deal at all.

>>PHILIP SHEPPARD: Okay. Doug, is it?

>>PATRICK CAIN: Pat Cain.

>>PHILIP SHEPPARD: Sorry.

>>PATRICK CAIN: No problem. If the OPoC is really limited to only natural persons, then making the OPoC equivalent to the admin tech may actually work really good. But particularly for corporate entities, stuff that goes to an administrative contact is very different than the school's going to blow up that goes to the operations contact. You don't want to have the internal guts of the company have to figure out where to send something. Does that make sense?

>>PHILIP SHEPPARD: Okay. All right. If you're using admin and tech in a good way to differentiate the roles, there is use in that from the perspective of the registrant. Okay. Other perspectives on this?

>>PATRICK CAIN: On the other hand, many of the individual kind of domain holders make everything the same because it is only them for everything.

>>DAN KRIMM: It seems to me if there is a differentiation Pat is talking about all the information could go to all OPoCs at once and the right OPoC that needs the information will have it.

>>PHILIP SHEPPARD: Exactly. You have the possibility foreseen already of having more than one OPoC, don't we? That's an alternative, indeed. Other perspectives on this? So where do we want to come out? Do we want to carry on collecting all that data as Jeff is suggesting and expanding to have OPoC as well and we would do that regardless of the nature of the person being legal or natural? That will make sense in order that there is some consistency at least in the fields being collected. I do see a slight burden maybe on certain users that you are now asking them for five potential sets of contacts, which should all be the same, but may or may not be different. Perspectives on this? Are we bored to tears with the concept? Margie.

>>MARGIE MILAM: I'm sorry. What's the purpose of obtaining OPoC information for non-legal -- I mean, for legal entities, not natural persons?

>>PHILIP SHEPPARD: Because we talked also about a remedy function which got -- if it's -- if it goes up to reveal then you have obtained the data, yes, and the data set available to the party asking it is the same as an open WHOIS. If we're saying also that there is a remedy function that goes beyond that and that the OPoC is being used -- yet to be decided as a messenger or actor for that, then there is a need also for the OPoC for companies as well.

>>MARGIE MILAM: Right. Would the OPoC be able to reveal the underlying information in a private registration? Is that something that's possible?

>>PHILIP SHEPPARD: Yes, that's an intent certainly under certain conditions, yes.

>>MARGIE MILAM: Yeah, I think that makes a lot of sense.

>>DAN KRIMM: Dan again. One question I had was whether this relay, reveal, remedy needs to be in exactly that order. It seems to me there may be cases where OPoC is asked to relay a message and if there is no timely response on something, then a remedy can be taken immediately either by the OPoC or by the registrar that does not necessarily require any kind of revealing of private data.

>>PHILIP SHEPPARD: Mm-hmm. That probably makes sense, depending on what's being asked. Good clarification, actually. Steve?

>>STEVE METALITZ: I just have a question. Are we on the third topic now about remedy?

>>PHILIP SHEPPARD: No, not quite.

>>STEVE METALITZ: We're not quite there, okay.

>>PHILIP SHEPPARD: I am just trying to clarify the nature of having an attack, if that's still going to be collected and, indeed, displayed for legal persons and where we go with that.

Now, Bruce, when we were chatting at the coffee break, you seemed to be in favor of that simple model in contrast to what Jeff was saying in terms of use there, that he seems to prefer the idea that all that data is continued to be collected and we have an additional field and we expand the existing database.

>>BRUCE TONKIN: Yeah. I think -- technically, it is quite complicated to change a system just in terms of all the usages of the database. What we would probably do as a practical matter is probably map the OPoC to an existing field that we had, which is admin. That doesn't change what Jeff's fundamentally saying, is that we will continue to collect the data according to those requirements of the registrant taking billing. And we will have a piece of data which is displayed which we are calling OPoC.

So I was talking to Steve over the break. If you separate the collection from the display and you just focus on the display, so OPoC is a display piece of data and it has certain roles and responsibilities associated with that data that's displayed, if you'd like, that makes sense. I think you are going down a red herring, in other words. And I probably partly crowded the confusion by saying map the two things because I am saying the OPoC to me is an equivalent of what we are currently displaying is admin/technical, according to the way I would put it. As Jeff says, there is a whole bunch of contractual requirements about collection of data, and I think we're saying leave that alone. And now we're saying we have got this display element called OPoC, and we are talking about the roles and responsibilities of that display element.

>>PHILIP SHEPPARD: We are going to be changing contracts, anyway, in terms of the outcome of this?

>>JEFF NEUMAN: It is not just the contract. I was just thinking about things like transfers.

>>BRUCE TONKIN: Transfers currently specifies the authority to contact per transfers the admin information.

>>JEFF NEUMAN: I am not sure the OPoC is going to be willing to take that responsibility on to get off-codes and make sure the transfer is actually authorized.

>>BRUCE TONKIN: It is a different topic, I think. Yeah.

>>ADAM SCOVILLE: Could you speak closer to the mike there. We are having trouble hearing.

>>PHILIP SHEPPARD: Understood. We are saying on the technical side you are happy about expanding the data collected. On the user side, we are happy there is an additional burden for registration of names. Is that what we're saying? Jeff?

>>JEFF NEUMAN: I want to add one more point that wasn't brought up. From a registry perspective, we would like to have the data as kind of an escrow vehicle as well, at least until there is a formal registrar escrow program that's implemented. One of the other reasons that we want that data is for cases where a registrar goes out of business.

An OPoC, while it may be someone who is appointed for the sole purpose of receiving service of process or something to that effect, it is not the same as actually having the information about the registrant for cases of registrar failure. Yes, the short answer is I am in favor of expanding the data set.

>>PHILIP SHEPPARD: Everybody comfortable with that? Yep? Okay.

Let us move on to item 3. There was discussion in terms of the remedy function as to basically how much power, I suppose, we are endowing upon the OPoC and should they in some way or another be the actor for take-down or whatever or are they always in the role of communicator. That discussion also came up on Steve's group, I think, wasn't it?

>>STEVE METALITZ: Right.

>>PHILIP SHEPPARD: Could you also just flesh out quickly that discussion, and then we will talk about it.

>>STEVE METALITZ: It was not an area where we really reached a clear consensus, but I think there was agreement in describing the capability for the remedy function would be that the OPoC either has sufficient technical access and permission level to remove content from a site to which the domain name resolves or disable certain processes of resolution or has authorization from the registered name holders to direct the registrar to do things like that, to make a site go dark, for example.

But I think there was recognition that there was something that the OPoC should only have the authority to do or to direct the registrar to do in a limited category of serious cases. In other words, if you think about a phishing situation, for example, as we've already discussed and the need for great speed in dealing with that problem, if we can define that category of cases clearly enough, that would be an area where the OPoC should have some remedial capability. But there would be many other cases where the OPoC's responsibility was limited to relaying and then if -- or was limited to relaying and revealing. But there would be some category of cases where they ought to be able to take this further step.

I couldn't I don't think we really got very far at all in defining clearly what that category of cases would be.

>>PHILIP SHEPPARD: Dan.

>>DAN KRIMM: It seems to me it would be useful to distinguish between authority and responsibility for remedy on the part of the OPoC. It may be that many remedies are carried out by registrars but OPoC has authority to carry out certain remedies, especially if they can forestall more general remedies that go beyond the specific need and the circumstances.

>>PHILIP SHEPPARD: Okay. Other perspectives on this? Milton?

>>MILTON MUELLER: Based on my understanding of what the OPoC is, I'm kind of uncomfortable with the OPoC having any remedy functions per se. Again, I think it is more of an identification or communication function and it goes back to the discussion we were having earlier this morning about who is the contract with and who's serving whom.

The OPoC is an agent of the registrant and the take-down functions or other kind of remedy functions should be executed through the registrar or the Internet service provider, I would think.

>>PHILIP SHEPPARD: Pat?

>>PATRICK CAIN: Pat Cain. But there is two types of take-down. By the way, I hate that word. One is the domain as a whole has some problems and the registrar can easily go whack the thing pretty quickly. The other thing is something like there is a bad page on Yahoo.com and although people may want to, you don't really want to take out Yahoo.com. You want to get to the guy and wipe out one legal piece of his big-honking server. The remedy could have one person that could deal with it.

>>MILTON MUELLER: (inaudible). They don't want OPoCs to be content sensors for the Internet. They are not in any position to be doing that.

>>PHILIP SHEPPARD: That probably leads more to, again, the OPoC as a communicator to make a request, huh, in that case to the ISP and the registrar. Where we are at the moment on a remedy, the question -- I am looking at 309, authorization from the registered name holder to direct the registrar to take steps to resolve the problem is I think where we're coming out. Is that correct? Steve and then -- Scott was in the queue anyway. Scott, off you go.

>> SCOTT VOWELS: One of the points regardless of the process, I am going to beat that horse again whoever that point of contact is should have not only the authorities but the accountability to be able to take action. Otherwise, as one of my primary functions is as an incident responder, all I see is a delay in the response process, that's been something that I think has been fleshed out?

>>PHILIP SHEPPARD: You are happy if the OPoC is doing their job, then, if that simply is manifest as them directing the registrar to take the side down or put it in a hold or whatever we laid out in the report, that works for you.

>> SCOTT VOWELS: The other side of this is something that was raised a little bit earlier, it is something I would be interested in hearing about because I don't really understand, how are those folks being held accountable for that privilege or that responsibility? In other words, there must be -- I am sure you can find statistics on these sorts of issues happening and the delay that's in there and if we find that any of these folks that are able to take action are creating delays that are resulting in fraud and other bad things, how are they being held accountable? Do you guys do anything in that regard? Are we reviewing that and are you taking action?

>>PHILIP SHEPPARD: The answer is I don't know, and think that's a function of the detailed implementation of this, in terms of the time frames we end up seeing for that and how satisfactory they are. That's a good point.

>> SCOTT VOWELS: As long as you make provision and actually act on --

>>PHILIP SHEPPARD: If the time frames aren't -- exactly. Steve?

>>STEVE METALITZ:

>>STEVE DELBIANCO: The status quo Bruce was kind enough to quickly share with us, the minimum requirements of adequate to facilitate timely resolution of any problems. Adequate to facilitate timely resolution.

>> SCOTT VOWELS: What does that mean?

>>STEVE DELBIANCO: Both "resolution" and "timely" are important terms and so is the word "facilitate." If by facilitated only means to reveal the person you should go call, I think that's what Philip is getting at. How much does remedy include?

But remember this group that came up with the three Rs, our charter, according to the work plan, was to define the roles, responsibilities and requirements of the context available for unrestricted public query access and what happens if the responsibilities are not fulfilled, okay?

So we came up with responsibilities, the three Rs, relay, reveal and remedy.

And within remedy, Philip, you were just asking about the "or" question, does the OPoC themselves have to have sufficient technical access and permission? That's a capability. The reason we wrote it that way, we were charged to say what are the capabilities. Someone can certify that, yes, I have the capability to access the server. I have the passwords. But they might certify that on day one. But on day two, things have moved around. The registered name holder is a bad actor who is evasive and the OPoC can't get to them.

It is not as interesting probably that we serve fight capabilities as it is that we impose responsibilities. After the "or," you have authorization from the registered name holder to direct the registrar or ISP, I would propose, so we don't get stuck on saying it is only the registrar. It maybe the ISP who handles the most immediate implementation of stopping a site from a denial of service attack or a phishing page. ISPs are in much a better position and they do so today at the request of law enforcement, which is to take steps to resolve the problem.

I would propose the second half of the "or" may be the way we go but maybe we should modify it to say registrar or ISP.

>>PHILIP SHEPPARD: That makes sense. Any other perspectives on this before we move on? Dan.

>>DAN KRIMM: It seems to me the OPoC would be acting on behalf of the registrant and it is the registrant who ultimately has the responsibility to make sure a remedy is made if there is a problem. So I would agree that sort of the principle choice for remedy would be ISP or registrar and then if that's not happening, the OPoC may have the capability to act on behalf of the registrant but the registrant, you know, takes the responsibility for action and if the registrant or its OPoC does not take action in a limited way, that creates the possibility that a registrar or an ISP will take more global action.

>>PHILIP SHEPPARD: Yes, yeah.

>>DAN KRIMM: It seems to me that's a preference structure that we might look at.

>>PHILIP SHEPPARD: I think that's the way we're going, yeah. Steve.

>>STEVE METALITZ: Just one other point. It may go without saying but not only does the -- I will say it anyway. Not only does the OPoC have to have the capability to do this or the authority to speak on behalf of the registrant, but the registrar has to accept instructions from the OPoC that are within the scope of its responsibilities.

>>STEVE DELBIANCO: As would the ISP.

>>STEVE METALITZ: As would the ISP. I am talking about here the registrar. It has to be made clear, if the OPoC asked the site to go dark, it is as if the registrant has asked that.

>>STEVE DELBIANCO: Yep.

>>PHILIP SHEPPARD: Steve.

>>STEVE DELBIANCO: We want to avoid a situation where an OPoC claims, I'm sorry, I understand you have a legal request for me to take down offending conduct or a phishing site. But I don't have authorization to do that. I've called the ISP, and I'm not authorized. I've call the registrar, and I'm not authorized.

I think we could all agree that would be an unacceptable situation so we are trying to anticipate that in our language in imposing requirements, trying to avoid that excuse that says "I can't do it."

>>PHILIP SHEPPARD: I think that falls into the same path as lack of response from OPoC, if they are saying I can't do what they are supposed to do. It is the same as not replying in which case you go to the registrar to take the action. It is failure of responsibilities. Okey-doke. Jeff?

>>JEFF NEUMAN: So it is the registrar or the ISP but not the registry? The reason I say that is because we often as a registry get calls from registrants or others claiming that a registrar is not taking a certain action. Of course, we have no situation with the registrant and certainly won't have a relationship with the OPoC, I want it actually put into the documents that it's not the registry's responsibility.

>>PHILIP SHEPPARD: Well, if we look at --

>>ADAM SCOVILLE: Speaker, speak up.

>>PHILIP SHEPPARD: -- the report, and I can't remember where it is, if it's in this version or --

>> Version 17.

>>PHILIP SHEPPARD: -- an earlier version.

>> Version 17, line 275.

>>MARILYN CADE: Philip, I just want to note that I think people on the conference phone seem to be having trouble hearing some.

>>PHILIP SHEPPARD: All right, thank you.

So under remedy function to be discussed, besides request to the registrar, line 275 was a request that the registry suspend website DNS, recognizing that may have a time delay.

>>JEFF NEUMAN: And that's not going to happen. That's not very peaceable at all.

>>STEVE DELBIANCO: Philip and Jeff, this is under the paragraph that says that a registrar would take the steps. And it's the registrar requesting that the registry. It's not the registry seeking to take out the content. It's the registrar/registry in your own agreement.

>>JEFF NEUMAN: That's not the way things work. The registrar doesn't request the registry to suspend DNS. The registrar does it itself. So it's not a request to the registry.

>>STEVE DELBIANCO: That's okay, then.

>>PHILIP SHEPPARD: That's inaccurately written, then?

>>JEFF NEUMAN: Yes. We need to rewrite it that the registrar may suspend the DNS. But it's not the registry.

>>PHILIP SHEPPARD: And the registrar can lock, in the same way? This is line 277.

>>JEFF NEUMAN: Right, the registrar can lock, yes.

>>PHILIP SHEPPARD: Everybody happy with that?

>>MILTON MUELLER: I'm not sure.

>>PHILIP SHEPPARD: Pat first and then Milton.

>>PATRICK CAIN: As a point of procedure, Jeff, will you use different microphone? I think you are talking into something that's dead.

>> No.

>>PATRICK CAIN: No? It's just Jeff?

>>JEFF NEUMAN: Is that better?

>>PHILIP SHEPPARD: You need to be very close to these mikes, yes.

Thanks, Pat.

Somebody here. Milton.

>>MILTON MUELLER: I'm not sure whether we are agreeing to allow the OPoC to be a decision-maker who decides if down or not, and we clearly wouldn't support that. So what do we mean here by remedy?

>>PHILIP SHEPPARD: Then who is a decision-maker?

>>MILTON MUELLER: Well, due process, legal due process, or the registrant.

>>JON NEVETT: Just to add to that, registrars have reasonable policies that can be implemented. Web hosts have acceptable use policies that could be implemented. ISPs have acceptable use policies that could be implemented.

I'm not sure why the point of contact which currently doesn't have any special powers other than the registrant itself could itself take its own Web site down, I guess.

>>PHILIP SHEPPARD: Yeah. All we are saying here, I think, is the OPoC is the conduit to the registrar to say do those things that (inaudible) can do.

>>JON NEVETT: Just a question. Why would the OPoC involved at all in a takedown?

>>PHILIP SHEPPARD: Who else would be?

>>MILTON MUELLER: Whoever is authorized to order the takedown just goes directly to the registrar or the ISP.

>>JON NEVETT: The OPoC is a conduit to the registrant. So the first step would be, perhaps, in the example someone used before, where there is a good actor that had some underlying page that is problematic, you know, that's a conduit to that good actor, and use that as a vehicle to get in contact with the good actor, the registrant.

But to have the OPoC have some kind of role in a takedown when the OPoC is, effect, representing the registrant doesn't seem to make a lot of sense to me.

>>PHILIP SHEPPARD: You are arguing about no remedy function at all for the OPoC. From what I am hearing.

Steve.

>>STEVE METALITZ: I think the question is, and I'm sure there's people on the other side of the room that can answer this. Currently, are there situations where it is necessary or advisable, preferable have the cooperation of the registrant in solving, say, a phishing problem.

If there are, then the OPoC needs to be able to give that cooperation on behalf of the registrant.

So that's really again the OPoC standing in the shoes of the registrant. You can't find the registrant but you can find the OPoC.

So the OPoC needs to have the authority to cooperate or to make a request, if that's needed, to facilitate the resolution of the situation, and whoever they are making the request to should honor it, as if it were coming from the registrant.

>>SCOTT VOWELS: If you don't do that, this is Scott, you are just creating a delay. You are putting another person in that chain of information that just delays the response time.

>>MILTON MUELLER: You are trying to get the OPoC to act as an agent for the registrant when -- if there's a legal problem, a serious legal problem, you should be going directly to the ISP or to the registrant. You shouldn't need the involvement of the OPoC at all.

>>PHILIP SHEPPARD: Pat.

>>PATRICK CAIN: This is Pat. One of the problems at least I have had in the past few months, and I'm sure others have, when we say OPoC everybody has a totally different picture of what that means.

Now, that maybe good. On the other hand, that may not be good.

>>PHILIP SHEPPARD: This is the tapestry we are creating here, stitch by stitch. Sometimes I think there is a Penelope out there undoing it at night.

>>PATRICK CAIN: As long as you don't come up with another name for it.

I think part of the concern is when I think of OPoC I think of this functional blob that looks a lot like the agent or proxy or something like that and mostly protecting the man's identity.

At the same time, if I am a registrar giving OPoC services or if I am a company giving OPoC services or if I am not very bright in giving OPoC services, I inherit a bunch of different functions that people kind of roll into the OPoC.

So from Milton's point of if I am just the OPoC and I am protecting my fine friend here, you send me something, my duty really is to give it to him, make sure he gets it or maybe send you back a, no the man is a Bozo and doesn't really want to talk to you before but if I am an OPoC with the other functions sucked in I may in fact own some of the remedy. If I am the registrar and I am acting as an OPoC, too, I may end up having to do some of that other stuff. And we don't seem to be very consistent in our -- an OPoC is really just a relay person and the rest of the stuff falls under something else.

>>PHILIP SHEPPARD: Okay. We've got Jeff and Mawaki.

Jeff. Let's have Mawaki first. You haven't said anything yet.

>>MAWAKI CHANGO: Yes. My understanding of OPoC, since everyone has a different picture, is that it's a proxy substitute to the registrant.

So whatever we need to convey to the registrant, we'll convey to the OPoC.

So the OPoC responsibility is to make sure that the registrant is -- there is no delay between the OPoC and the registrant. There is no communication delay. So the OPoC has the responsibility to ensure that the registrant is informed, and whatever they need to do to solve the problem, they do it.

But if there is a problem like phishing problem or content related problem, then there are other means to resolve it, like ISP. Because the registrar actually registered the domain name. They are not really involved in the content normally.

So I think that's the distinction, or that's my understanding of the OPoC.

>>PHILIP SHEPPARD: Thanks.

Jeff.

>>JEFF NEUMAN: Two things, and John Cain just pointed this out. The OPoC could be the registrant itself. So asking the OPoC to take these kind of actions would be kind of bizarre. It's really not going to order itself -- it's own domain down.

And isn't the real remedy the reveal? We are mixing the two R's up. But the remedy for failing to, you know, do what it's supposed to do is the reveal of the actual information.

And I would think that that is the remedy.

And that should be the sole remedy of the OPoC.

>>PHILIP SHEPPARD: Bertrand.

>>BERTRAND DE LA CHAPELLE: I'm incredibly happy that somebody dared to say what I have been feeling so much in the past about seeing different perceptions of what the OPoC is. I think the distinction that was made earlier is very clear now in my mind. When you have the two functions, one is sort of an anonymizer, which is basically a relay function. I put somebody in between but with the agreement that anything that should be sent to me or asked from me goes through this person. It's just so that I don't have the -- my contacts available. But it can be almost fully automatic, just like another e-mail address for another contact.

And the second function, which is the proxy service function, where it's actually in lieu of the person -- some other actor is providing the service, usually a paid service, where this actor will take the full responsibility.

So aren't we actually going in a direction where we are trying to find a regime that handles the two questions, the proxy activity and the OPoC that would then be restricted to the anonymizing service? Would that clarify the picture if we were using OPoC for the anonymizing function and proxy for the real stepping in?

>>PHILIP SHEPPARD: So what we're saying is, is the OPoC is doing what we so far described as relay and reveal. And it is only in the case, then, when there is failure there that the requester then goes directly to the registrar and seeks remedy.

Is that what we're saying? And does that work for everybody?

>>STEVE DELBIANCO: Steve Delbianco, I propose a scenario. I am a U.S. user, I am on a cable modem. I am a natural person, and I've set up a home Web site. And I appoint an OPoC. And my site then is hacked, unbeknownst to me, and it is service up denial of service attacks.

The OPoC is contacted about this by perhaps the company being attacked. It may not even be law enforcement.

And what is the OPoC's first responsibility? If it's relay, they immediately and automatically relay an e-mail to me, and I am on vacation in San Juan and unreachable today.

And so within some period of time that we have yet to be determined, they would then reveal; right?

So I don't think there's much controversy about that, and they would reveal that information, provided that the demonstrable harm is conveyed in the requester's request.

But let's not just scrap the able of remedy for that OPoC. Because if the OPoC relayed reliably and they revealed and the OPoC is reachable on a 24/7 basis. If they have the authority with my ISP, let's say it's Cox Cable, if they have the authority to act on my behalf because nobody is home at my house, the Web site is still up, and they can ask Cox to take down the site, well, then the OPoC is in a much better position to do that immediately, I think, than the requester in that case.

They have authority to do so. And why would we not want to encourage, perhaps even require the OPoC to have the authority to do so?

>>PHILIP SHEPPARD: And the advantage, of course, is you have already proved the responsiveness of the OPoC by the nature of your first request to them, which led to the reveal function. Whereas responsiveness of the registrant, once revealed, is untested and unknown.

Okay.

I've got Pat, Milton, and Jeff.

>>PATRICK CAIN: It's Patrick Cain.

Steve, I think that's actually a bad case or a bad scenario. Because for operational kind of things, particularly for cable modem things, you call up the ISP and say we're having this problem and the ISP is just going to -- or at least we're just going to kind of wipe you out. I don't really care who it is at the end. The machine is just going to go off the network.

And so that's why a lot of the OPoC things I see are related to content, where you can't just wipe somebody out but you have to go back and talk to the person.

So I would use a different scenario as in somebody said really bad things about Pat Cain and it's on somebody's Web site and I went off and I don't get any response. Then what happens? Because then I need to know who the person is because there may be some follow-up legal stuff that I want to do.

>>PHILIP SHEPPARD: All right. That was Milton next.

>>MILTON MUELLER: And that simply makes the point that I want, which is you don't want an OPoC deciding who gets censored, and you don't want -- you see, there can be bad actors in terms of people generating denial of service attacks or putting up bad content. There also can be bad actors who are manipulating the system who get sites taken down that shouldn't be taken down. You have to be aware of that.

And the idea that somebody has volunteered to or relay information to a registrant can decide whether this Web site is libeling Patrick Cain and should be taken down is just not on. That's way too much authority to load onto this person.

And in both cases -- again, if it's a copyright case in the United States, for example, there is the DMCA that you go directly to the ISP. So you don't need the OPoC for that. And many other countries would have similar processes.

So there's really no need to load those kinds of functions onto the OPoC, which is -- And even if they were responsive and revealed and you are still on vacation in San Juan, unless you put your mobile phone number in there, which I wouldn't advise you to do, they are not going to be able to reach you anyway.

So under the DMCA you might get your site taken down while you are on vacation if you don't respond, and that's tough. I mean, that's the law. It may not be right, but we have to be aware of both ends of the coin here, that a takedown process can be abused and has been abused.

So let's not put that on the OPoC.

>>PHILIP SHEPPARD: Okay. Jeff.

>>JEFF NEUMAN: I guess I was just going to agree with both of those comments from Milton and Pat.

I'll try to move closer. There we go.

The other question is, Steve, it almost -- you almost made it sound like you wanted the OPoC to have some sort of direct access to the registrar to make these changes itself. Is that -- I hope that's not what you were implying.

>>STEVE DELBIANCO: No, but they would have the same authority as the registrant since they are stepping into the shoes of the registrant.

>>JEFF NEUMAN: But when you are saying that, if you have the same authority as the registrant, then I guess access has to be given to the OPoC, to the actual domain name registration, which means the OPoC can make changes to any part of it. And I don't think that's really contemplated by any of the registrars. And I'm not sure -- Again, if I were to appoint an OPoC, it wouldn't be to be able to make any changes to my records. It would just be for hiding my information, essentially.

>>SCOTT VOWELS: This is Scott.

>>PHILIP SHEPPARD: I have Bertrand on the queue first.

>>BERTRAND DE LA CHAPELLE: Actually, this goes to the distinction that was made earlier. And anytime now I hear the expression "is acting in the place of" or "in the shoes of," this is in the category of the proxy thing. If it is just the relay function, it is a different thing.

If it is a proxy, I understand, because it is the actual registrant, it has all the access that is needed; right?

So there isn't necessary to something. It is the registrant acting on behalf of somebody else with all the liabilities attached.

If it is just an anonymizing function, what we could call forsake of discussion here, the main OPoC function, I designate somebody who has the role of sending information to me, the question I wanted to ask is in the present situation, what happens when there is a need to take down, either because there is a phishing and a very immediate danger, or because there is libel or anything that needs to be taken down or copyright infringement or whatever, what is the procedure today? I have my data available in the WHOIS. I don't think anybody is going to come to me for a notice on takedown. It will be to the ISP or to the host company for user-generated content type of thing, like MySpace. Is that right?

If that is the case, I agree, I don't think it is necessary to put the burden on the OPoC in the anonymizing function to do anything. It's the present procedure that should be put in place, going to the ISP or going to somebody else, with the understanding, as Milton said, that it can be abused, but no more than today.

So I'm interested in the present situation.

>>ADAM SCOVILLE: Adam in the queue.

>>PHILIP SHEPPARD: Adam, yes, and I have Scott as well and Jon in the queue. Anybody else? And Pat.

>>PATRICK CAIN: Answer his question.

>>PHILIP SHEPPARD: Scott.

>>SCOTT VOWELS: I guess my immediate question, then, would be -- this is really getting deep with the OPoC thing. But as an anonymizer, as you described it, if I am able to get in touch with that anonymizer and immediately get the information, what's the value of having it?

>>BERTRAND DE LA CHAPELLE: The main -- The main question goes to the conditions by which you have access to this information.

There are certain cases, and this goes back to the natural and legal entity and commercial, noncommercial. You can have the full access to the data the way it is today. You can have a reveal function that is, for instance, on a case-by-case basis with a very light system, with a clearinghouse or whatever that could be put in place. If, for instance, there is an agreement in the group and the future regime that if an individual is conducting a commercial activity, then this information should be available upon request, for instance. Not be accessible for everybody all the time. But if there is sufficient information and there is a decision that this should be implemented, it's possible.

But that would be for activities that are fully legal, and you have a reveal function.

Then you could have a reveal that is going even deeper, if there is a malevolent action, then you could have further information, further action, maybe go to the credit card and so on.

So you can have deeper and deeper levels of information depending on the gravity? No, no, the gravity -- how bad the behavior --

>>PHILIP SHEPPARD: Gravity of the alleged bad faith, yeah.

>>BERTRAND DE LA CHAPELLE: So that's -- that can be accessed but not necessarily in the way it is accessed today. Or requests can be logged or that sort of thing.

>>PHILIP SHEPPARD: Okay. Adam on the phone.

>>ADAM SCOVILLE: Yeah, I just -- I want to agree with Milton with respect to the extent to which we're a little uncomfortable with the OPoC as the censor.

>>PHILIP SHEPPARD: You are a little faint, Adam. Can you talk a little louder?

>>ADAM SCOVILLE: Is this better?

>>PHILIP SHEPPARD: Yeah,ish.

>>ADAM SCOVILLE: I am agreeing with Milton, I am a little uncomfortable with the idea of OPoC as the censor. But I guess to some degree it also comes back to how in these kinds of severe cases that we refer to as these reveal events -- sorry, remedy events, how the registry and registrar do some of that already. And we've heard people refer to if someone contacts a registry or a registrar, we've heard a couple of folks, I think from each camp say -- if someone comes and says there's a phishing page, you know, we're going to take action.

And, you know, it's a little bit of a legal black box, because I'm not sure that there's anything that requires them to necessarily take action on that, but my sense is that when it's clearly so egregious a case, then -- I don't know exactly what the legal framework is, but maybe they are just saying look, the risk that this complaint is not valid is very low and we are willing to take the risk in order to sort of be good citizens, I suppose.

And it's a little bit the same kind of black box. So I think we should figure out whether this kind of function is necessary for the OPoC.

I think we need to go back and get an answer to the question that Steve posed, which is is it ever useful to go to the registrant in cases like that? If it's not useful to go to the registrant, then it's true that we don't need to go to the OPoC. And if we don't go to the registrant, maybe we go to the OPoC and they make the same kind of judgment of, gosh, is my client conducting a major financial phishing scheme that the registries and registrars make right now.

And maybe that will solve the problem for us and we say, look, in these kind of cases you are never really going to care to go to the registrant. And if that's the case, then maybe we don't need this kind of function.

But maybe we should answer that.

And just to add the last thing. I'm not sure that anyone, just in terms of scope here, I'm not sure that anyone would say that defamation -- the idea that oh, there's a Web site where someone is saying really bad things about Patrick Cain, to use his example, I'm not sure that I would have thought of that as being the kind of egregious case that's in the remedy function in the first place, just to avoid sort of expanding that scope beyond what we perhaps intended it to be.

>>PHILIP SHEPPARD: No, I think you're right to some extent. I think once we clarify that the OPoC is really playing an agent role, I think that leads us down certain paths and closes off others. I think that clarity will help us going forward.

In the queue I had Jon Bing.

>>JON BING: Thank you.

I am -- just as we have mentioned, made mention of the DCMA, I think we also should remember that the electronic directive of the European region probably have some relevance for this, and we should be able to make the host liable, if not removing offending material.

It is of course more complex than that proposition. But it does have that type of regulation for the position of what the director likes to think of as a host. And it also does that for proxy service and main conduit of data.

I don't think that -- I think that only the provisions of the host really has a bearing on this issue. Thank you.

Sorry, and it extends not only to corporate infringements but to all type of ending material content.

>>PHILIP SHEPPARD: Are you saying, Jon, the relevance of that would be the role of the OPoC as agent for the registrant in terms of fulfilling that requirement?

>>JON BING: Well, the request will be posted to the host itself, and the host has to have the means to follow that request if the host does not want to become fully liable for the violation or infringement.

>>PHILIP SHEPPARD: Right. Okay.

Pat.

>>PATRICK CAIN: I wanted to answer Bertrand's question on what happens now, and I will keep it short and I am going to generalize so I won't get beat up by any of my friends.

When a phishing report comes in, you normally do a criminal versus civil kind of check to see if it's obviously something that's a criminal activity versus something that's kind of shaky.

The criminal stuff then is handled pretty quick which is you go out to site, pull out the domain data and all the contact data out of it, quickly send off a message to the person to point out that they are doing this thing that's bad.

You can also use the domain data to look at local database to see if this is somebody we know, is it one of the 35 or 37 groups that do this kind of stuff. Do we know where the guy lives already, that kind of stuff.

Then when you don't get a response back from the person, you go off and try to figure out what are the means you can use to get the collection site disabled.

And sometimes that's calling up the hosting company. Sometimes that's talking to the registrar. Sometimes it's talking to friends in some place.

And you show up mostly with this kind of form that we have been working on, which is the "dear Mr. Person. Here is how we are going to prove that this is criminal activity and probably shouldn't be there." And we're working with the registrars to come up with a best practices kind of piece, so we can go to a registrar or to a hosting site and say, "See, it meets all ten of the boxes for bad person. Can you please deal with this pretty quickly for us?"

A number of them will handle it pretty quickly, within a couple of hours. A couple of them will take a month because they have to do an investigation and think about it. In a couple of cases we have to translate it to the right version for them to understand it.

And then we keep an eye on it to see if it comes back someplace else or if the person is moving around.

>>PHILIP SHEPPARD: Okay. Jeff.

>>JEFF NEUMAN: I think we need to make a distinction between certain types of activities.

If it's an intellectual property infringement, please from our registry perspective, that's something that we, as a registry, don't deem as something that we would take immediate action on.

Whereas if it's something like if there is a domain that's infected with bots or if there is other malware or phishing, unlike intellectual property infringement, there's a lot of evidence out there when that activity is going on, evidence you can't really hide.

So when we are presented with that evidence, and I am not going to say exactly how but we have laboratory environments and other things where tests can be run. And that is pretty obvious on its face.

And when we have that evidence, then that's something that we will do a takedown. And to answer the question, no, we do not contact the registrant nor should we. In a lot of cases contacting the registrant could make it a lot worse because then the registrant could just turn off that domain and go to another one.

And oftentimes, there are so many domains infected with these bots that if you are lucky enough to find a command and control bot, you want to turn that off and not let the registrant know that you found that, because that could damage its entire registration. And if you move it, you just jeopardized everything you were hoping to do.

So, you know, the simple answer is for extreme cases, no, there is no reason to contact the registrant and no reason to contact an OPoC for that.

Now intellectual property infringement and all that other stuff, in a lot of case, a lot of gray area, that may be a completely different scenario.

>>PHILIP SHEPPARD: So for more serious stuff, indeed, you could have a request straight to you. You can check it out and see how -- see how simple that request is and check that anyway. So we don't even need to discuss that because that can happen today regardless as if we know who the registrant is or not.

>>JEFF NEUMAN: It can happen in dot biz because we have it in our restrictions document in the new contract that was approved for dot biz, although nobody actually focused on it and everyone is focusing on terms and other stuff. There is a provision that gives a registry the right to take that action to take down those names. And just also -- it is usually --

>>PHILIP SHEPPARD: Are you saying that's universal? That's clearly the case of dot biz? Is that a universal requirement?

>>JEFF NEUMAN: That's something in our biz. Also to point out, the evidence usually doesn't come from one person but there is lots of organizations of ISPs or other organizations, something called Castle Cops, other organizations that would notify us. It really doesn't come from an IP owner or a brand owner. It comes from known sources.

>>PHILIP SHEPPARD: Okay. Steve.

>>STEVE DELBIANCO: Pat, I had a question for you. This is Steve Delbianco. You said in some instances when your group prepares a request to a registrar or ISP, they do not act right away. My question would be, are any of those

instances of delay due to the need to check with the registrant to where the ISP -- or registrar feels the need to check with the registrant? And if those situations do cause delay, substantial delay, causing harm to consumers, I would ask, isn't that stuff justification to give the OPoC agency responsibility to step into the shoes of a registrant who will not reply?

>>PATRICK CAIN: I wouldn't have characterized my explanation as we don't do anything. In trying to be polite, we hit up somebody with, hey, guy, you have this problem and there is a pretty short timeout before we do anything. We send a message to eBay and we don't say, Let's wait a week. Most phishing stuff has to get shut down in four hours or we have a real problem. So you send a message out and you wait maybe a little while, maybe a half an hour.

Then you say, we know this guy, he is not going to reply.

>>STEVE DELBIANCO: And then you do what? You go to the registrar?

>>PATRICK CAIN: We escalate it up to the next place.

>>STEVE DELBIANCO: When you escalate it to the next places, it is an open question, do those open places ever delay their response to you because they would like to check? In slam-dunk cases, it's easy to check. Where it is sort of marginal, do they want to check with the registered name holder, in which case the OPoC might be an appropriate proxy?

>>PATRICK CAIN: Since the next step we go to includes a lot of the ccTLDs and places like that, every country has its own kind of odd behaviors. So some places we can show up with a -- not only is it phishing, we already saw this stuff and, hey, look they already phished you, but they won't shut down the site for a month because they have to do some type of investigation.

Other places you show up and say, Look, it is really this bad, you should do something, and they go, You're right, we should and it goes very quick. There is no global -- it would be nice if everybody did it the same way but there is no chance in hell.

>>PHILIP SHEPPARD: Are we saying that typically there is a number of requests which can go straight to the registrar for which it is unnecessary to discover who the registrant is? And that can happen anyway? And, therefore, that's happening today basically out of the scope of our group?

But there are other types of requests for which we need to go a slightly lengthier path where take-down is less clear and we do need to find a route to remedy function, which we're saying is at some point needs an attempt to contact the registrant once you know who they are from the OPoC, if you're told that.

And if that happens, fine, that happens, end of that path. And if it doesn't, then what do we do? Do we need to go back to the OPoC? Or do we go straight to the registrar again? Or ISP? Otherwise, it is going around in endless circles. Are we all agreed with that as a path through in modifying where we are on the remedy function? I'm hearing nobody against, so I shall assume we have agreement at least here. We shall see that in black and white and we can all change our mind next meeting.

>>MILTON MUELLER: (inaudible).

>>PHILIP SHEPPARD: On what I just said.

[Laughter]

Basically, we are modifying what we said in terms of the remedy function and the ability of OPoC to act on that. We're saying that it's -- it will be a path that goes to the registrant -- in some cases, it will need to go to the registrant and failure in terms of responsiveness from the registrant can then lead to direct contact to the registrar by the requester, the OPoC, in that extra path is what I am saying.

>>MILTON MUELLER: Are we just saying straight out there is no remedy function by the OPoC per se?

>>PHILIP SHEPPARD: I think -- yes, certainly as an actor, I think we're basically saying as a relay, the paths go different ways. I think we are saying that because we are saying it appears for some of the more problematic stuff we

don't need to go that route anyway because you can go straight to the registrar or the ISP.

>> Or the host.

>>PHILIP SHEPPARD: Bertrand.

>>BERTRAND DE LA CHAPELLE: In that case, which is an interesting evolution in the discussion, the only question that has to be addressed is the one that was raised before, is should the OPoC be informed of the remedy action that has been taken or not? And under which conditions? In a similar way, under which conditions should the domain name holder be informed of any remedy action?

>>PHILIP SHEPPARD: Registrars, I presume if you are taking a site down, do you bother to tell the registrant that's happening? Do you just wait for them to wake up?

>> Yeah.

[Laughter]

>>PHILIP SHEPPARD: That's what I thought they might do. Okay.

Grand. We probably have done all we can on Item 3 for the moment. Item 4 is a really easy topic and, therefore, best taken this afternoon. Since we only have a few minutes left of this session before we close it anyway, we close it now and convene this afternoon to tackle Item 4. Thank you all very much for your thoughts and cooperation today. I think we made some very good progress.

Thank you.

Maria, explain the next bit of the timetable to all of us.

>>MARIA FARRELL: So the next thing is we will be having a lunch -- a working lunch here with GNSO council members. So there will be food outside within the next ten minutes. And you will all be free to take some lunch because God knows you have worked hard enough to deserve it and mingle with the GNSO Council. It is going to be a working lunch, so I think there will be a little -- it will be a little free forum but ultimately people will get their feed, eat it, mingle a little, come back in and sit down. I think we will probably, Philip, do an update to the council, an informal update, on what we have achieved this morning and there will be some discussion. I think they will be curious about how far we've gotten, where we are. They may just want to prepare a little bit for their discussions with the Government Advisory Committee this afternoon.

So food, mingling and returning to the room and informal updates.

>>PHILIP SHEPPARD: Very good. Thank you very much.

(Lunch break)

AFTERNOON SESSION

>>PHILIP SHEPPARD: Good afternoon, everybody. We are going to start. So please take your seats and end your conversations. We will launch into Item 4 of our agenda in just a second. Before we do that, we will go around the room and those who weren't here in our morning session, perhaps if you could just introduce yourself with name and any affiliation you care to share with us and starting at the far side there.

Mark, you didn't have a chance last time, did you?

>>MARK McFADDEN: Mark McFadden from the ISP constituency.

>>PHILIP SHEPPARD: Who else wasn't here this morning?

>> Wim Degezelle.

>>AMADEU ABRIL i ABRIL: Amadeu Abril i Abril.

>>PHILIP SHEPPARD: Anybody else or was everybody else here?

>>BILL MANNING: Bill Manning, ICANN Nominating Committee.

>>PHILIP SHEPPARD: Other faces who weren't here this morning? Okay. Thank you very much.

So Item 4 is picking up some discussion that has been on one of the subgroups in terms of, perhaps, high volume, repeated access by third parties. I thought it might be useful to discuss a little bit more the conversation that started on the subgroup in terms of determining the right to access to such data, perhaps split between law enforcement agencies and the private sector.

Just to see where we can sort of come out from that, there was some ideas, I think, being floated in the subgroup, not only I think there was some informal discussions I had with government necessarily fly in terms of LEAs.

Perhaps, we can just kick off with some thoughts there and perhaps, to me, the first question would be sort of one of proportionality. We are looking at a world we may be moving for some data which is open to a closed set and then we are looking at how you might grant access of that to the likes of law enforcement.

Perhaps, it would be worth just airing, first, the discussion in terms of the need for verification upfront that's positive as opposed to a system maybe that is more passive in terms of, I think this is a strange requirement, I might ask more questions. Perhaps, anybody who has a reflection on that might be a useful start to verify things.

I have Milton. Anybody else? Okay, Milton, start off.

>>MILTON MUELLER: I'm not starting off on that. I just wanted to make a point about a procedural point about the report. In describing the type of access, you have Type III bulk access, Type II bulk access, Type IV access. The word "bulk" should not be in there. It could be very confusing to retain those words. Type III is described as ongoing query-based or bulk access and all the other forms of access do not involve what we currently think of as bulk access. I think maybe --

>>PHILIP SHEPPARD: yeah, yeah.

>>MILTON MUELLER: (inaudible). It would be very important to change that.

>>PHILIP SHEPPARD: We're talking about options for repeated access rather than bulk.

Back to the original question. Rationale for verification in particular for law enforcement agencies or alternatives for doing that? I mean, one idea we floated was agencies like Interpol, there is some work being done by consultants, reporting back to us in a few weeks, ten days.

>>MARIA FARRELL: Yes.

>>PHILIP SHEPPARD: Which may shed some light there. My understanding is that Interpol is probably well-suited to do that. I also -- the bizarre twist that registrars are expected to be gatekeepers for law enforcement as opposed to the other way around. Perhaps any thoughts on that anybody has? I have got Jon.

>>JON BING: Thank you, Mr. Chairman. It is, of course, a recurring issue, access that law enforcement agencies both national and (inaudible) who have to incorporate different types of services (inaudible). This is a rather broad issue. And I -- my inexperience is shining through. I have difficulty in understanding that this an issue that is resolved on its own in special reference to ICANN and not be part of the general regime of law enforcement's access to traffic data, assimilate data from all types of (inaudible) data systems. (inaudible) to establish (inaudible) convention systems to police corporations which are extensive and a type of system in its own right. (inaudible).

>>PHILIP SHEPPARD: Jon, in other areas, the nature of access is granted essentially on trust. The law enforcement agency is who they say they are. Is that the case, or is it a different system?

>>JON BING: I am certainly not an expert in all countries. But there are (inaudible) in place (inaudible) different laws which also embrace traffic on the Internet which law enforcement agencies are authorized to request data and then they would then have access to data. Apart from (inaudible), there is corresponding the obligation to gain traffic data then, of course, we have the (inaudible) coming in and (inaudible) to traffic data.

Let me point out it is not only mobile telephones and Internet but they're (inaudible) systems (inaudible) which keep track (inaudible). We move on to relationships, we also have a (inaudible).

>>PHILIP SHEPPARD: Thank you. Observations on this? Milton?

>> MILTON MUELLER: The basic observation of making a response to Jon is, yes, there are existing legal procedures for law enforcement agencies to get access to data within the framework of the national institution, and the problem is the global scope of the domain name system.

>>PHILIP SHEPPARD: Okay. I will get a response to that first and then come back to you.

>>JON BING: I'm sure that is right. But there are also at least international systems, for instance, (inaudible) a treaty which is convention (inaudible). And there is a (inaudible) for assisting law enforcement in the context. That has been designed to be appropriate assistance and, of course, in evaluating the provisions of that convention, (inaudible) especially designed with this in mind (inaudible). Thank you.

>>MILTON MUELLER: Just to respond to that, we would be perfectly happy to say, you know -- we have been saying this for, I think, seven years -- we could and should probably be relying on formal conventional -- conventions and negotiations to resolve many of these issues but there are -- there is a point of view that we should work it into the way the DNS operates which is seen perhaps as more quick and reducing the transactions cost involved. But I think you raise a serious issue that we need to consider.

>> ROBERT FLAIM: My name is Robert Flaim from the FBI. I have been an observer on the working group. Unfortunately, I have some of the comments that this gentleman to my right made. As far as law enforcement is concerned, I have been in consultation with Interpol and at this point, it is a little premature to talk about certain engagements with Interpol or other groups because we don't have that in place, putting kind of the cart before the horse at this point.

I can't say we are going to rely on that. If we are going to do anything of that nature, we need to make sure that is in place and make sure that gets done before we go forward with any OPoC proposal or say anyone is going to serve unless we actually have that person or organization that's willing to do that. Right now we don't.

>>PHILIP SHEPPARD: To my knowledge, impersonation of law enforcement is a criminal offense in most countries. Do you have any issues elsewhere in requesting data and a needing to prove who you are, or is this contract unique in the ICANN world?

>> ROBERT FLAIM: The whole problem and the issue with OPoC is the time sensitivity of the information. If you want information that we have to obtain legal process, MLAT was referenced in the document, so on and so forth or in some of the discussion, that's legal process. That could take, you know, months, sometimes years so we are talking about authentication of a law enforcement agency. In certain countries it is very easy, everyone knows who the FBI is, the RCMP, that is very self-evident.

A lot of times you have local law enforcement agencies. You have municipalities. From within the United States itself, I can only refer to the U.S., within the United States itself, and even trying to authenticate those people are very difficult. You are the sheriff from Tuscaloosa County? How do I really know that? Who is that? So on and so forth. That becomes a real issue. In the United States, you have that literally thousands and thousands of law enforcement agencies. So on paper it sounds like a good idea. But in reality in putting that into practice, it would be so, so very difficult. So...

>>PHILIP SHEPPARD: Okay, I have got Mike. Anyone else want to be in the queue? Steve, Dan.

>>MICHAEL PALAGE: Thank you, Philip. Just to follow up on Robert's comments about the complexities of identifying people. In a different context, Afilias

was tasked by the ICANN board to allocate the geographic names who were reserved in ICANN board resolution 01-92 in connection with the Afilias rollout.

One of the problems we had to do was to see who would get certain country names, such as Canada.com. One of the complexities that Afilias ran into was there were multiple agencies within the Canadian government coming forward to say, I want it, I want it, I want it.

What Afilias was able to do was to work with the GAC secretariat to help identify who was the appropriate contact within that country who would be able to act on behalf of that domain name request.

Again, it is kind of something outside the context of WHOIS, but, I think, it at least shows some of the efforts of where ICANN and the GAC in collaboration in trying to identify a single contact or point within a country. So, again, that's just a data point I thought might be helpful in this context.

>>PHILIP SHEPPARD: Steve?

>>STEVE DELBIANCO: Steve Delbianco. Philip, my question is mostly about the document. Maria, you could be helpful on this, too.

Having heard Robert's comment with respect to Interpol, on the bottom of page 12, the report suggests what's been agreed is that global certification mechanisms for an organization status should be explored. We have the words "should be explored" many there. There was a staff note and presumably Robert's comment will make another staff note.

My question is the things in here listed as agreed, do any of the others imply that the LEAs have to be certified or that even private sector has to be certified? Or is certification only brought up to the extent we said it ought to be sort of explored?

>>PHILIP SHEPPARD: Milton, go ahead.

>>MILTON MUELLER: It was agreed that private sector actors should not have unrestricted access, at least under the OPoC paradigm and that, therefore, there would have to be some kind of mechanism for -- as a logical implication of that, there would be some mechanism for handling requests. We talked about self-certification. We talked about some other kind of certification, but we didn't reach any agreement on those mechanisms. So we did talk about certification and other ways of restricting access to the full WHOIS record for private acting.

>>STEVE DELBIANCO: With respect to LEA?

>>MILTON MUELLER: With respect to LEA, again, there was an agreement at the very least nobody disagreed that LEAs should have access of Type I sort. The problem was how to deliver it and that one reason there was less agreement -- or more agreement about that was that people could easily certify that LEAs would be publicly accountable institutions. It would have almost by definition a legitimate reason to be going after that information. Of course, we recognize that LEAs could abuse that privilege as much as a private actor but that, as a categorical distinction, it is almost uniformly the case around the world that LEAs have some kind of right to request information that would normally be private in the conduct of a criminal investigation or any kind of a law-breaking investigation.

>>STEVE DELBIANCO: If I may with a follow-up. In the places where we list our "agreed," mostly on page 12 then, I'm just really trying to understand if there is an implied -- look at line 146, for example, where it is agreed LEAs should be granted access to data elements. Is it implied that that's certified LEAs or self-identified LEAs? Is there any implied certification necessary to support the agreement that we're going to report?

>>MILTON MUELLER: I would say it was implied because of the discussion within the report about this business of using Interpol or some other mechanism to identify WHOIS and LEA. I do think you have to worry about that.

You're right, in the report as it now stands, we should not come out of my subgroup. But as the integrated report, that's an ambiguity.

>>PHILIP SHEPPARD: Which we are now exploring, yeah, exactly. I had Dan first and then Carole and I will come to Jon.

>>DAN KRIMM: Thank you. A few points, first, I think it would be useful to consider whether standards of certification could be different between governmental entities and private entities seeing as, perhaps, private entities would have a higher standard and, perhaps, there may be somewhat less of them and they might be easier to certify.

Secondly, one of the approaches that had been discussed in the subgroup B was the idea that technological tools could be used in order to help streamline a process of access in legitimate cases and, therefore, if there are sort of bureaucratic obstacles, even if the solutions are implemented in the realm of national governmental realm -- public realm, ICANN might provide some of the resources and, perhaps, some sort of standardization of protocol in order to help build systems that enable a more timely response.

>>PHILIP SHEPPARD: Okay. Thank you. Carole?

>> CAROLE BIRD: If you will indulge me. I have a couple of points. I believe the discussion --

>>PHILIP SHEPPARD: Can you speak into the mike. Quite narrow gain on these.

>> CAROLE BIRD: Can you hear me now? Okay. Let's try this again.

>>PHILIP SHEPPARD: I am getting nods from transcription. That he is very good.

>> CAROLE BIRD: With regard to subgroup B when we were talking about law enforcement, specifically we were talking about -- I think you will see in line 143, they were defined as governmental agencies and not just police departments. So the devil in this document is going to be in the details, quite frankly.

It is too easy to look at certain terms and make an assumption that something is included when, in fact, other people are interpreting it to be excluded.

For example, if you look at Type I access in the second line where it says "where we have a registrant is causing problems," if I can go back to the example earlier provided by Steve where he spoke about an innocent party whose Web site now has a botnet (phonetic) attached to it, again your definition of "causing problems" is the person knowingly doing so or not. The devil again could be in the details.

With regards to certification, I'm going to say that the idea that the GAC representative should be able to tell us which agencies within their respective countries fall under the definition in line 143 of a governmental agency legally mandated to investigate and/or prosecute the legal activity, really to me that's what I am looking for from my government representative sitting on the GAC to do, to identify which ones are bona fide governmental agencies that are specified within legislation to having a mandate to investigate illegal activities.

Mr. Flaim from the FBI hit on a very key point in that time is a huge issue for us. We try and react as quickly as we can. Sometimes it is not as quick as our clients would like us to. But turning over information so we can pursue an investigation because people that are committing illegal activities are fast and quite often have resources that exceed our resources, and this isn't a pitch for funding.

[Laughter]

The existing processes, the MLAT processes, even the convention for cyber crime, they're all looking at putting measures in place, but many are not able to react as fast as we need them to react. We're not just talking about what we call crimes against property or crimes for profit. There are, in fact, activities on the Internet that can result in harm to an individual of a physical nature and so time -- the timeliness of accessing information cannot be emphasized enough.

The other issue we have is, is we may well have a situation -- And I spoke to this in subgroup B, but I would like to share it with all of you.

We may well have a situation where something that is occurring is an offense in one country but not an offense in another country. And if the law enforcement agency from one country is unable to get that information but the law enforcement agency from the second country isn't seeing it as a criminal offense because it is not mandated as one in their area, then our ability to get that information and pursue to it is significantly hampered if we don't put measures in place that will allow us to access the data.

And let me give you just a simple example where in Canada, we may have -- we may be trying to find someone who has done a noncustodial abduction, noncustodial parental abduction. In Canada the courts can order us to do an investigation and find the individual. If they are in a country that does not recognize that as an offense, our investigation can be fully hampered.

Now, that looks like not that great an offense but we will see the same thing when it comes to crimes against children of a significantly more damaging nature than that.

So we have to ensure, or at least I am hoping that we can ensure that law enforcement can access the information in such a way that we're not bound by whether the other country agrees that, in fact, it's an offense.

We are just looking at whether the law enforcement after particular country is mandated by its country to do the investigation.

Thank you.

>>PHILIP SHEPPARD: Carole, thank you for that. Just going back to your question on definition, our current rather slim definition in lines 143 and 144 of the report defining public law enforcement agencies as governmental agencies legally mandated to investigate and/or prosecute illegal activity, do you think that's adequate as a working definition?

>>CAROLE BIRD: Yes, from my purposes, and I just want to reiterate here speaking on behalf of the (inaudible), not on the government, governmental agencies for us will cover federal, provincial and municipal law enforcement. And so for the RCMP's purposes, that definition serves our need.

>>PHILIP SHEPPARD: Okay. Everybody else happy with that definition before we take another queue? Okay. That's fine.

I just got Jon to go and then Norbert.

>>JON BING: Thank you. I sympathize very much with the arguments put forward and feel a bit silly by being so formal. But if you look at the sentence in 146 that the law enforcement agency should be grounds for access to data elements not shown in the in the post -- published WHOIS. You find that in my own country, which I happen to know quite well. This data would be under statutory secrecy or retained. It will be confidential in the statutory process. And can be on the day released to a third party when there are statutory grounds to do so or a court order.

And therefore, also, there is statutory provisions which makes some law enforcement agencies able to access this in a very timely fashion.

But it will be -- You could not, by a contract, bind the operator to release such data into orb or to law enforcement agencies of other countries without there being a breach of contract, and actually a crime. And we don't want to do that.

So I think that many of the problems that we encountered is problems over the national world where they haven't been solved. And they are especially transnational and crimes across borders play a much more important role of the Internet.

But it seems to me difficult to solve these grave and pressing problems through these mechanisms. They won't go away.

We need to have better instruments than the contract between ICANN and the different operators to do that.

Thank you.

>>DAN KRIMM: May I ask a question in follow-up?

>>PHILIP SHEPPARD: Yes, Dan. I will come to Norbert after, if I may.

>>DAN KRIMM: Is it the case that data that is currently public in the WHOIS database is accessible in those countries, and the mere fact that privatizing that data would make it inaccessible -- or is it the fact that currently data that might be published currently in WHOIS already violates national laws and must not be accomplished one-third.

>>CAROLE BIRD: If I may, because I think I was the next speaker, it might vary from country to country.

Each of our countries, if I may state it this way, and please feel free to correct me if I have it wrong, each country has reached the point where it either has or is working to strike the balance as per the dictates of its population or its government between privacy right and the law enforcement. If I can use Canada as an example, and I recognize that legislation in Canada is going to be different than it is in other countries, what is currently publicly available on WHOIS databases is information that even if it is shielded can be provided to law enforcement. And I apologize, I know this morning you spoke about credit card information. That's not information that can be provided to law enforcement in Canada without a search warrant. So that's not what we're asking for.

But the currently available WHOIS data, even if shielded, the Canadian legislation, it's called HIKITA (phonetic), it's a long drawn-out thing, that's the acronym, it's permissive and it allows businesses in Canada to provide the information to law enforcement. It uses the terminology "may provide."

Now, just to go back to what Mr. Bing said earlier, at no point am I counseling that we enable someone to commit a offense in their country by providing them information that in doing so violates a privacy law. What I am saying is each country has struck a balance between its privacy and its law enforcement, and we shouldn't be looking at being more restrictive than whatever the countries have already put in place because that's what those countries and that population has developed to meet the needs of that country.

So I'm not sure that we're going to be able to find a one size fits all that's going to meet everybody's needs.

But we should never be counseling someone to give out more information than the law enables them to get. But if they are entitled to it as a law enforcement agency, we hamper them by not providing the information that they are, in fact, legally allowed to get in their countries.

Thank you.

>>PHILIP SHEPPARD: Okay. Let me take Norbert first because you were there before, and I've got Steve and the FBI and Milton Mueller.

>>NORBERT KLEIN: I just wanted to make an observation.

When you made this example from Canada that certain things which are not legal in Canada are legal in other countries, and therefore the problem how to get to this data, I just have to say I live in a different country. I live in Cambodia, and certain data which are not legal in Cambodia are legal in other countries. And I'm quite happy to know that other countries will not have all access to the data which in Cambodia are under certainly control.

I mention this because it is so different from which side you look at the same problem.

Thank you.

>>PHILIP SHEPPARD: Yeah, thank you.

Steve.

>>STEVE METALITZ: Steve Metalitz.

I think part of what we're wrestling with here, which I think distinguishes it from all of the other situations that Professor Bing referred to, is that right now the status quo is that this information is publicly accessible.

So -- And we're talking about moving to a regime in which some of it is no longer publicly accessible.

The question isn't whether it's legal or not legal in a particular country to publish it. The question we need to focus on is, is it legal or not legal in a particular country for law enforcement to access it.

If it's publicly accessible now, if a country has a law that says that law enforcement can't go to a publicly accessible database and access this information, or can't do that for certain purposes, then obviously the law enforcement in that country has to obey that law.

But I would suspect that in most countries -- well, I won't say that. But certainly in some countries, if it is publicly accessible to anybody, which is the status quo, then it would also be publicly accessible to law enforcement.

So we're talking about a situation in which something which is always -- in those countries which has always been accessible to law enforcement would become inaccessible to them except under certain conditions.

But that makes it -- That's why this, I think, becomes so much more difficult.

It's not like traffic data, which is not publicly accessible. And maybe accessible to law enforcement under certain circumstances, but this data is quite different.

>>PHILIP SHEPPARD: Thank you, Steve.

Milton and then Robert.

>>MILTON MUELLER: Yeah, again, I think we have to be very careful about circumscribing the context in which we are discussing these issues.

We all know that ICANN was set up to be a global regime for handling various kinds of policy issues associated with DNS. And that's its advantage.

And so whatever ICANN does is going to be global.

What we have come to an agreement on, I thought, in the subgroup, Carole, was that we all agree that we understand the need for law enforcement to get access to certain kinds of data quickly and efficiently, and we are just trying to figure out a way to do it.

But you have to also recognize that the status quo is not something that we can continue. That it is, in fact, against the law, as Jon keeps reminding us, in certain countries for this information to be public.

And therefore, it is relatively easy to grant access to information that is shielded than it is to -- You can't retract the information once its public. You just can't do that.

So it's an issue of defining what our policy is to make this information accessible to law enforcement.

Now, the other point I want to make, when Carole talks about getting access to the information, I want to question that word, "the information." Let's be very clear what we are talking about here.

All we are talking about being shielded is the street address, e-mail address, and the telephone number of the registrant.

Okay. All the other information is going to be there. And for many, many, many law enforcement purposes, particularly those requiring rapid action, that information will be sufficient.

Now, if you want to track somebody down after you have taken a Web site off, that doesn't take such rapid action.

I mean, maybe it will and maybe it won't, but that's a question of pragmatics.

And again, when you want to talk about child abduction and those kinds of things, you aren't going to solve child abduction cases by having the e-mail address of a domain registrant.

So we are talking about a much narrower class of crimes and activities that have to do with the actual use of the Internet to commit crimes, and that's when the rapid access becomes essential.

So the intent of the report was, again, to basically agree that there's a need there, and that we have to figure out whether we meet that need by providing Type I access or Type II access or even Type III access in the case of law enforcement.

That's what we should be debating. We should be figuring out how to make this work, not whether we should do it, in my opinion, at this stage.

>>PHILIP SHEPPARD: Thank you, Milton.

Just one clarification. I thought based on our clarification this morning about admin and tech and how to obtain admin and tech in terms of collection, am I right in saying that on the OPoC, unless we make a proposal differently, the shielded data is, in fact, including all of admin, all of tech, and elements of registrant. Margie is nodding. Does everybody agree with that as the implication of what we said this morning? Because that's different to what I think we may have had in wording previously.

Steve, did you want to say something on this specifically? No.

I'll come to Robert.

>>ROB FLAIM: Okay.

I just wanted to kind of address what Dan was saying earlier. People are saying that this is -- the current WHOIS or current system is in contravention of some of the privacy laws. To date, there has been no case law. I mean, it's been brought up in GNSO council meetings before, public forums. I know people have asked the question point-blank, which country it's -- the laws of violating, and nothing has been brought forth in any country where the government has brought an action against a registrar for publishing data that was against the privacy laws.

If you recall, I don't know if any of you were there, but a couple of years ago we did have law enforcement representatives from various countries that do have the data privacy laws in Europe -- namely, Spain, the United Kingdom, we had Australia there, we even have Interpol there -- and again, their privacy laws, the way I understand them, are more stringent than the American laws, which I am familiar with. And they all seemed to agree with whatever is on the WHOIS now in its current form is acceptable, it's been in use, it hasn't been against any privacy laws that they are aware of or they aren't breaking any laws at that point.

And if there are privacy laws being broken, I think a case needs to be pointed out, there needs to be a lawsuit, there needs to be something. Because as of right now, I don't see that -- you know, I'm going to have to totally disagree that there has to be an OPoC. I think the current system right now, unless we can come up with a good, viable alternative, I mean I think, you know, solving a disaster by creating a catastrophe is not the solution at this point.

I think unless we have a fail-safe method of coming up with something better, with I don't think it behooves us to come up with something that we know won't work.

>>PHILIP SHEPPARD: Okay. I've got Amadeu to speak. Amadeu, you need a microphone.

And then Jeff.

>>AMADEU ABRIL i ABRIL: Thanks a lot.

Regarding the absence of K {?} laws and actual focus in that, are you willing to sign a check to pay for the fines in case they arrive?

I'll tell you a story. I don't work for dot cat anymore, but I am inviting them on this WHOIS issue because in the contrary, we try to set up different WHOIS provisions and we are negotiating that now on the forum.

The situation with local protection agencies is wait and see. But they don't even want the name of the individual registrants being published.

And we think it's better to solve that before we get a formal fine, instead of, you know, putting the corpses on the table, that apparently is what -- you know, I can stop and other people seem to prefer as a solution; right? First get fired or go to jail and then come here and we will think about a solution.

Thinking preventive, it's a good solution sometimes.

And they clearly disagree with the current state of the WHOIS.

The rule should be made for the rule and exceptions treated as exceptions. What is the statistical situation outside of the U.S. and dot com and net and perhaps info and biz? Think, for instance, what dot fr has done and dot cat did something very similar, which is the registry is, in fact, the default contact for all those individuals that opt for not publishing the personal data. They have the right to make that publicly available, and if they decide that, that's perfect. But the law requires that they opt in in that public available source or choose not to publish the data.

If they choose not to, explicitly choose not to, then the registry is the contact point; right? And the request will be sent to the registry by e-mail, in a Web form, and the registry will make the contact with the party, the party will respond or not and we will have it that way.

Then it will be individual access for law enforcement entities.

And in cases that (inaudible) reasonable happy to tell law enforcement will immediately sent this information in case there are doubts. The local contact point will be contacted to see whether they can help or not. And we know it's not a complete certification, but we will try to do the best on that.

In case of doubt, probably the data will be sent. There's some formality there. And always in less than in 48 hours. Probably in 24 hours.

Now, do you know how many times law enforcement asks for gathering the personal data in dot FR since they change it? Do you know how many people have used the Web form for contacting the illegal registrants? Between zero and one. Okay? That's the official data provided by the French registry.

You know how many times the dot cat registry has been contacted for getting the personal data of the registrants? Today, dot cat is not publishing and we are not in compliance with active norms willingly. Zero. Between zero and zero. That's the official data.

So let's take into account that this problem is not always a global problem for all TLDs and all law enforcement agencies.

And therefore, perhaps we could have some more imaginative solutions for places where there is really no problem.

>>PHILIP SHEPPARD: Amadeu, thank you very much.

This work group is always open to imaginative solutions, not just questions.

Jeff, you are next to speak.

>>JEFF NEUMAN: Yes, I guess to kind of dovetail on that, to make the assumption that just because there's been no action taken that what exists today must be in accordance or compliance with the laws, I think there's a pending request by the registry Telnic to modify their WHOIS policy based on conversations that they have had with the UK commissioner on privacy. And I may be stating the person wrong. I know we have representatives of Telnic at the meetings here, and possibly we could talk to them, if we want.

But I do believe that they are making the allegation that the current system that they are supposed to launch with as approved in their ICANN agreement is not in compliance with the UK data protection laws.

>>PHILIP SHEPPARD: Okay. I've got Carole next and is that Steve also?

All right.

>>CAROLE BIRD: I am going to digress a little bit from that, and I'm sure that Steve and Robert will come back to it.

Actually, Milton, I'm in agreement with you, which frightens me.

[Laughter]

>>CAROLE BIRD: In fact, in subgroup B we had come to an agreement with regards to the fact that in the context of the OPoC, when we are looking at what type of access can be granted should OPoC be implemented that there were a number of different accesses. And in fact I thought that's what I was debating is the different accesses and why we need the different accesses.

But I don't think we have gotten to that level of detail when we talk about the need to access data. Because I see the differences between Type I, Type II, and

Type III, and I know in our discussion although we said at the very least law enforcement should be granted Type I access, they used the words "at least." Because there were a lot of discussions whether that should be Type I, Type II, Type III, or Type IV. Because there were support for others, and there were some alternative views, and I could see there is some real debate here as to whether or not the overall workers as a whole has an agreement on a Type I, Type II, Type III, or Type IV. And that's where I thought the debate would actually occur.

>>PHILIP SHEPPARD: Carole, quickly in response, on Type I access, which is the sort of one to one, one domain query type access, it's perhaps probably an open question to the board at the moment as to whether or not that's sort of rolled into the reveal function in terms of those discussions. And therefore the working assumption is yes. It's requested to anybody making a certain set of assertions, because typically it's an assertion of harm and the -- it's different in terms of the access and the privacy to repeated requests or type of database.

>>CAROLE BIRD: Correct me if I have misunderstood, and perhaps I am misunderstanding.

In Type I, we were talking about law enforcement having access to the data but not requesting same directly through the OPoC.

And I have a concern if any data request has to go through the OPoC because I'm not convinced that given how complex organized crime has gotten, that organized crime won't be able to set up its own OPoC, and every time we have to make a request, if that's what's being proposed, that that -- that the fact that we're doing an investigation into an organization that is that complex won't then be revealed in the investigation be jeopardized.

Have I misunderstood the point there, Philip?

>>PHILIP SHEPPARD: Okay. So you are talking about the cases where you have an investigation and you wish to have discreet access to the data without alerting the registrant.

>>CAROLE BIRD: Without alerting someone who may be too close to the registrant or the registrant. Well, certainly the registrant.

But there's no way --

>>PHILIP SHEPPARD: And certainly at the moment the OPoC is rather close to the registrant because it's already been said it's got to be an agent of the registrant.

>>CAROLE BIRD: Absolutely. And I recognize not in all cases will the OPoC be close to the registrant, but we have some very wily people there that are bad actors, and anytime an opportunity presents itself, and some of them are very organized and very complex, they are certainly able to identify themselves as an OPoC or coordinating body that has the same illegal interest. And if we have to request the information from an OPoC, that investigation will be revealed at a time where it may jeopardize the investigation.

>>PHILIP SHEPPARD: Okay. That's useful clarification and probably answers questions one through three in the report.

Next in the queue is Steve.

>>STEVE METALITZ:Steve Metalitz many.

Just to note in regards to the murky question as to whether the status quo is illegal in any country.

This issue was foreseen by this body, the GNSO council and the WHOIS task force, several years ago, and unanimously we passed, the GNSO council unanimously passed, the board unanimously passed a policy statement for establishing a procedure to bring greater transparency to any such conflict situation that might arise and to try to have a path to resolution for that. And so I think that issue is being addressed elsewhere.

>>PHILIP SHEPPARD: Thank you. Robert.

>>ROB FLAIM: I just wanted to respond to a few of the comments.

Obviously as a representative, I am speaking for myself, of the FBI, we would obviously never advocate to going in contravention to any laws.

My whole point is we are constantly talking about these privacy laws but yet I have seen no documentation as to what exactly the laws are.

Obviously if you have a car with no brakes you are not going to say step on the gas and let's head toward the brick wall and we will make sure the car has no brakes.

No. What I am saying is if we are going to rely on this data that people are saying we are relying on, then I think we should actually see it, meaning the national laws.

And in response to referring to the UK law and Telnic and stuff like that, according to what I read it was an informal discussion with that commissioner.

So again, I would just like to narrow in on the specificity of what these laws are and what exactly we are referring to.

>>PHILIP SHEPPARD: Okay.

Scott, and then Milton and then Jeff.

>>SCOTT VOWELS: So one of the things that appears that we may be doing, just in regard to the policies and procedures that we're setting up, is setting up a situation where people can get access to data after something bad has happened.

One of the things that we're trying to do, and I think it's important that we maintain, and that everybody maintenance, the ability to be able to do this, to try to analyze data prior to something bad happening.

What you guys are doing is hey, we could get access to the registration information after a crime has been committed.

One of the things we will often experience is we will see five or ten domain names registered by the same registrant. One of them turns into a phishing site and we want to quickly get access to information to be able to contact folks to tell them, hey, we have suspicion that these others, that the same thing is going to happen. And oftentimes it will.

So access to that information in that in between, to be able to prevent these bad things from happening, I think that's very important.

And the other thing, just to reiterate, and I don't know whether I'm the lone voice in here, just in regard to the registrars, but we'll also see a common theme with the registrars again and again allowing what is quite obviously bad data being entered into the registration data.

And I think they again need to be held accountable for that.

And there's got to be good stats on the companies that are doing that. And they should be held accountable.

And I still have -- I asked a little bit earlier, how many registrars have actually had their -- whatever, their license to do business pulled based on enabling fraud? Has anybody analyzed that, even know what that looks like? Zero?

>>JAY WESTERDAL: They don't get paid to verify data.

>>SCOTT VOWELS: So they are being paid to enable fraud, then?

>>PHILIP SHEPPARD: We need the conversation through the microphone.

>>JAY WESTERDAL: Just from a registrar perspective, since I am one, that if you enable a person to provide a domain name, there is no cost built into the process where you say well, fax me your identification, fax me where you live, fax me your identity. That's not in the process.

>>SCOTT VOWELS: Maybe it should be.

>> Maybe it should be.

>>AVRI DORIA: Can I ask a clarifying?

>>PHILIP SHEPPARD: On that issue?

>>AVRI DORIA: Yes. I want to make sure I understood the statement that was made correctly. And I understood it to be said that there was a necessity to have access to personal data because one needs to go through it to decide whether someone may be about to commit a crime with it.

Is that -- I mean, basically, that you need the data so that you can check, because there's a possibility that something will tell you that I am about to commit a crime.

>>SCOTT VOWELS:Well, yeah. What we will often look at is iterations of our company name, Kompany.com swelled with a K, spelled with two K's, spelled with two Y's on the end, et cetera. And we will submit cease and desist, stop using versions of our name.

And so yeah, we definitely do send those things out. And what possible use could there be of registering my name misspelled or with three S's. Does that sound like me?

>>AVRI DORIA: It sounds to me like fishing with an "F" instead of P-H, but yes.

>>PHILIP SHEPPARD: Milton, you are next on the list.

>>MILTON MUELLER: Yeah, I think that's the issue we are talking about, is the people who want to, in fact, have the full run of the data to basically do data mining.

Basically people who have purposes, legitimate purposes, whether law enforcement or private to mine that data.

A couple of comments about, again, this issue of the legality. I think there was a letter sent to Vint Cerf by the Article 29 working group of the European Union which clearly spells out the legal concerns. To say that the UK case is based on discussions is a bit disingenuous, because any -- any business in their right mind and any law enforcement entity in their right mind is going to avoid litigation if they can.

So they are not going to say, "Oh, go out there and do something illegal, and then we'll prosecute you."

They are going to go into discussions and they are going to avoid getting into trouble.

So that's clearly what happened in the UK case.

And then there's the fact that, which seems to be being ignored here, is that the country codes themselves, particularly Canada and certain others including the Dutch, do restrict WHOIS data in ways that are consonant with their national law. So I don't think there's any doubt about the conflict.

The fact that we -- somebody hasn't raised enough money to conduct a lawsuit to sue one of the registries or registrars yet is something we should perhaps be grateful, or not, for depending on your appetite for conflict.

Let me just call your attention in a more constructive manner to one of the options mentioned in the draft report, and Type II access. It is basically the status quo with accountability. In other words, it says, perhaps, to law enforcement agencies, you have the full run of the data but there is some kind of accountability mechanism in place that would reveal whether you are abusing that or not. And I think this is just normal sort of good practice in law enforcement.

We say, for example, the FBI has its own accountability checks and balances and, for example,, recently, there was a discovery that the FBI itself released that some of its access to data had been abused by agents.

So that's all we're talking about when we talk about Type II access. It is not simply everything is published so that not only you but any identity thief in the world can get access to it. We are talking about let's find some way to keep track of what people do with this data in a way that would provide some accountability but let's also find a way to give law enforcement agencies the full run of it when they needed to do an investigation.

And the implementation of the issue are not trivial but it is not dealing with policy now but leave the implementation to other people.

I think if we focus more again on the constructive issue of how do we deliver a kind of access that's consistent with legal privacy protections, we will get a lot farther rather than questioning the need for any change.

>>PHILIP SHEPPARD: Just a time check. We have got about 30 minutes of this group to go and I would like to get on to the even easier subject of private sector access and have that suggestion shortly. Perhaps, if you can wrap the discussion the current queue which is Jeff, Shaundra, Dan and Carole and my attempt to sum up the agreement we have around the room.

>>JEFF NEUMAN: In the risk of not being constructive, going back a step. Just to clarify the record, there was a procedure developed to handle conflicts with nation's laws. In fact, I think I was the chair of the task force at that time. It seems like a long time ago.

I initially -- when we drafted it, I thought that would be the appropriate place. But according to ICANN's May 11 announcement in which the Telnic proposal came out, they basically said since there is no pending enforcement action against Telnic, this is not a situation that would trigger that process.

I think it doesn't apply in that case, although I don't know -- maybe Patrick is looking at me but so maybe he can clarify.

>>PHILIP SHEPPARD: Let's not dive too much into the detail of Telnic. I think it is probably worth what we are saying, that is that, Telnic is taking a particular stance being based in the European Union which is different to what is the basic European Union so there is uncertainty as to the root as a means that we should take -- as following whether or not they are doing something that is for themselves, the sound thing to do or not.

>> SHAUNDRA WATSON: I work with the U.S. Trade Commission.

>>PHILIP SHEPPARD: You need to be close to the microphone, I'm afraid, Shaundra.

>> SHAUNDRA WATSON: Can you hear me now? I was actually just going to echo something that Carole had said earlier with regard to the type of access that we had provided for law enforcement agencies. I wholeheartedly agree that Type I access would not work because we absolutely would not want to basically give a red flag to the registrant's designee, which is the OPoC, that we are actually looking at that target and with regard to Type II access which is better. I feel it is problematic with regard to implementation because basically there is a disclosure of a non-public investigation or of a target if there is going to be record keeping or auditing requirements that are imposed. I think in the report it just refers to unless there is a national security investigation, but I think that there are other investigations that are sensitive and confidential that don't rise to the level of national security that we would be concerned about.

>>PHILIP SHEPPARD: Dan.

>>DAN KRIMM: A few quick clarifications. With Scott's response to preventive queries, we talked about defining the nature of a single registrant. Certainly, if a single registrant has caused a crime, created it a crime, criminally, whatever, against one domain, it might legitimately open up a query into the rest of their domains but that's not the same thing as sort of phishing generally for domains that might have some sort of pattern to them.

Then just a few comments on the Type I and Type II. I think when we were discussing Type I in the subgroup, we were not considering these requests going through the OPoC at all. They were going directly, I think, to the registrar, so the idea of having an OPoC in a reveal is sort of an alternative pathway that we just hadn't considered.

For Type II, I don't think we necessarily considered that the audit trail would be public. It would be subject to due process as well. In other words, we are not saying the audit trail would be -- anyone can go in and -- there needs to be some sort of oversight of that.

>>PHILIP SHEPPARD: Okay. So it is merely a record-keeping function until such time as there is due process to access the record.

>>DAN KRIMM: Yeah.

>>PHILIP SHEPPARD: Okay. Who is next? Carole?

>>CAROLE BIRD: So I am just going to continue on that line. You're absolutely right. With regards to the audit/record-keeping, if my memory serves, the issue that was raised there is there will be some strong concerns or I will have some strong concerns depending on who does the auditing and the record keeping.

In other words, currently in Canada for the RCMP, there are certain systems that we self-audit and have to report back on. There are other systems where, if you will, the office of our Privacy Commissioner can come in and do the audit and there's a number of different audit groups.

So to me this is one of those issues where the devil again could be in the details, depending on who does the audit and who does the record keeping, will depend on whether or not this is an option that can be supported. Certainly for me, for what I do in law enforcement, I'm quite comfortable if the government of Canada identifies who needs to be the auditing on the RCMP.

However, that is not necessarily the case in every country. And so while we've said there needs to be an auditing and record-keeping function, how that is fleshed out, if you will pardon the expression, is really going to have an impact on whether or not this is an option that can be truly feasible and supported by multiple law enforcement agencies. That's my thoughts.

>>PHILIP SHEPPARD: Thank you. Just on this idea about Type II access and the record keeping and auditing, did the registrars make any comment during discussion on that in the subgroup? Is that something you are looking forward to doing or look at with horror?

>>MARGIE MILAM: I'm sorry?

>>PHILIP SHEPPARD: The concept of having to have some record keeping, auditing of access queries that you might be required to follow due process to give out. Is that something that you are -- that's easy to do and is acceptable or is it something you would oppose?

>>MARGIE MILAM: I don't really know. We can talk about it at our registrar constituency meeting. I have a feeling it is probably pretty burdensome, but I would want to talk to the group.

>>PHILIP SHEPPARD: That would be easy to know, I think. Jon, instant feeling?

>>JON NEVETT: I don't think we would be going out on a limb to say it would be burdensome and of concern to registrars.

>>PHILIP SHEPPARD: Okay.

>>DAN KRIMM: One follow-up. I don't think we considered that the registrars would necessarily do the record keeping here, but there might be a system developed within public sector to do that under the authority of the public sector.

>>PHILIP SHEPPARD: Who?

>>MILTON MUELLER: (inaudible).

>>PHILIP SHEPPARD: Okay. Let's move on to the private sector. Where we are on that in our discussions -- Bertrand, quickly.

>>BERTRAND DE LA CHAPELLE: Sorry. Just one quick point on the last exchange, I think the notion noted on record keeping function is very interesting. And following up on what Milton said, the distinction between policy and implementation, there are actually different levels. There can be an agreement that there should be records kept or a log kept of those requests as a principle.

Second, there could be another layer saying that any agency doing that kind of thing should keep the record under mechanisms that are established at a national level.

Third, maybe -- if this is agreed, possibly give out third-party neutral copy of that log for any kind of further control, could be entered. I am exploring the theoretical potential, the three possibilities. One is the principle of the record keeping. The second one is that agencies doing such queries should be keeping something that can be audited.

And the third layer is any other possibility of monitoring under any other circumstance that could be used as part of this log or access to this log in certain circumstances. I think if we distinguish the three layers, we're okay at that stage.

>>PHILIP SHEPPARD: I would certainly sense the agency themselves would be the ones doing the record keeping because they presumably have to anyway rather than imposing that upon registrars. Would that make sense, agencies?

>>CAROLE BIRD: Certainly within our agency, that's something that we would look at. But, again, how cumbersome that would be and what would be required, those are the parts of the implementation that have to be looked at to see if it is truly feasible.

>>PHILIP SHEPPARD: Where we are on that so far, I think we're certainly on one question -- the report on Type I access is the same as the reveal function of OPoC. The answer seems to be a universal no on that because this isn't a function of OPoC, it is going directly to registrars. On the other issues, no change in terms of the desirability of LEAs wanting access. No resolution in terms of how any verification system might be done there. Recognition that the ideas floated so far for verification are probably not flyers. And I think we have to wait to see if there is any light shed of the work of the consultant in ten days' time and revisit that question.

But the working assumption may be that we will need to have a system that is not verified by a third party until we see something that we can actually see as something that is actually -- that can function pragmatically.

Private sector, would it be any different in terms of a lot of what we discussed properly sort of no in terms of the mechanics? Just get to the question in terms of that same issue of verification in which case you are either looking at some sort of external body or the other concepts I think were floated in the group which was a self-certification based on alleged checklist of allegations and why we need this -- why I as this type of organization need that data. Presumably, subject to a challenge mechanism from the registrar to say, Well, wait a minute, that seems a bit odd for whatever reason.

Thoughts on where we go with that? I think the subgroup didn't make any particular headway on those discussions. Is that right, Milton?

>>MILTON MUELLER: Right. The problem with private actors is that, with law enforcement, most of us feel comfortable with the presumption that the need is legitimate and then having an accountability that would say when that has been abused.

With private actors, it is hard to make the assumption that access is legitimate. Some private actors are abusers of data we're looking for. We're looking to prevent from having access. Obviously some private actors are perfectly legitimate in their efforts to gain access to the information.

So it is hard to make a categorical presumption. That means you have to make some kind of filtering process for the requests. And if that filtering process is case-by-case and very case specific, then it becomes too slow for everybody. And if it is not case by case or case specific, then it becomes too indiscriminate for people. That's the conundrum.

>>PHILIP SHEPPARD: Reflections on the conundrum?

>>DAN KRIMM: One suggestion that was brought up in the subgroup was that this certification process could be split into a sort of a broad categorically -- not categorically oriented but a broad eligibility to make queries and then case-specific queries so that you do -- you don't have to recertify from the top down for each case. You basically make a case that you are a kind of entity that would generally need to be able to make queries from time to time.

And then when you make your queries, you provide the case-specific information in that context.

>>PHILIP SHEPPARD: Okay. That could be done essentially from whoever that entity is to each registrar, that's agreed. You're on the list and then you have (inaudible). That sort of broad outline idea?

>>DAN KRIMM: I think also the idea had been in the case of private actors, private sector, that the governmental agencies would be the gatekeeper for that access and then the agency's own access would be used and, therefore, you wouldn't burden the registrar with that process.

>>PHILIP SHEPPARD: I thought we had kickback from the agencies saying that was a problem in terms of what they're able to do. Was that not correct?

>>CAROLE BIRD: If I can speak to that, Philip. Yes. We checked with our privacy experts and although -- it will significantly -- well, it will depend on whether the law enforcement agency actually has, at least in Canada, an active criminal investigation going on requiring the data to be accessed to begin with. If, in fact, I am doing -- am not doing a criminal investigation, somebody else asks me to do a query, I'm not necessarily legally allowed to provide that information to the private sector. And so that option then would not be viable in terms of providing access to the private sector because I wouldn't be allowed to give them the information. That takes us back, I think, if I can just finish this one off, to the last point on the law enforcement -- on the access Type II when we were talking about record keeping and auditing.

Philip, you asked if you expected the agency to do the record keeping. While that's certainly an option and it may well be the best option, the other option is to allow the government itself to determine who should be doing the overall record keeping for that country.

I think that option still has to be on the table and would be one that we would probably put forward -- not "we" would put forward but would be something that the GAC would be a good group to provide advice on.

>>PHILIP SHEPPARD: I had Steve wanted to say something. Anybody else in the queue? Lots of them. Palmer, Steve Delbianco, Margie. Okay. Steve?

>>STEVE METALITZ: I would just say with regard to Subgroup B, I think Milton has summarized the conundrum well. You can also look at it a slightly different overlay which is there are some private sector entities with legitimate needs for access to this data that are in heavily regulated sectors and might be feasible to have a government agency certify in some way what their access would be -- what their level of access would be. Indeed, there was a proposal along those lines I'm sure Palmer will speak to. But I didn't command agreement within the subgroups certainly.

There is also a lot of other actors that have legitimate needs for access that are listed in the GAC principles as among those that have these legitimate needs, and they are not heavily regulated by a particular agency. There is really no one that you can go to in government to be a gatekeeper, no one you can really even go to in the private sector feasibly to be the gatekeeper.

That's where, I think, the logic sort of dictates some type of self certification process and you can talk about the record keeping or auditing functions or what would be the remedies for abuse which obviously could occur in that set.

But I think among the private sector world, you can divide into two rather unequal halves. There is a small group where there is a government agency that takes care of those entities but the vast majority of the legitimate data seekers, if you will, aren't really in that category.

>>PHILIP SHEPPARD: Palmer.

>>PALMER HAMILTON: I'm Palmer Hamilton. Dan's reference a moment ago was to a proposal that we had made, and I don't think we would advance it as a panacea as Steve noted. It does deal with a particular sector. The notion was that banks, by their nature, are in business not simply of protecting their own interest but protecting the interest of third parties and through preventing identity theft, other forms of abuse over the Internet.

And that they need immediate access because of the danger to the consumer. And the notion was that through -- if they were governmentally charted banks, they could be certified as such by their primary regulator so it would be a universe that could be easily defined and identified.

Furthermore, some ideas that Dan had during our subgroup considerations we adopted as part of the proposal, which would have provided that not only would the regulator certify access, that the access to the data would be through the regulator and there would be an audit trail where the information and the reason why the information was sought would be kept so that there could be an after-the-fact determination to make sure there was no abuse by the bank of that information.

As to Carole's point a moment ago about approval, I think that's exactly right. I think in each case, you would have to look at the national law to determine the authority of the bank regulator to perform that function and it would be up to the banks in that country to convince their regulators they had the authority. If they lacked the authority to obtain it through legislation, if necessary.

That was the notion, I think, Dan was alluding to.

>>PHILIP SHEPPARD: Okay. So I suppose the concept of self-certification per registrar in the private sector which had been a dialogue between the private sector and the registrar to have ongoing multiple access. Within the scope of that, be open to certain sectors to have, if you like, a fast track of doing that by saying, We're certified by this external gatekeeper authority, so the job of that dialogue in terms of registrar will be happy with that is easy. They can say, Fine, that's okay.

>>PALMER HAMILTON: Philip, I think we went further even and said that the inquiry by the banks, first National Bank of anywhere would be through the (inaudible) controller of the currency to the registrar. The registrar would be dealing with the regulator.

>>PHILIP SHEPPARD: With the regulator each time, okay. Steve, go ahead.

>>STEVE DELBIANCO: Thank you, Philip. The document that we're working on in trying to clarify and achieve the consensus currently says that there is agreement of the entire working group on page 13 -- that there is agreement that the private sector does not get Type III. Private sector would not get Type III. And earlier Milton cleared up a typo, I think, with respect to what Type III is on page 10. The document you all have in front of you says Type III is Type III bulk access. And then the description indicates query-based or bulk. And, Milton, I think you clarified that the word "bulk" shouldn't have been in the title.

Given that fix, does that alter the understanding of anyone here with respect to the level of agreement we have that the private sector loses Type III access? I would put that question to some of the private sector, particularly trademark or anti-phishing groups here, is that do we still have agreement in this working group that you don't have query-based one-record access anymore that doesn't have to get precleared or prechallenged in some way? It is really a procedural question given the fix to the title. Do we still have agreement in here to that?

>>MILTON MUELLER: It is not that you don't get query-based access. It is that you don't get open access making any query of any domain for any reason. You would still have query-based access under Type I, for instance.

>>STEVE DELBIANCO: It is subject to screening or approval clearing, so it is not unimpeded. Do we still have agreement that the private sector loses unimpeded access?

>>MARGIE MILAM: I certainly don't agree.

>> No.

>>MARGIE MILAM: I was in the queue anyway. In looking at these agreements and statements in the report, I am a little concerned about limiting private access

to that information and, particularly, I come from the perspective of a service provider that provides a lot of reports to the kind of entities like Scott's company and people fighting phishing and anti-trademark infringement. It is a little simplistic to say you have one-up lookups with the registrar because the way you access the information, you get very limited information. You can only look up the domain name, and you can't do multiple queries and look at different levels such as the e-mail address or the phone number.

And so companies like Markmonitor, we are certainly not the only one, there are a lot of companies that have bulk access under the current regime to be able to filter that information, to provide information to companies like banks and other parties so they can focus their search and identify the person that is either violating the law or violating their rights.

I really have a strong opposition to limiting that kind of access. Right now we have access under the current regime because we agree that we are not going to use that information improperly and currently that means you will not use it for marketing purposes and anti-spam. And there is also the bulk access agreement provisions into the current ICANN agreements where there is further restrictions that can be put into it. But to just say outright that should be prohibited is a problem.

>>PHILIP SHEPPARD: Was it understood in the discussion in the group that in a post-OPoC world, Type III access would mean access to full records for legal entity it is and shielded records for private persons? Is that the working assumption you have? Or was it there was full access to everything?

>>MILTON MUELLER: The reason I was agreed, we know perfectly well that the private -- a lot of the private parties on the working group prefer the status quo to OPoC. The question was if you are going to go down the record of doing OPoC, it makes absolutely no sense to give private parties what we know of now is Type III access. Why bother to implement OPoC if you are going to basically let anybody drive a truck through it. That's the logic.

So you have to limit access to the shielded data which, again, as Philip reminded us, only applies to natural persons now, not necessarily corporations.

>>MARGIE MILAM: May I respond?

>>MILTON MUELLER: What's the point of having the OPoC?

>>MARGIE MILAM: I understand we are talking about private persons, but private persons can violate laws and can infringe on people's rights.

There may be situations where you have to go beyond the OPoC to get that information and even in the OPoC environment, you can put restrictions -- I am not saying unrestricted access. I am saying you could have contractual obligations as to what you do with that information.

So I'm not willing, at this point, to rule out bulk access. I am just saying if you have bulk access, perhaps you have an additional burden of complying with certain requirements and you can specify what those requirements are.

>>MILTON MUELLER: That becomes Type II.

>>PHILIP SHEPPARD: I want to be clear on the definition of terms. You could imagine you would continue with bulk access of the current data set which would be a mix depending on the nature of the registrant of shielded and unshielded data. That could continue -- that's irrelevant almost to the OPoC discussions. You can getting access to the shielded data as well.

The separate question is access to the shielded elements. And to my mind there is no -- it is almost out of scope of this group to deny that first, or was that distinction already discussed by the subgroup? Or were you assuming the Type III access is the shielded elements unshielded?

>>MILTON MUELLER: With respect to the unshielded OPoC, under an OPoC system that only applies to natural persons, everything remains the same for legal persons. Nothing changes.

>>PHILIP SHEPPARD: Yep. Okay. I got Steve Metalitz.

>>STEVE METALITZ: Thank you. I think the problem here is that perhaps when Steve Delbianco read this out he didn't give enough emphasis to the first phrase which is well within the constraints of the OPoC proposal." I am looking at line 180. Type III access is defined -- I am taking out the word" bulk ," I think we agreed. Type III access is defined in the box after line 130 as to the current status quo. And all this says is if you -- if you go to OPoC, you are changing the status quo. So Milton is correct, we insisted that this have that first phrase," within the constraints of the OPoC proposal "because I think the first proposal was agreed that private actors should not be granted Type III access.

We feel strongly private actors should be granted Type III access. But we recognize that if the OPoC proposal were to be implemented, that private actors would no longer have Type III access. Public would no longer have Type III access.

So it may be something of a tautological statement but that's the extent of it. It doesn't say that the group recommended that we do away with Type III access.

On the other point about whether we took into account what subgroup C came out with versus natural versus legal persons, I think we didn't. I think all the three subgroups were working independently and so I'm not sure we assumed that there would be that distinction made. If that distinction were made, I don't think it would change things substantially. But obviously for the legal persons registrations, we would have Type III access.

>>PHILIP SHEPPARD: Steve Delbianco.

>>STEVE DELBIANCO: I would just ask for a clarification. The abuses that we -- this is probably something a lot of you have been over many times. The abuses we seek to remedy with OPoC, as you said the reason we're here, do they prior may have to do with harvesting and did the harvesting occur with what's known here as Type III access?

>>MILTON MUELLER: Yes. That's a yes.

>>PHILIP SHEPPARD: Bertrand.

>>BERTRAND DE LA CHAPELLE: I would like to focus on the notion that raised some concern but it is important is the preventive type of access. In addressing this, I would like to take one step backwards and say this discussion right at this point, the question of bulk access and the fact that a lot of actors are actually losing it through the OPoC is probably one of the reasons of the protractive work of the whole discussion on WHOIS because there is a whole category of actors who has absolutely no benefit to gain whatsoever in the implementation of OPoC. All they get is lose. And it is not very conducive to moving forward.

The reason why I raise this is that I'm not sure we are addressing all the potential of the data that is collected for the kind of users and preventive users that can be done to avoid, for instance, cyber squatting and a certain number of things.

In the various discussions I've had with people, I was hearing repetitively the notion of pattern, pattern analysis, looking at whether something is recurrent. It can be a single person. It can be a type of typo. It can be an e-mail that comes regularly. This is as far as I understand where the bulk access is used mostly. It is the type of data mining that is not marketing data mining but it is pattern detection.

There is absolutely nothing that prevents with full respect of the privacy revealing (inaudible) WHOIS services of patten detection to be put in place. For instance, if you want to make a query that allows you to detect any domain that has been registered with a type of typo, you could have some automated mechanisms.

People are reconstructing reverse WHOIS databases actually. I am absolutely amazed that I have never heard the expression "reverse WHOIS lookup" in any of the discussions I have participated in in the recent months. It is a tool that I understand has been established on the side and is very useful.

For instance, you are identifying one specific actor that has registered a domain name that you consider is potentially infringing on I.P. rights. It is completely different if this actor is only registering this domain name and may be in perfectly good faith for whatever reason.

Or the same person with the same e-mail or connected e-mail is actually registering a whole range. You can have a query that is completely blind that says I have this e-mail from another search or from something that I have today and I would like to make sure that this e-mail has not been used for 20 registries. You have the data. You just query.

I would just like to open the door to some kind of innovative thinking that would allow the community that is actually data mining this data in a way that is perfectly acceptable and useful for the whole community to try to see whether new services could be respected in privacy fully that would provide them additional services because it might even facilitate to moving to something new. The choice services rather than choice data and access to WHOIS data.

>>ADAM SCOVILLE: Do you have Adam in the queue?

>>PHILIP SHEPPARD: Yes. We need to conclude this meeting very shortly, we will just take a final queue. I have Adam, Milton, anybody else? Margie I have already got and Carole, Jay and Doug. Jon?

>>JON NEVETT: No.

>>PHILIP SHEPPARD: That's the end of the queue and that will be our final queue.

Carole?

>>CAROLE BIRD: Just to go back to the question you asked earlier whether we looked in Type III for the private actors, whether we distinguish between the type of data whether we were just talking about the information that's currently available and which would subsequently be shielded. That's the interpretation I was working under. Was anybody else working under a different interpretation as to what Type III meant?

(No response).

>>PHILIP SHEPPARD: Okay, Adam on the phone.

>>ADAM SCOVILLE: I want to sort of -- there has been a lot of discussion about private actors who are looking for access as being -- using this access mechanism for data mining and, I guess, I think it is worth -- I won't take up much time. But very briefly exploring why -- and also in response to Palmer's sort of bank-based proposal, you know, why I.P. rights have a place here. Just briefly --

>>PHILIP SHEPPARD: Adam, you do have to be brief.

>>ADAM SCOVILLE: I will. And that is the purpose of particularly trademark rights is in order that we protect the consumers. That's the whole reason that the legal systems around the world have granted us these intellectual property rights. They don't exist except for the fact it is a bad idea for consumers to be confused from who they are buying from and law enforcement doesn't have the resources to be going after it themselves and there is some synergy if we have part of that function being done by the private actors. That also gets around the fact of determining on a substantive basis whether -- trying to come up with an exhaustive list of which sectors that applies to because we then have -- we then -- we know that someone has got a trademark and we know that someone else is using that mark to try and fool the consumers as to who -- as to who they're dealing with.

And that's a public harm. I guess I'm not sure I think that's correct to characterize that as data mining. I think that's perfectly legitimate.

>>PHILIP SHEPPARD: Okay. Thank you for that.

Milton, briefly.

>>MILTON MUELLER: Briefly, I want to thank Bertrand for calling attention to how much data is in the WHOIS record even post-OPoC, how rich a source of information that is and how deeply and thoroughly that can be mined for various purposes. I think we have to get realistic again about the context here.

All we are talking about is pulling out the street address, e-mail address and a phone number. Everything else is there. Okay, city.

(multiple speakers).

You have got names, for example, to the privacy advocates, even including the name is a huge compromise, okay. And now we're pulling all legal persons off the table. Let's not be greedy. Let's try to find a compromise that everybody can live with, and I think we are very close to that with the OPoC proposal and certain types of Type II access for law enforcement. If we don't, if the consensus around that breaks down, lots of bad things will happen. I guarantee it.

[Laughter]

>>PHILIP SHEPPARD: Jay very quickly.

Margie, even quicker.

>>MARGIE MILAM: We offer reverse WHOIS service. The only way we dock that is through the bulk provisions we are talking about. They are used legitimately to support UDRPs and other legitimate actions. What you're talking about is removing a set of services that are out there currently available under the current conditions.

>>PHILIP SHEPPARD: Thank you. Jay?

>>JAY WESTERDAL: Yeah, I think that's similar to what we do as well. When we offer those services, we find that it's generally legitimate people using them, law enforcement and lawyers and those type of people. So, yeah, I think you are actually hampering law enforcement by not extending the information and by restricting what's in the OPoC because by not having zip code and some of the other defining areas that don't really give away the privacy of the person, I think that it is a bad thing.

>>PHILIP SHEPPARD: Okay. Thanks for that perspective. And, Doug, final comment quickly.

>>DOUG ISENBERG: Just to further Margie's and Jay's comment, I want to direct the group to why this is important. Section -- paragraph 4(b)(2)of the UDRP creates one mechanism by which bad faith under the UDRP can be established which says you have registered the domain name in order to prevent the trademark or service mark from reflecting the market of corresponding domain name provided that you have engaged in a pattern of such conduct. That is the importance of the reverse WHOIS service.

And any change to WHOIS access that frustrates this paragraph with the UDRP should be carefully considered.

>>PHILIP SHEPPARD: Thank you for that. In conclusion, next steps, you will see will be a new version of the report. I think we made some very good progress this morning in terms of clarifying some of the questions in the report. We will try and capture as much as we can a clear thread of what's agreed, a clear discussion of where we are so you can see a thread going through the proposal so far. That will allow us to make a judgment as to whether or not we've got the bones of a practical structure and help to identify those areas yet unresolved.

Based on the conversation this afternoon, we may need to start to phrase some of our recommendations conditionally which is to say it is an ideal world, we are looking for this type of mechanism in this case and we are doing work to try to find that. If we don't find that, then we need to go to second-best and see what level of agreement is in terms of going around that because, otherwise, we won't have a robust structure all together. We will try that structure in the next report and clarifying as much of the questions we have got here and fencing some of those areas that are, perhaps, now new to the discussion based on the clarifications and agreements we had to today.

I think it has been a very positive session. I thank you all for your contributions. Please continue with constructive comments and suggestions, questions at this point online. That would always be helpful. And we will now adjourn this meeting and continue our discussions online and on teleconferences with a schedule -- I think it has already been sent out and will be repeated. Thank you very much.

(3:28)