
Heather Dryden: Good morning everyone. If you could take your seats we will begin this session between the GAC and the WHOIS Policy Review Team. So you will recall that we had a brief update at the last meeting that we had in San Francisco and so today, hopefully, we can get into a bit more of the substance now that the Review Team has really begun its work.

And next to me I have the Chair of the Review Team, Emily Taylor, and you will recall that Australia, Peter Nettlefold, has agreed to participate on the WHOIS Review Team in the GAC Chair's Representative role. So I will look to Emily and Peter to lead the discussion that we have today. So with that, can I turn over to Emily?

Emily Taylor: Thank you very much, Heather, and before starting, I would like to thank the GAC for making time for us at this ICANN meeting and also at the last ICANN meeting amidst a flurry of activity in other areas. It is very much appreciated because part of the way that we're working is to try to build up the picture from the point of view of the different stakeholders. And to have your engagement all the way through the process as well as Peter's full engagement in the Review Team itself has been extraordinarily helpful and I'm looking forward to continuing this dialog.

So what we're going to do is just, I've got a slide deck and in our other interactions some questions don't spark any reaction at all

and others spark a lot of reaction. So I suggest that we just go with that, and we try to have as freewheeling, free-ranging discussion as possible in order to get to the issues that really matter to you as the GAC members.

So if you could go on to the first slide, what I'm going to do is just remind you a little of the context. The WHOIS Review Team is one of the three reviews mandated by the Affirmation of Commitments, and so it was really part of the deal, as I'm sure is incredibly familiar to all of you, is really part of the deal in transitioning ICANN away from the JPA into the AOC, the Affirmation of Commitments.

Our scope, which we had to formulate in the early stages of our work, is taken very much from the wording of the Affirmation of Commitments in that we have to look at the extent to which ICANN's current WHOIS policy and its implementation are effective, and meet the legitimate needs of law enforcement and promote consumer trust.

Now I'll just quickly highlight various other streams of work that are ongoing. We are very fortunate to have on the Review Team Sharon Lemon from the U.K. Serious Organized Crime Agency. And with a small group within the Review Team, she has formulated a questionnaire which has been distributed to her worldwide contacts from law enforcement. So we're really trying to get at, from the horse's mouth as it were, what law enforcement expect from WHOIS, what their needs are, and the extent to which those needs are being met. So that's one stream of work.

Another is this concept that we have struggled with of consumer trust. And I would expect you as the GAC also to have your views on what you think promotes consumer trust or otherwise. But the way that we've decided to deal with this and also reflecting, I think, the spirit of the Affirmation of Commitments which talks about the ICANN community, but also the much wider community of internet users worldwide who may not be aware of ICANN, may not even be aware of the WHOIS, but nevertheless have valuable input to make about what elements make them trust or otherwise the internet and how the WHOIS may have a role or not in that.

So before going on to the substantive questions in this paper, I just wanted to let you know those other parallel streams of work. Our early work and something that we spoke to you about – and thank you very much for your input on – was our early attempts to define the key terms in our scope that we're moving forward with a common understanding. I'm very happy to take any other comments on applicable laws which formed part of your input to us.

But really, if we can go on to the next slide, the format for today's discussion is an issues paper. The whole idea of trying to surface the issues early in the process was something that Peter came up with and so necessarily it's short. We're now about half-way through our work and the issues have started to bubble to the surface, as you would expect.

So what we tried to do was to capture those issues in as simple a way as we could and really formulate questions which I hope will

then build up into a deeper analysis as we go through. So the rest of these slides are the questions from our issues paper. And what I'm going to do is just give you the slides and open up the floor to you for any comments or reflections.

But we also want to know what we're missing. So if there's stuff that you don't see or you haven't seen in the issues paper, or just random thoughts that you want to share with us, I would encourage you to be as random as possible.

So if you can go to the next slide. The first five or six questions are dealing with the initial element of our scope, policy. So we're looking at the extent to which the policy is effective, and one of the tasks that we set ourselves was to do an inventory of the WHOIS policies. This might be something that you can help us with here because there's a confident statement of the WHOIS policy in the Affirmation of Commitments itself which talks about the key concepts being availability and data accuracy.

However, we have looked in vain for a statement of that core policy itself. I think we understand the reasons why this might have just slipped through because, of course, WHOIS predated ICANN. It was part of the set-up of ICANN that WHOIS was part and parcel of it. And for the policy not to have been written down, it doesn't mean that it doesn't exist. So that's the background really for these two questions. And it might well be that the policy is somewhere, we've just not found it.

We've certainly come across the three or four consensus policies that have been developed through the GNSO, but I'd like to throw open these questions to you. What measures do you think ICANN should take to clarify its existing WHOIS policy? And thinking about the GAC principles, the wording of the Affirmation of Commitments itself, how can ICANN clarify the status of these principles because we're not quite sure of the linkages. How does this link help with the GNSO processes; is this the formulation of policy that we should be looking at or is there another one? What do you think? Would anybody like the floor?

Heather Dryden:

I think if you can continue with the issues, or... Bill, there is a request. Great. European Commission.

William Dee:

Yes and thank you actually. I don't have any... I'm not wedded to any fixed ideas but your question is a very relevant one actually. How do we clarify – if I understand it properly – how do we clarify what ICANN's policies are for WHOIS.

It's one possibility that you ask the Board what they think the policies are formally and ask for reply in writing. And if the answer is, "We don't know," fair enough actually. But then I understand that there are WHOIS provisions in the contracts. That's immediately a problem actually. If they don't know what the policies are, they're in the contracts then I think it emphasizes and increases the urgency in resolving this issue. Thank you.

Emily Taylor:

Thank you very much. Clearly we've been looking in some detail at the provisions of the registrars' contracts and the registries' contracts. I suppose on a purist type of level those I would think of as an implementation of the policy rather than a statement of the policy itself, but that might be because I'm being too uptight about it and that's as good as we're going to get. But I don't know whether there are any other comments from the Review Team itself on these issues or whether we'd like to move on to the next issues.

Bill Smith:

Hi, I'm Bill Smith. I'm with PayPal and also a member of the Review Team. I just want to... There clearly is, I would say, a policy in a sense because we talk about it and stuff like that. But when you search - do a search for ICANN WHOIS Policy - you actually don't come up with a document. If you search for WHOIS Policy, what you end up with is a document for .nz, which actually is a nice policy document.

So we have followed the trail. I've gone back; I've read the green paper; I've read the white paper, just so you know, and we communicate these things and discuss them on the team. But there is no... Policies need to be clear, concise and communicated. So that's just where I am independently. We believe there are, as Emily has put, implementations of a policy, but for any outsider or someone new coming in, it's very difficult to find a policy.

Emily Taylor:

Have we done this one? Shall we go onto the next slide? Nods will do. Yep. Next slide please. This is an area where you may be able to help us. We felt that the tension at the heart of the WHOIS and we had a very illuminating call with the Department of Commerce's Larry Strickling at the early stages of our work.

And he put it in the same way – it's the balancing act between individual's expectations of privacy as opposed to the needs of law enforcement and others who might seek to enforce maybe private law rights who want to get access to that data. And not just those enforcing rights, people who might want to buy or sell domain names or contact the registrant for whatever reason.

So in the landscape of domain name management and outside of the ICANN environment there's the ccTLDs who have their independent policy making processes, have also been grappling with these same issues and the same balancing act. And we wondered whether there might be any insight that either you or they could give us on how this has been approached in other contexts. Does anybody want to give us any information about that? European Commission?

William Dee:

Thank you. I'm not sure I've got information actually, just an observation that I think is very useful, actually, to look for insight. I guess though the problem is that the ccTLDs are in a very different situation because they're normally within a single

jurisdiction actually and they have a much more direct relationship and they have clear, applicable law; whereas, if I understand correctly, we're talking about gTLDs here and their global operators and it's the old conundrum actually and therefore internet governance people about how you try and deal with global operators acting across a number of different jurisdictions, potentially conflicting applicable law.

So I think definitely look for inside actually, but bearing in mind I imagine I'm telling you something you actually know, I sure, that the situations are very different, the challenges are very different for developing WHOIS policy at the national level for ccTLD, compared to a body like ICANN trying to develop WHOIS policies at the global level effectively. Thank you.

Emily Taylor:

Thank you and that's a point well taken and something that one always has to bear in mind when making comparisons. But one of the interesting aspects is our dialog with other sections of the community is the level of frustration at the process itself and how long it's gone on for, and the sense of it being road-blocked, but without really understanding why.

And one of the things that we thought might be helpful is to look at how controversial this issue continues to be in other contexts, always remembering the differences to the global context as well. Any other comments on this? Thank you.

The next slide. This is again kind of getting to the heart of what we saw as the key balancing act. And, in fact, also the growth of proxy and privacy services which have arisen as a market response to individuals' need or desire not to have their details published. And I suppose, Bill, this comes to your point as well. The use of proxy and privacy services seems to be something that registrants are using across all jurisdictions, not just in areas where there may be applicable laws granting rights of privacy.

There's something there that the market is responding to. At the moment, as far as we're aware, there's a policy lacuna in that there is no structural way of running proxy privacy services where there's an expectation about how long it will take to deliver the underlying data. We've had extremely favorable reports about some of the proxy privacy services and how responsive they are in giving up data to legitimate queries.

But also on the other side of that coin, others where there's no response at all and that that is one of the key problems that has bubbled up to the surface. So I wonder whether anybody here has got any experiences of this and also, if you don't mind, looking to some of the law enforcement colleagues who are in the room, whether they can contribute to that, if that's allowed. Is that allowed?

Heather Dryden:

Certainly I think this topic is of considerable interest to law enforcement and it was one of the topics for today, along with

consumer protection, so I think GAC members would be quite happy if their law enforcement representatives would like to contribute to this discussion, certainly. U.S.?

Bobby Flame:

This is Bobby Flame from the FBI. With the issue with proxy services, obviously, as law enforcement, it is a hindrance. It does delay how we do investigations because once you have a proxy or privacy registration, it puts up another layer in which law enforcement would have to serve legal process and that slows down the investigation, especially in international investigations.

In other words, if my U.K. colleague from SOCA would have to go to a United States registrar, you would have to go through a very complicated and lengthy legal process which would basically kill the investigation. So that's the first thing.

In the world in which proxy and privacy registrations exist and we don't see the end to them, the ideal solution would be to kind of stick to some of what even the European Commission, I think was Article 29, refers to as a non-commercial entity, non-commercial entity of private individual, if you will, that engages in non-commercial practices.

In other words, you can be a private individual, but if you have a business or your website is being used for a business, your domain name that you registered is being used for business practices, that is something that I don't see would fall under any privacy

protection or would need a privacy or proxy registration to justify it. If that is not the case, then yes, maybe.

Also if you're a business and you register a domain name, I can't understand how you would need to hide your identity. If you're a business, there's obviously laws that you have to make your existence public, the transaction has to be public. So that's kind of some input on that.

Heather Dryden: Thank you very much. Greece?

Panagotis Papaspiliopoulous: Thank you. European Personal Data Protection Law does not make a distinction between businesses and individuals. To the extent that it is data which allows identification of persons, it is personal data and it falls under the European Personal Data Protection legislation.

And there are two main principles which apply. One is the purpose limitation principle. In other words, the personal data which is public should be used for the purpose for which they have been made public. And in this respect WHOIS data may be limited to as much data as is necessary for the purpose of WHOIS data and therefore, the purpose of WHOIS data has to be well-defined. It may be already, but I'm saying it as a matter of principle. We cannot simply open the purpose for whatever reason and keep adding on purposes and therefore, keep adding on all

sorts of data that should be included. We need to be clear as for what purpose WHOIS data is there.

And the other limitation is that... One is a purpose limitation and one is a quantity limitation so you don't need more data than is necessary for that particular purpose.

Another matter, of course, is – and I'm fully sensitive to this because I have been involved in law enforcement requests since the 1990s when I was in the European Commission – international investigations. This is a very difficult matter because here, albeit most of us if not all, are more familiar with law enforcement processes which are under the rule of law so there are clear rules as to how law enforcement has access, how they operate and therefore, there is a certain confidence of citizens and users as to the legitimacy of this law enforcement involvement.

In some cases this may be more complicated, and in some cases I'm not sure we would want to give access to whatever law enforcement inquiry from whatever part of the world. I will leave it at that. It's a delicate matter.

Emily Taylor:

Thank you for raising those and for raising the issues of purpose and quantity because it takes us back to where we started in a way in that part of the purpose of a statement of policy perhaps would be to make it clear why this data is being gathered, what it will be used for and force the consideration of how much or how little is

necessary to fulfill that purpose. So thank you very much for raising that.

I also would say – because I’m aware that as GAC, you may feel that you need to give us a consensus view, but please do feel that you can give us a view from your own perspectives or from your own country perspective; that we’re not looking for that very... the formal consensus advice and I’m sorry, I should have made that clear right up front. Should we go onto the next slide please.

This is another aspect of proxy and privacy services and one that’s been mentioned in some of the comments. But here we start to come to the key concepts of accuracy of the data and the availability of the service. And perhaps, first of all, are there any concerns about proxy and privacy services from your perspectives? But what do you see the impact being on these things of accuracy and availability, if any? If there’s no comments on that, I think I’ll pass through to the next slide.

These questions and the questions following on relate to the other aspect of our scope which is namely, the implementation of the policy and how effective it is. And just to give you a little bit of background, so far the feedback that we’ve had from other stakeholders – and I’m thinking particularly of the users of WHOIS data in this way – that they’re saying that more or less they could live with the contractual provisions, the obligations that are set out there, as long as they had a perception that they were being effectively enforced or complied with.

I don't know whether you as GAC members have any – or our law enforcement colleagues – have any general comments to make about how effective you see the compliance effort as being at this time. United States?

Suzanne Sene:

Thank you, Emily. Actually the GAC has addressed this in the context of our multiple statements of consensus GAC advice on the introduction of new gTLDs, and we have made the point repeatedly over the past several years that it is a concern with the apparent inadequacy of the current contract compliance situation that has given us great cause for concern as we look ahead with the potential introduction of 200, 500, 800 new gTLDs, all of those contracts need to be enforced and all of them will have similar provisions that, of course, pertain to the elusive WHOIS policy.

So, yes, we the GAC have gone on the record; we the United States have gone on the record as well multiple times over the years, expressing concerns about the inadequacy of contract compliance. And if I can just go back to proxy for just a minute, for what it is worth in .us, we actually do not permit proxy registrations because we consider it a public resource; therefore, the database needs to be public.

From our perspective there's a great deal of logic to that approach and we have expressed concerns as well to ICANN about the proliferation of proxy services and the fact that they seem to have become unmanageable and there's no real policy to guide them.

And we understand that in some cases registrars and/or their resellers apparently have marketed these policies differently.

So some are called privacy policies; some are called proxy services and they're not entirely the same. So it's very confusing out there. So we have certainly noted that and I imagine you all might have as well. And that is part of the problem. There is no uniform "policy" for privacy/proxy services. Thank you.

Heather Dryden:

Thank you very much. I have Denmark.

Julia Kahan-Czarny:

Thank you. I've just got through a few sort of high level comments from my law enforcement and they are worried. They don't think that the policy is sharp enough according to validation and that the sort of ongoing control of registrants and other persons was cold and the real persons behind it is good enough. And that makes their work difficult and that it's too easy to just write sort of an arbitrary name or incorrect names when you make websites and the like. And they believe that there should be fast and effective consequences if there are lack of or false information. Thank you.

Heather Dryden:

Thank you very much. Any other comments on this?

Bobby Flame: Another thing that I would like to point out is it has been shown in our agency that criminals have actually used privacy and proxy registrations for botnets, even more severely or – I’m not thinking of the right word, but more alarmingly – in national security cases. So they will pay money. Criminals will pay money to use proxy and privacy registrations.

There’s been an argument that, “Oh, criminals wouldn’t need to go so far as to pay money for a proxy or privacy registration. They could just obfuscate by putting frivolous information in the WHOIS, the regular WHOIS.” But they will. They will spend the extra \$10 to hide their identity and to use proxy and privacy registrations.

Heather Dryden: Thank you very much. Singapore?

Nora’in Ali: Thank you, Chair. Just I will echo what Suzanne has said. I think increasingly we are facing pressure from the public. Practically those individuals who register second level domain names and who ask that their contact and their particulars be masked.

And we know that so-called privacy and proxy services are not effective at all. In one or two cases when we tried to find further on the contact details, we just find a black hole and we just don’t know what to do. And I think it’s happening to see that in the U.S. for the .us policy you require contact details to be shown.

Certainly this is what we would like to learn from you to see how fast we can address this issue with an interface and introducing the data protection registration. And this is an area where we have to look at it closely.

I just want to respond to the gentleman from the U.S. law enforcement agency remarks. So we see is that having the proxy and privacy service provider is not just one day you will be able to go to the contact. The very fact that you had to go to another party and that party would alert the registrant, in fact, compromised the law enforcement agency investigation. So we see that ICANN needs to come out with some policy on this use of privacy and proxy services; otherwise, you would just make the (inaudible) very difficult. Thank you.

Heather Dryden:

Thank you very much. I have the U.K. and then Estonia.

Mark Carvell:

Thanks very much and I think one of the issues, and it was picked up in our GAC principles, was the importance of monitoring what's going on with gathering information about WHOIS, its use, how it's being abused, what's happening in the market of delivering WHOIS services, emergence of new forms of proxy services, the legitimacy of those, the abuse of that avenues of proxy registrations to avoid the key objective of WHOIS which, as the U.S. says, really is in the interests of the whole community that there is an effective WHOIS database.

That was one of the recommendations from the GAC when the principles were drawn up that there should be effective sharing of information and so on so that some sort of handle on this would develop and responses to failure new developments could be constructed quickly by the community and pushed forward by ICANN through contractual avenues or whatever.

So I guess that whole kind of expectation of the GAC when the principles are drawn up is what is most relevant to these questions. Has there been absolutely no monitoring and gathering of data? No monitoring and so on? I mean, it's... For us as civil servants you set up a policy, you implement it, you construct the means to insure the policy's limit; you monitor; you gauge how effective it is and then institute changes necessarily. So that's the kind of approach governments would take. Is it the parent or the Review Team that's been a complete failure of ICANN in this respect? Thank you.

Emily Taylor:

Thank you very much for raising this issue and yes, indeed, the GAC principles – when was it, 2006, 2007 – asked for a number of studies to be undertaken. The one that's available to us is the WHOIS Accuracy Study which was completed in 2010. And that actually I think does a reasonably good job of just giving us a baseline to say – and this is the point that you've raised is one that I was talking to somebody from the registry and registrar community about earlier this morning – the fact that the policy conversations at ICANN could really do with an injection of some

real data and evidence base to help everybody to understand whether their perception is borne out in the numbers.

So there's one study. We're aware that other studies are just about to start; have not been completed at this stage and perhaps the next Review Team, when that cycle comes around, will have more evidence in terms of independent studies than we have the benefit of.

We also do have the reports of the Compliance Team itself of its interactions and its compliance efforts, and we'll be looking quite carefully to see what is being reported and to see whether there are adequate measures in place to see whether those compliance interventions are actually having the required effect.

So I hope that gives you a little bit of a flavor for how we're approaching it. So I think we have in the list Estonia and European Commission and U.S.

Heather Dryden: Thank you. Estonia, please.

Marek-Andres Kauts: Thank you. Marek-Andres Kauts from Estonia. My question is connected with this issue raised by Denmark. So I agree that identification of registrants, it must be considered seriously. In our document it is said that only 22% of WHOIS records could be considered truly are correct. So this day forward is there going to

be some improvements and innovation in increasing the accuracy of WHOIS and identifying registrants.

For example, using public infrastructure which is number of countries implementing it is going to increase or using identification methods which are used to verify the origin of money and money transfers.

There is much done in the field of efforts trying to compete against money laundering over the last decade so organizations like this G7 found financial action task force of FATF and the 8-month group of Financial Intelligence Unit. They have been operating very successfully to stimulate different states to introduce international legislation sets of measure against money laundering.

There are such provisions like FATF 40+9 recommendations. They can be used to change domain registrants' personal identification. For example, we have done it Estonia that stipulate that banks must identify the person that is the account holder and that also stipulate the bank receiving the transfer is only allowed to accept it when sending bank complies with these recommendations and this second aspect could be used by registrars to identify these registrants' identification. So have you considered these issues in your Review Team and also these issues which are considered in fighting against money laundering? Thank you.

Emily Taylor:

Thank you very much. I think Australia would like... or Peter from our team as we know him would like to respond to that one.

Peter Nettlefold:

Thank you to Australia for raising those points. That's really interesting and I'd be more than happy to discuss your Estonian experiences with this kind of approach. That would be very useful. But, yes, so the Review Team has had a look at this and as the GAC saw with our interaction with the registrar community in our meeting here in Singapore, the question of validation is a very sensitive one for the registrar community itself.

As the situation is at the moment, we understand from our reading of the contracts ourselves and our interactions with ICANN's Compliance Team, in the first instance at least the obligation to provide valid and correct and accurate registrant details falls to the registrant.

The next step in the chain is if there is an issue raised, a complaint or there is some concern about the accuracy, then someone can complain to the registrar and the ICANN Compliance Staff has identified to us potential concern they have in their ability to enforce this obligation because the registrar's obligation to take any action is caveated.

It is the registrar if there is a period of time to require the registrant or to ask the registrant to correct any problem with accuracy and then after that period the registrar may take action, is my understanding.

So that's been identified to us as a potential concern as well. So that's the existing frameworks. The obligation, as I understand it,

falls to the registrant in the first instance and the registrar's ability to take action or their willingness to take action is caveated.

So one thing we will be looking at is the question of validation. But I think we can assume that this will be a very sensitive one for some member of the community.

Heather Dryden: Thank you. European Commission.

William Dee: Yes, thank you. I'm very interested in discussion. I think Peter's probably covered party what I was going to ask actually, and I think along the lines of the U.K. intervention as well. I look at that question how effective are ICANN's current WHOIS related compliance activities, and I think I don't know actually. I don't know how effective they are.

I guess we know that law enforcement are unhappy with the current policies – if they exist, I should add in brackets – and we know there's problems with data accuracy. We all know that. I guess the questions I'd ask in terms of how effective the Compliance Team are, it would be interesting to have – and maybe you have this already – how many complaints they get from people; how many times they've intervened; how many times corrective action has been taken by the registrar and how many registrars have been de-accredited for non-compliance.

And then probably evaluate how effective the compliance policy is. I don't think the GAC have been kind of provided with any of that information so far. But I guess normally, as I think you explained, Peter, normally the registrar would assume the data was correct until they received a complaint, and then they either take corrective action or they ignore the complaint or feel it's unjustified.

At some point then somebody has to complain to ICANN and then the Compliance Unit have to take action. If we're talking about ICANN's compliance, I think we need to look at their performance in that context. And I don't know if you've had any. Have they de-credited – simple question – have they de-credited any registrars for non-compliance with contract provisions related to WHOIS? I don't know if you've asked that question or you have that information. Thank you.

Susan Kawaguchi:

We actually asked part of that question... Oh, I'm sorry. I'm Susan Kawaguchi and I represent the CSG and I work for Facebook, so we face a lot of issues with the WHOIS. And we asked, specifically I asked that question to the Compliance Team on inaccurate WHOIS reports cause you initially report them directly to ICANN. They then refer that to the registrar.

And the registrar has the right to determine if the information is patently false, to go ahead and cancel the domain registration. But ICANN did not. The Compliance Department did not have

numbers. They don't track that; they don't ask for a report back from the registrars and it is solely left up to the registrar's discretion.

So I see that as very problematic in the fact that many registrars are very good in all of their compliance activities, but the ones that aren't really are not good and are the most problematic. So in the inaccurate report right now to me, the system's not really working well.

Emily Taylor:

I think if I could just follow up on Susan's point and in response to your question, and it comes to the point made by the U.K. as well, that there's the enforcement activity, then there's how you measure it and then there's how you communicate it. And the fact that you are asking that question at all tells its own story perhaps. I have U.S.

Mark Carvell:

I just wanted to make a couple of comments with kind of a vicious loop or cycle with the Contractual Compliance and the WHOIS. A few of us went to go speak with Contractual Compliance last month and one of the things that was pointed out was that once they get a complaint of false WHOIS information, they would go back to the registrar and then the registrar would go pretty much to the registrant.

I think a lot of this problem would be solved by the validation of the registration information at the time of the registration and periodically audited throughout. That was a big issue that we spoke with the registrars about, stating that that's something that we need to look at that would be a difficult issue. But I think this would go to the very core and the heart of the matter.

If you're getting good data at the beginning, the best to your ability based on validating that data, the best to your ability, you would solve a lot of these problems. And that was in our law enforcement recommendations.

The second thing that was in our law enforcement recommendations was that we were asking for ICANN to actually provide audit reports on such things such as de-accreditation and reports of abuse. So that was another thing that we had seen and we had tried to address in our recommendations.

Heather Dryden: Thank you. I have Bill Smith.

Bill Smith: Bill Smith. Two things – one to echo Susan's comments from another supplier of internet services, PayPal and eBay, and we find exactly the same problem. Many registrars, in fact, are extremely good actors. They may not be perfect, but many of them are extremely good actors and we find a smaller number that are extremely bad actors.

We don't expect perfection, but it's our hope that we would find a way to call out the bad actors and if we could encourage compliance in that regard, it would be good. One other thing is if we talk about registrars, I think we kind of need to separate them into, in essence, those two camps. We don't want to paint them all with the same brush because they react very negatively.

Something else following on Bobby's comment. I'm a computer scientist, engineer by training, and you learn very early on in these disciplines the earlier you catch a flaw, the less expensive it is to correct it. So if you catch it in the design phase, it costs next to nothing to fix it. If you catch it after it's been deployed, it will be several orders of magnitude more expensive to correct the problem and I believe that applies here in terms of data. There's also garbage in; garbage out. But it's really much less expensive to catch things early on.

Heather Dryden: Thank you.

Susan Kawaguchi: Susan again. So actually I just received an email and ICANN has de-credited registrars for non-compliance with the WHOIS inaccuracies if they do not investigate. He's going to provide me some numbers, but also they're working on additional upgrades to their system so in the future we'll have some of these metrics.

Emily Taylor: Thank you. Could we move to the next slide please? I'm sorry. U.K.

Mark Carvell: Sorry, yes, thanks. If I can just come in quickly. I'm not sure if it's relevant here cause I'd have to be reminded where the obligation to update data lies. Is there an enforcement role with the GAC or is it purely discretionary for the registrant to commit to update? My impression is that a lot of the stuff is just simply outdated and then becomes useless to law enforcement or to anybody. But is that an issue to cover here under these questions or elsewhere?

Just one thing – lady on the left, Susan, could you speak closer to the mic because I'm having difficulty hearing you and I'm sure on the far end they'll have difficulty too. Sorry, it's just the dynamics of the room more than anything else. Thank you.

Emily Taylor: Thank you very much. On where the obligation sits and whether they're just, you know, discretionary or mandated, the Registrar Accreditation Agreement makes it very clear that ultimately it is the registrant who is responsible for providing and maintaining accurate data. The registrar is obliged to include those terms in the registration agreement.

And also there is a policy which is managed by the ICANN Compliance Team whereby each registrar has to send out a

notification to each and every registrant every year to remind them of those obligations. And the compliance in following that obligation, *i.e.*, to send out the notice, seems to be very high.

However, unfortunately, it's not at the moment possible to track what happens as a result of the registrar contacting the registrant. In other words, we don't know what effect this intervention, this costly and convenient intervention for many registrars which gives them a support load, we don't know the effectiveness of it for what it's intended to do, *i.e.*, does it make the data more accurate or not? We don't know.

Shall we move on to the next slide? Still on the issue of compliance. What do you think ICANN should do to insure the WHOIS commitments are effectively enforced? And does it need any additional power or resources to effectively enforce its existing WHOIS commitments?

And I think this is a point made by the U.S. earlier that this may have been an issue that has been more recently in your minds in relation to the new gTLDs. So this might provoke some reaction. European Commission?

William Dee:

Thank you, yes. I'm just intrigued by the expression "does ICANN need any additional power." What was your thinking behind that?

Emily Taylor:

I think this may be awful to not making the question very clear and you're not the first person to phrase that. I think we may be conscious that the glue that sticks everything together in this world is contracts, private law contracts. I think that we were thinking very much in terms of contractual provisions, whether in the registry, registrar accreditation agreements or otherwise. But we're very interested in free-flowing ideas on this. U.S. and then New Zealand.

Suzanne Sene:

Thank you. It's just sort of a passing thought that you could also present the question in a slightly different way, which I know the registrars might not be particularly happy with, but does the approach to amending the Registrar Accreditation Agreement itself need to be re-examined. Because actually the flip side of that is should there be improvements in the RAA; should there be additional provisions in the RAA. That is the other side of the coin.

And the problem has been and seems to be at the moment a continuing impasse, if you will, that the registrars are resisting further amendments and that even should they accept some, there's this four-year cycle apparently. So that even if you could get agreement on some amendments now, they wouldn't actually come into force until three to four years from now.

So that's another problem, I would think. So you're quite right. I believe the issue is the provisions in the contracts. So do we have

the right provisions? Because a otherwise, really, ICANN's enforcement has to track to the provisions themselves. Thanks.

Emily Taylor:

And just as a point of information, I believe that the last Registrar Accreditation Agreement was introduced in 2009 and I think what you say about the cycle is correct. However, my understanding is that many of the registrars, or the vast majority of the registrars have voluntarily adopted. So I think there's a difference between the backstop – what will happen if not – and in fact the reality is a slightly rosier picture.

But certainly the feedback that we have had from members of the Compliance Team is that they would... They feel that they don't quite have the contractual powers that they would like to in order to be as effective as they would like to be. So I'm sure if that's misreporting that one of them will correct me on that. New Zealand?

Frank March:

Thanks. This is a very simple question really. How much information is available to the Review Team about the effectiveness of ICANN's actual enforcement of existing contracts? This is one step back, I guess, from the point being made by Suzanne that there's not much point in having all sorts of revisions in contracts if those contracts are not actually being enforced. And I get the impression that that is quite a gap, but I may be completely wrong so I'll just leave that question with you.

Emily Taylor: Thank you for that question. I would say that we've been in dialog with the Compliance Team throughout the process. Our most recent meeting with them was a couple of days ago. We have a small group within our Review Team who are looking specifically at the area of compliance and some of them are going to be visiting the Compliance Team sort of on their home patch to see them at work.

So they have been very open with us and providing us with the information that they have, and have also been open with us about not only what they see to be their successes, but also their frustrations, which is exactly as one would want and expect at this stage. And we're obviously going to be looking at the information they provide us with very carefully. U.K.?

Mark Carvell: Thanks very much. Are you looking at whether the Compliance Team is resourced sufficiently? Is that within your remit of things?

Emily Taylor: Yes. Yes, it is because part of our understanding of what we've been asked to do is look at the effectiveness of the implementation of the policy and clearly resources, organizational priority are part and parcel of that. Shall we move on to the next slide?

Let's think for a moment about accuracy – something that we have talked about in this session, but do you have any suggestions for how accuracy can be improved? The member from Estonia mentioned a figure of 23% being as the sort of fully, fully accurate at the moment.

But I think in fairness would just highlight that on the same study there was roughly the same percentage, *i.e.*, 20-something percent where it was totally impossible to make any contact. So there's clearly a sort of 80 percent-ish amount, 75% I think, where it's possible to make contact with the registrant kind of somehow, but a quarter where it's not really.

So do you have any suggestions? Can you point us in the direction of lessons to be learned from ccTLDs on data accuracy, efforts that are being made in that regard. So please let us know. Estonia?

Marek-Andres Kauts:

Thank you. My question was to be in this topic, not this previous, but I have another one. Your approach is this accuracy is connected to this issue that is it possible to contact the registrant or not. But my question is that I would also consider that this accuracy is important because to put some responsibility of this domain name to this registrant. Thank you.

Emily Taylor:

Thank you.

Male: Again, a fairly obvious question – who pays for these domain names? I mean, how many registrars offer free domain names? Is it not possible to follow the money? Is that too simple a question? Somebody’s paying for them somehow; they must be contactable somehow. Am I missing a point here?

Emily Taylor: Not at all and in fact, one of the issues I think we need to explore more closely is the extent to which registrars are using the same dataset to contact their customers. U.S.?

Suzanne Sene: We’ve had these discussions ourselves with registrars and I’m looking at Bill here because I know he’s very mindful of this. And I may get this wrong so, Bill, please feel free to correct me. But because we pointed out it’s obvious – if you are selling a domain name, you certainly know how to get paid as a registrar. You know who is paying you the six or seven or however much you charge.

And my take away – and they’ve always said yes, but that’s only for payment – and then we have to delete those records or there’s no way for them – and maybe it’s a software issue as you were saying – there’s no way for them to somehow transfer that data and retain it as the source of data for appropriate or accurate WHOIS data for the registrant.

And that has always struck us as being just a bizarre situation and a big part of our problem. We know they're getting paid. So it seems odd that they can't somehow use that same data to actually populate the WHOIS database.

Heather Dryden: Sharon Lemon.

Sharon Lemon: Sharon Lemon, Serious Organized Crime Agency, U.K. I'm probably talking about the 25% where we're never going to track the registrar. And what we're finding is that people are bulk buying domain names using algorithms that last about 30 seconds on stolen credit cards. And they've worked out exactly what the level is for them not checking out the amount that's spent on the credit card, so by the time that they realize that that's a stolen credit card, it's all over.

And also for the legitimate purchase of domain names I understand it's not simple as, you know, AmEx or MasterCard we've got their name in accounting, it's very often done by third party paying systems, so that's quite complex layering as well, certainly for the ones we can never track, many of them are bought on stolen credit cards so we can never track anybody.

Emily Taylor: Thank you.

Male: Sorry to ask another question, but am I to understand that something like a quarter of the WHOIS database comes into that category? It's 25%, 23%, something like that?

Bill Smith: This is Bill Smith. We are referring to a WHOIS Accuracy Study that was done. I believe the number is 23%. Yeah, I'm trying to recall exactly. It's not as bad as the 23% number might indicate. I'd have to go back to the study. It's broken down into patently false which is not 23% I don't believe. Maybe Peter recalls or Sharon.

Sharon Lemon: Sorry if I've confused. I'm not suggesting for one minute – I think it's 21% that you can't track anybody. What I was saying was the crime type I'm talking about will fall into – that will be within that 21%, not the whole of the 21%, so I've confused you.

Emily Taylor: Does that make it clearer?

Male: Yes and no. And I'm sure she has the same level of confusion I do.

Peter Nettlefold:

Again, I don't have the study right in front of me but I can perhaps expand on what Bill has said. This is an ICANN study; it's one of the few that we have like very clear and substantial data or that I should add for the benefit of some members, I understand that some members of the community there's some questions about the exact metrics they used in some, but that's probably like would be the case with any study in my view.

But the study broke up the accuracy or inaccuracy of WHOIS data into a number of different levels – I think the scale was about five. And the figure that we're talking about with the 21% is an amalgamation of the worst two figures. So I think the way they're broken up is substantial failure and complete failure.

I think the complete failure was around 8% and the substantial failure was around 13%. And those two categories are essentially that you cannot make contact with the registrant. So 21%, you simply can't find them. And obviously there are the other categories and scales and so on. But that's the 21% figure we're referring to.

Emily Taylor:

Okay, we'll just go on to the next slide if we may, which is I think our last questions. And I don't think we've actually managed to get through to the end of the slide deck in any of our meetings, so that's some achievement.

The next is really talking about on the one side the barriers to compliance, the cost, perhaps of compliance; but also the costs of

non-compliance. Maybe you can help us with your perceptions about what do you see as the major impact if there is non-compliance? Perhaps we could start with that one. Anybody? U.S.?

Suzanne Sene:

Just an observation from our perspective, the non-compliance by registrars with WHOIS policy creates enormous problems for any legitimate user of WHOIS data. And, of course, as you know from the GAC principles of 2007, we had quite a long list of legitimate uses of WHOIS data. And so all of those legitimate uses suffer and in particular, we have our law enforcement colleagues here today. Law enforcement in particular, whether it's civil or criminal.

So I think that's a real huge problem. I guess the flip side too is kind of interesting to look at. What's the cost to the registrar of non-compliance? Doesn't seem to be very high.

Heather Dryden:

Thank you. U.K.?

Mark Carvell:

Yes, thanks. We kind of touched on one already – the registrar having to notify the registrants. I mean, that must be a very costly exercise, an extensive, massive, exercise. Are there more cost effective ways of doing it? Are they sending letters or what? Thanks.

Emily Taylor: Well, I think that there's the cost in financial terms of that compliance. This is my understanding from speaking to registrars. I believe that it's done by email primarily. However, the knock on effects of that is that often they have a support load of people saying, "Why are you sending me this stuff? Who are you? What is this all about?" It creates a support load which has a cost but it also sometimes gets blacklisted for spam as well.

So they have all sorts of difficulties. And so I think that your question does hit it. What's the most effective way of getting to where we want to be. Sorry. Denmark.

Julia Kahan-Czarny: Thank you. No, just one thought that it's also about the trust in the internet as a whole I think.

Heather Dryden: Thank you very much for that. Bill?

Bill Smith: To the U.K.'s question about cost – the thing I would throw out – and this is Bill Smith. Sorry. – is in a different setting in basically password resets for any organization, prices 10 years ago ranged to do a password reset between \$75-\$100 U.S. dollars. At the high end, \$150, the cost then to send out a notice or deal with it in some effective way would be about \$1.5 million per 1,000 such issues.

At one point ICANN was dealing with something like 35,000 or 40,000 per year, to give you an idea of the potential scale of the problem.

Emily Taylor:

Thank you. If there are no further questions, we can conclude this session and I'd like to thank you all very much for your participation and for the ongoing support that we've received from you for this process and we look forward to continuing that dialog as we progress.

Heather Dryden:

Thank you very much for coming again today to meet with us. I would note that you have a public comment period open on your paper and so GAC members certainly can comment on that, and we can continue the discussions within the GAC as well and I expect Peter will be guiding that as before. So thank you again.

Some announcements for GAC members. There will be a meeting at lunchtime today from 1 to 3 p.m. in the Sophia Room of the ASO. They're holding a workshop on IP Addressing. Activities and the Board will be present at that meeting, so that might be of interest to some of you.

Also we are going to set up a meeting tomorrow at 10 a.m. We don't have a room yet, so that the GAC can receive a presentation from the ASO, in particular around IPB4 depletion. I know there's been recent developments in relation to that that may be of interest

to GAC members. And so by holding these two sessions and inviting the GAC, this is our way of trying to create a time for those of you that are interested to actually talk to the NRO and get some information about their activities.

Also, there is a preparatory meeting over this lunchtime or a preparatory discussion might be a better way to couch it. Katim Touray from the Board is proposing a developing country summit and so he has requested that those GAC members that are interested go to that meeting, and I know that there are various activities happening in relation to developing countries, and so if some of you would attend and would comment to Katim around what you think the priorities are and what views there may be about holding such a summit.

I know, for example, that the Senegalese hosts already have a meeting proposed for before the ICANN meeting in Senegal and also we're very much preoccupied with the new gTLD program and how to find a way to address developing country needs. So I have my own questions around is this the right timing, how could a developing country summit be used to good effect? So we haven't had a chance to really discuss this.

But I'd like to plant those thoughts and ask those of you that are interested to please go and insure that there are some inputs coming from this committee from you and so that we can influence that. Would anyone like to comment on that before we break? No, okay. Planted the seed. So we meet back in this room at 2:30 to

meet with the Security Stability and Resiliency Review Team.
Thank you everyone.

[End of Transcript]