WHOIS Policy Review Team – Commercial & Business Constituency Meeting Transcription
Tue, 21 June 2011 14:00-15:00 SGT; 06:00-07:00 UTC

Note: The following is the output of transcribing from an audio recording of the WHOIS Policy Review Team – Commercial & Business Constituency meeting on 21 July 2011 at 06:00 UTC. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. The audio is also available at: http://audio.icann.org/meetings/singapore2011/cbuc-1-21jun11-en.mp3

Tony Holmes: We are very much looking forward to this. The WHOIS has been something very close to our hearts for a very, very, very, very long time. So welcome. Emily, I think at this stage I should hand over to you. Thank you.

Emily Taylor: Tony, Marilyn, thank you very much for -- sorry, and J. Scott. Thank you very much for your invitation or accepting our request to come speak with you. What I'm going to do is I've prepared a slide deck, but really based on what's happened in similar situations, I think that people will just end up talking about the issues that are sort of interest to this particular stakeholder group. And that's great because as Tony said, we're all acutely aware that you've been living with this issue for a very, very, very long time. And I'm sure that you have valuable insights and inputs to make to us.

So if we could just move onto the slide deck. I'm not sure who's driving. Who's driving? Okay. Just a little background because both at meetings here and in San Francisco, I'm aware that there's been a little bit of fuzziness about whether we are another WHOIS initiative, working group, PDP, vigilantes, whatever. We are -- our background is that this is one of the affirmation of commitments reviews. So along with the accountability and transparency review team, the sort of stability and security review, this is mandated in the affirmation of commitments as one of the things that ICANN agreed to put in place when it transitioned from the joint partnership agreement to the affirmation.

So we're about six months into our work in earnest, and so far we have identified our end scope which is just in brief to evaluate the extent to which ICANN's existing WHOIS policy and its implementation are effective and meet the needs, the legitimate needs of law enforcement and promote consumer trust. So there is actually a whole raft of quite tightly or complex issues contained within that scope that all need to be defined and unpacked. And our early work has been on trying to reach a common understanding about what these different terms actually mean to us so that we can go forward on that basis. And we did a public comment around the time of the San Francisco meeting on those definitions.

So the next slide, the reason why we're here, our excuse to be here today, is that now at this point in our work, and in fact throughout it, to be honest, the issues bubble to the surface. The points where sensible people disagree, areas within the WHOIS dialogue which will be very, very familiar to you and to this group over the years, are coming to the surface. And what we wanted to do to take the work on was to highlight those issues as early as possible and to get the community's feedback on them. Of course we want your feedback on the issues, but we also want your feedback on issues we may have missed as well, so please keep that in mind.

So the next slide is just a rundown of the different questions and issues that we have identified. And so at this point what I'd like to do is just highlight them and if there's any that you want to jump in on, please do.

Broadly speaking, and in accordance with our scope, what we're doing is looking at policy and then looking at implementation. So the first few slides relate to policy. When we started our work, what we found is that in the affirmation of commitments and indeed in the gap principles, there are quite confident statements of what the WHOIS policy is. And broadly speaking, it's talking about availability, accuracy of data, subject to applicable laws. But in -- we decided to do an inventory of the policy documents and the statements of policy. And to our surprise, we found that these were rather hard to locate. And in fact, we haven't been able to find an enunciation of the core WHOIS policy. Whereas of course we are aware there are a number of consensus policies that have been developed over the years that sort of are riders to WHOIS, but the central policy itself we haven't been able to find. If any of you know where it is, please tell us. Marilyn.

Marilyn Cade: Well I'm just going to comment on this as a placeholder. WHOIS was imbedded as a requirement for ICANN as was the UDRP. And I don't know if Phyllis is still here --

Unidentified Participant: Is there a white paper on it?

Marilyn Cade: Well no, it was -- that wasn't how it was imbedded. But it was sort of a criteria. There's language, Emily, that says something like ICANN will maintain a database that will do the following things. So it's not called WHOIS, but the characteristics of that database equal WHOIS. And that was given to ICANN [DNUCO] as a requirement as was ICANN Shall Have A Process, that sort of roughly defines dispute resolution, right? It was in five working groups, A, B, C, and D, four working groups maybe, that developed the policy around -- so if you look there, that would be the place I think to look. But you wouldn't -- WHOIS was not versed at ICANN. It came in as a requirement.

Unidentified Participant: It would be a great help to the review team if someone could point us to a document, okay? We are doing an evidence based approach and the evidence so far is there is no document that talks about the WHOIS policy. There are a set of consensus based policy, I would say, amendments. There are pieces of language in contracts that could be taken as policy. But we view those as implementation of a policy, not the policy itself. And so in doing this review, we're just communicating back to people in the community. It is very hard to locate one or more documents that clearly state the WHOIS policy. Policies are supposed to be clear, concise, and well communicated. And as a review team, I think we are unanimous or very close to it, that we can't find it.

Ron Andrew: May I -- I'm sorry, Ron Andrew from BC. WHOIS has been around for [as long as] the Internet, predates even I'm hearing. So I would think you've been sifting through rafts and rafts of documentation. Is that correct? And so you're saying you've got just a dog's breath as to documentation? There's no clear cut documents?

Emily Taylor: That's a very fair summary, Ron.

Ron Andrew: I'm sorry to hear that for you, I really am. But more importantly, I'm sorry for the organization because it should not be that way. That is a big staff oversight that --

Marilyn Cade: I'm just going to make one other short suggestion. There's a guy named [Louie Tuton] and if you haven't e-mailed him and asked him that question, sorry, but I would try that.

Mike Rodenbaugh: I'm Mike Rodenbaugh with the BC and the IPC. I don't know, I just feel like you're spending a lot of time cycling around on kind of a non-issue. I understand you'd love to find this perfect, granular policy document. And whether it exists or not, I don't particularly care, because I don't think there's a whole lot of uncertainty as to what today this policy is. I think it's embodied pretty clearly in the registry agreements which are consistent and very detailed. And I don't really hear people -- I don't ever hear questions about what the obligations are today. It's about how to improve it. And that of course is the whole point of your effort, yeah?

Emily Taylor: Absolutely right. And I think that we have to separate the librarian instinct for wanting everything to be documented and easy to find. And I think that that is, actually, an issue particularly for people coming into this environment for the first time and wanting to educate themselves and get up to speed on the issues. But of course, then there is the practical aspect of is this really a problem and what are the problems relating to it? And as we go on through the slides which I might just do in the interest of time, just progress, so I think that the second question probably goes to your point. In brief, it's really saying, we've got these statements and high level principals, do we need to clarify them? How?

But if we go to the next slide, this moves onto a different issue, a different aspect of policy which is the well worn and familiar balancing act between individuals' expectations of privacy, business use of proxy services or privacy services, and also how to make the data available while also not transgressing applicable national rules.

One of the things that we thought we might look at is what the rest of the landscape look like, because this is -- WHOIS is applicable to the G space but also to the ccTLD space as well. And others have been grappling with the same issues. And so the next question is really looking at the proxy and privacy services, but also a more general question about how, what is the right balance to achieve? And maybe we could just pause here if anybody wants to come in and ask or make any comments on that.

Unidentified Participant: I was just trying to understand what role the RFC played in your search for documents.

Unidentified Participant: I did the searches on the RFCs. The WHOIS protocol is very clearly defined. We have no problem with that. But WHOIS actually is not just a protocol, there needs to be a data scheme. What has to be included in the WHOIS? And then the service. How is the service operated? And the RFC goes to the protocol and a bit about the service, saying it's a Port 43 service. But that's it. Beyond the -- if you look at the RFCs on the history of the RFCs, because the latest RFC is actually just a one-page document that says it's operated on Port 43, you send in requests and you get back answers. That's basically what the RFC says.

Unidentified Participant: Is that the 2004 drafts?

Unidentified Participant: No, it's not the draft, it's the one that has been approved. It is an Internet RFC.

Unidentified Participant: Which one is that?

Unidentified Participant: It's the one that Leslie Daigle did.

Unidentified Participant: So that's the draft from VeriSign, from September, 2004?

Unidentified Participant: Well there is one that is an approved RFC, I believe, in about that time period and it's by Leslie Daigle.

Unidentified Participant: Let me just make a quick comment that on their previous point about clarity of policy, what we're setting out to do is look at the effectiveness of the policy and looking at how effective it is. That's why clarity is one of the things we're examining, is like how clear is it. And so a lot of organizations don't have formal documentation of policy. It's just a way to examine it and say, is the policy clear to everyone? So I hope that helps.

Unidentified Participant: I want to just expand on that. As an example, many of us work in companies. We have policy documents, policy manuals. When you have a question about a policy, you go to the manual and you read it. Okay? And it's either clear or it isn't, but you know where to go. There is one place to go and it is written down there and it's obvious. And what we are attempting to communicate back to you is, it's not obvious. So I certainly, I won't speak for the committee, I see that as a problem.

Unidentified Participant: But I guess I go back to sort of what Mike Rodenbaugh said, was this isn't an issue of policy, it's an issue of what contractual requirements they have to provide certain types of information which comply with an RFC which you just said is very clear. So -- and in the balancing act, to your point, Emily, the intellectual property constituency has always taken the position, or has historically taken the position, that there is a modality to take care of privacy concerns. The problem we have is that modality is being gained and abused and that through the contracts, the self regulatory framework is not working because they are not enforcing those provisions to make sure it's not being gained. So -- but I don't know -- policy shmolicy, I think we're getting caught up in a lot of semantics. The reality is there are contractual obligations that clearly set out what registries and/or registrars, depending on whether you're a (inaudible), have to apply or provide on a query and whether they're complying with that.

Emily Taylor: I think you're going to be very interested in the compliance questions that we have later on. And I think that probably what we can do is just move to, move through. Because I think we've made the point this, again, is about privacy proxy services, one that you spoke about. How do we get the balance right? Next one. Okay, compliance. How effective are ICANN's current WHOIS compliance activities? And perhaps this is a thought that's imbedded in your previous comment that -- how enforceable are the current commitments? Are there any intractable issues there for compliance? Or do you feel that it's something that ought to work but doesn't?

Unidentified Participant: I think that it ought to work if they actually enforce the contracts. I think in the situations where they have enforced the contracts, and there have been some, not just on WHOIS issues, but on other issues, and it seems to have worked very effectively. The question is, are you actually taking actions? And what I'm concerned about is the fact that I don't believe there is resources, both in staff or in funding, to continue and do the kind of auditing they need to do and then take action. And I think that -- but to your question, I would say this is an organization whose private regulatory ability is based completely and solely on contracts. And everyone continues to forget that. And unless you enforce the contracts, you have absolutely no ability to self regulate.

Emily Taylor: Thank you. Marilyn?

Marilyn Cade: This particular question, how effective are ICANN's current WHOIS related compliance activities? If we're expecting a broad number of people to respond to that, did you provide a backup list that lists what the current WHOIS compliance related activities are? Because there's more than one, right? And I might answer A is working well, B not working well, C -- I'm just trying to figure out the granularity.

Emily Taylor: Yes, please answer the question in whatever way seems most appropriate to you. And if that sounds like a fudge, it's because these are all first attempts to articulate the issues and get them out there for responses from communities such as yours. In fact, the questions oftentimes go on and on and we have got some techs to explain why we got there. But it is intentionally brief. I think our working pattern is going to be to expand on these issues as our work progresses.

Mike Rodenbaugh: Mike Rodenbaugh again. I would argue that the entire WHOIS policy, well not the entire policy, but overall the general policy to the requirement that you have accurate WHOIS information in the database has proved to be unenforceable essentially. Every time -- ICANN gets thousands of complaints a month, basically showing that I've tried to reach these people, they don't exist, it's false WHOIS. And those reports generally go into a black hole 99% of the time. It takes months and sometimes never do you get a response from ICANN. And the reason is because there is no, there are no firm commitments on registrars or registries as to responding to those requests. So

ICANN kind of does its best, it forwards off the complaint to the registrar and registry, but there's no obligation on the registrar or registry really to do anything. And I'm pretty certain that none of them have ever been punished for doing nothing in that regard.

Emily: It may be that some of the compliance team want to comment on any questions of fact on this, because I know that we've got some members here I think.

Unidentified Participant: I'm just going to say I think some of the problems with WHOIS stem from the fact that there isn't any proxy. And I think your first question about how effective is the current policy, it's pretty simple. There's no policy, it's pretty ineffective. And the issues that Mike raised, I think a lot of the problems with enforcement of contracts stem from that fact there isn't a stated policy. And whatever comes out of this work, one of the things that needs to be fixed is that lack of policy. I think that's why we've struggled so much in the past, that that wasn't there.

Kristina Rosette: Kristina Rosette, IPC. I have a question actually about this question number 7. And that is, is there a lot of different ways to look at not currently enforceable? And to the extent that you all have a particular perspective in mind, having some clarification on that I think would be helpful for me. And just to be a little clearer as to what I'm talking about, are you taking about from a perspective of they're not legally enforceable? They're not enforceable because you don't have sufficient contract provisions? They're not enforceable because you don't have sufficient contract provisions and you don't have sufficient compliance staff? I mean just getting a little bit more detail to what you're looking for here I think would be particularly helpful so that we can give you the best answer that would be most helpful to you.

Bill Smith: Bill Smith. I'll answer that in just a second, or respond. I just want to say to folks that generally the review team, what we're looking for is verification for a bunch of what you're saying. We have gone off, we've done a lot of work, we know there are lots of issues. Some of what we're asking for on these things are open-ended questions. So if it isn't effective, tell us how not.

We have anecdotal evidence amongst ourselves. We're asking -- we are doing an evidence based approach, so we need the evidence. We need you guys to supply stuff to us. And on the -- that's okay, we need more of them because otherwise it's just the review team that it is doing it. That's why we're asking these questions, inclusive of the community. On your question on an example, is it enforceable? I would say one thing that I would respond in this, I don't believe that ICANN's current contracts are practically, as a practical matter, enforceable with respect to accurate and available WHOIS information. If you read the contracts and you go through it, and know what is being done on the other side, it's not possible to enforce the contracts.

Marilyn Cade: Emily, I'm sorry, I know we only have five more minutes. We have a 30 minute slot. And so we could run a few minutes over, but we actually have other speakers coming. I'd better apologize about that, my watch is wrong.

Emily Taylor: Could I just -- Kristina, can I just come in on your question as well? Thank you for that. Because I think that there's a huge number of acceptable points on enforceable. Like there's absolute perfection, so you've got 200 million domain names in the world, every single one of them has absolutely perfect data. That's one example of enforceable. Then there is what people could live with. And I think that really we're trying to get a sense of what would be acceptable to the different stakeholders out there in terms of enforceability given that we are all human and living in this world and nothing is actually perfect.

There's always a tolerance level between what you'd actually want in an ideal world and what you can live with. And then when it falls below that, that's when you've got to really do something. And so we want a sense from you about where it is on that scale.

Kristina Rosette: Absolutely, and I'm sure it's no surprise that I would say that as of right now it's kind of, it frankly can't get much worse.

Unidentified Participant: Yes, it can, because there are going to be 500 more of them. I mean it can get worse.

Tony Harris: My name is Tony Harris. I did have some involvement with WHOIS in the past as some people at the table know. And basically I think -- I'm sure you've read it, but there was a study conducted on behalf of ICANN on accuracy which is extremely interesting. The findings on that I think are pretty significant as to the fact of traceability. Basically, I mean when we had this great excitement and introduced competition into the domain sale, the upside was we had very low prices now to buy a domain name. But of course those people who sell domain names make like $1.00 or $1.50 on a domain name. And what are they going to do about validation? You buy a domain name, you go in, you pull in a template. If your credit card checks out, the domain name is yours and it's free. And you could say you're Napoleon and you live on Mars. I mean that doesn't matter. So unless you fix something like that right from the beginning and those who sell domain names can actually do traceability without losing their shirt, that's what the sale has always been in my opinion.

Emily Taylor: Yes, I think one of the aspects I'm interested in is to try and understand the tolerances here. One response would be to validate data on the way in. Another would be to live with what exists at the moment. But if people felt -- I think some of the comments earlier felt that something was being done about inaccurate data when it bubbles up and causes a problem. That's another also sort of response.

Tony Harris: Can I respond to that? Right now you're in a reactive mode. What a registrar would, I think, they used to say at least, is they will react when there's a complaint. But the rest of the data just sits there as is. That may still be the case, I'm not sure.

Unidentified Participant: And the problem I have, Emily, with responding to getting some level of what's acceptable and what isn't, is that it's never the bad guys that are the ones that don't play the game. And that's the problem in trying to put some level in that. I think you can improve the situation, but a lot of the problems that exist create for law enforcement or trademark enforcement come from the fact that people do manage to scoot around this. And the guys that benefit from that are not the ones that are going to be under that level wherever you set the bar.

Unidentified Participant: I would say in respect to your question about tolerances in the room, Steve [Metale] is jumping out of his chair over there, so he wants to talk. But bottom line is there's this really inherent conflict, right? Registrars have tremendous market pressures. They're a very low margin business, they don't want to have any upfront costs. Consolidation is obviously an upfront cost.

If, however, that cost is forced upon them by everybody, I think everyone in this room would be perfectly happy to pay more money for domain names and have that validation done. Nobody in here believes there's a God given right to a $10 domain name, yet everybody in the registrar and registry constituency believes there is and they can't sell them if they have to charge more than that. Well if they all have to charge more than that, then that seems to me, and I think to most folks in this room, it would go a long way towards solving the problem.

Jonathan McCowski: Jonathan [McCowski] with the BC. I just wanted to point out again that WHOIS is a protocol that lacks security, including integrity. So how do you enforce a policy around a protocol that is insecure without addressing the insecurity of the protocol from an integrity perspective?

Unidentified Participant: So if you're referring to the security considerations in the RFC, that is boilerplate that is in every RFC or virtually every RFC. You would have to ask similar questions about email, HTML, HTTP, the web, basically everything on the internet as we use it today except for those protocols that are designed with security in mind. So it's a valid point, but it is not just WHOIS that has this issue. It's the protocols we use every day in our work that have these issues.

Jonathan McCowski: All the more reason that there needs to be cross coordination between the technical level of the Internet and the policy level.

Unidentified Participant: Yes, this is exactly the kind of thing we'd like you to give back to us for this discussion paper. Because as Emily said at the beginning, we don't want to limit comments just to the questions that we formulated. If you have other points to contribute, then I think this would be one. Please submit that and comments for us because I do think it's a valid point.

Marilyn Cade: A question coming in for me -- sorry, I don't know all of your names --

J. Scott Evans: We were in a meeting about two years ago and a very large registrar told the story of how they were talking to their marketing people after hearing some of the complaints about inaccurate WHOIS. And we're very concerned that perhaps they were missing the opportunity to get renewals within their registrar because they weren't keeping accurate WHOIS. And on the record he said, well they said you don't need to worry about that because we have all the accurate information in our accounting department because we get paid. So I think it's a red herring to say that they can't validate. They're getting paid, they're getting their money, and I don't understand why the information that they so accurately rely on to make sure they keep the domains active, they can't use the same technology to make sure that the information is accurate. I think it's a red herring. I don't think we need to put in all this cost. I think they know how to get it, I think they're just not wanting to do it. Because in many instances, bad actors own a lot of domain names and they want to go to those areas where it's easier for them to perpetrate their bad acts because they can hide.

John Berard: That was J. Scott. He didn't identify himself before he started. That's okay. My name is John Berard. I think that the conversation that J. Scott is talking about from two years ago has probably continued on and on. And my last taste of it came from the law enforcement side. And I don't know if you've spoken to the law enforcement folks who have had the ongoing conversations with the registrars about just that and some other issues. As it was posed to me, the mechanism by which the credit card is certified is -- it's Visa, it's MasterCard, it's American Express -- it's somebody else's network. And so the registrar is just relying on the fact that the bank is going to transfer the funds at the appointed hour.

If Elliott Naas at Two Cows in Toronto gets a request from an individual in Singapore to register a dot US address, it introduces, at least as the law enforcement people have said to me, a bit of a complex headache. And just how do you establish the protocols by which you can certify the identity of the person in Singapore and in the same kind of way that you do the credit card? So yeah, I think there probably is some infrastructures that would have to be built. And then of course if it has to be built, it has to be paid for and if it has to be paid for, the question is, who is going to pay for it?

Emily Taylor: Can I introduce Sharon Lemon from the Serious Organized Crime Agency who is our law enforcement representative? You might want to make a comment on that.

Sharon Lemon: Yes, hello, everybody. I agree with everything that has been said. Yes, it is very complex trying to track down somebody. Somebody (inaudible) collection of things from international law enforcement so we can make our contribution. But I can say from our own investigations that people buying domain names on big scales are used -- they know the number so they can get on there with a stolen credit card. So they know the exact number (inaudible) and they've got the domains and their algorithms and they're using them for 30 minutes and they're going on stolen credit cards. So it is a very complex picture that we are collecting from law enforcement.

Steve Metalitz: Steve Metaliz with the IPC. I just wanted to mention -- your work is taking place in an environment of a lot of activity on WHOIS. Much more than there's been for the last several years within ICANN. And I just wanted to mention that you should be aware of these things and they might be reflected in your report. One is that there's an internationalized registration data working group which is studying the question of how do we -- in effect, how do we expand these commitments to the IDN environment? And the existing protocol does not, really doesn't work for that purpose in terms of other scripts. So that is one area.

Second, as I'm sure you know, there's -- the WHOIS service requirements paper that the staff put together at the request of the GNSO about two years ago is now being -- or maybe a year ago, is now being turned into a survey that's going to try to solicit input from the community about what they want to see in the world of WHOIS. And so that's still in an earlier phase and I'm sure you got that paper.

The other item that we learned from reading the operating plan and budget is that during the next fiscal year, ICANN plans to develop a new registration data directory service that will not be limited by the issues that current WHOIS has, e.g., supports internationalized registration data and is extensible to support a wide array of policies, present and future. That's on page 32 of the budget and operating plan.

So some people within ICANN are working on this problem and I hope you all will be in touch with them and ask them to brief you on what they're doing. In all of this murky area about what the policy is and is it enforceable, I think your question 7 is very well worded. What you're about is the commitments that are in the affirmation of commitments. And whether you call that a policy or not, that is what ICANN has pledged to do. And I think as I understand it, your job is to measure the degree to which they are doing that, living up to those commitments. And if they -- if that degree of compliance with the commitments can be improved, maybe there's some suggestions on how to do that. Maybe these technical protocols will have an impact on that.

But I would just encourage you not to get -- in an ideal world, yes, there would be something labeled the WHOIS Policy and it would be clearly communicated, but you have a one sentence description of what ICANN has promised to do and I think that's kind of the touchstone that you should be using.

Emily Taylor: Thank you, that's very helpful. And I think the task of trying to track down all of the relevant documents, all of the relevant work is a bit like trying to catch an octopus. It's pretty difficult. So the point is that you're giving us to what you're finding relevant, what you think we should be looking at, is very, very helpful. Shall we go onto the next slide, just for the sake of a change?

So this slide is looking at what ICANN is doing, and also what should it do to be effective in enforcing its commitments. And do you think that it needs -- one of the earlier comments is about resources, was about both people and money for the combined effort. Could we just have a brief think about that? Anybody want to take the floor on that?

Marilyn Cade: The question of whether we think they -- 8 or 9?

Emily Taylor: Either. What should they do, and do they need any additional power or resources to effectively enforce their existing commitments?

Marilyn Cade: So I chaired -- this is Marilyn Cade speaking, I chaired the first WHOIS task force which worked for multiple years. It was Tony Harris' extremely polite reference to the torture that we put people through by doing a two-year working effort. We did a study, we did a survey, and then we analyzed it using volunteer resources. And we had two 2-hour conference calls a week, including over Christmas holidays. I was extremely popular as the chair. But we did this analysis and one of the things that we proposed at the time, one of our recommendations was that ICANN needs to do a better job of educating everybody in a uniform way about what the WHOIS commitments are. That it needs to be a clear, easy to understand, easy to find, consistent material that is provided to registrants. And we received significant pushback from the registrars who wanted to differentiate themselves in the mechanisms that they use to communicate.

I personally would say one of the problems that still exists today is the lack of clear communication. And if a registrant -- I cannot believe that it is a -- yes, a UN Human Right, to registrar a domain name and hold it. It hasn't made it to the UN Charter yet. But if it's not a right, then the registrant needs to be advised of their obligation in a much more clear way than they are. And I think in a consistent way. And what the consequences are if they don't live up to it.

So it isn't that the registrars aren't telling the registrants, and it's very obscure, different from registrar to registrar, and education and awareness. I think also ICANN needs a lot more willingness to accept the fact it has that obligation.

Emily Taylor: Marilyn, I'm conscious all the time that, as we're going around the different sections of the community, there are people who've been involved deeply in WHOIS work for a decade, the best part of a decade or more. Looking at the situation now compared to when you're working group finished its work, what are the key differences? Do you think the general environment is better or worse? Do you think the same challenges are there? Do you think they're different? Can you give us just a snapshot of how things are? If we're thinking about this aspect -- you were talking about education awareness, consistent communication. Is it better now? Is it worse now? Is it the same?

Marilyn Cade: It's vastly different now because of size and scale and scope. We were talking early Internet, we were talking early days of the web. We were talking about parents who were using WHOIS and school teachers who were using WHOIS and law enforcement who were using WHOIS and businesses to make sure they were dealing with an authentic body. Today, the information -- authentic entity. Today the abuses and risks and therefore the reliance on accurate WHOIS, they're much, much higher. And I think the scale of the heart is much higher than it was.

Unidentified Participant: I think that you need to also consider that one of the problems we've had is there are players in here who are more naïve than when we first started this. They're coming from third world countries where this is new to them. And so you have some innocent problems that they're not educated very well. They're -- when you -- and I think also, one of the problems that ICANN has not been able to get its head around and regulate effectively though the contracts is the fact that about 7 or 8 years ago, market infrastructure providers became market participant. Okay? When we started this in 1998, there was one registrar and one registry. Then there was a registrar and registry that were separate. But all they did was push the names through the system. Except for a few reserve names that were on the reserve list, they didn't own any names. They didn't arbitrage names, they didn't sell them as assets. They just were like a telephone company and they gave you a name and they made sure the name worked.

Well now you have a system where on the registrar level, many of those companies are selling to each other. I mean, you have one entity that has like 100 separate registrars, it's just their name and a number. So the market participation of the infrastructure providers is something that I think has made this a bit worse because it lends itself to not being accurate, not providing, because there's money to be made in just hours of providing the inaccurate information. Just the hours.

Emily Taylor: Could I just ask a question on that very interesting point? I'm not sure, and I'm not loathing this in anyway, I actually just want to know how does it lend itself to inaccuracy? How do you see that working? Because if people are buying and selling, then they also need to contact each other.

Unidentified Participant: No, because they're buying and selling to each other, to themselves. They own and they're buying and selling within their own selves. And the way it lends itself is because it thwarts law enforcement and legitimate owners from finding out what's going on. Even if it only stops them, and you can look at this, Verizon has some very interesting numbers that they have done to their enforcement program where they have actually redirected traffic and look at the amount of money that can be made in hours. So there's where it's incentivized to give incorrect information is because any time you can keep it in the system, in my system, I'm making millions of dollars.

Emily Taylor: Okay, I have a question from -- yes, Sir?

John McCowski: Just a comment. John McCowski. From a -- and I'm not in law enforcement, but from the law enforcement perspective, and also from the business community's perspective, I think it's important to realize the nature in which WHOIS can be spoofed. And people have come to rely on WHOIS for more than it can offer as opposed to querying DNS and understanding the role that IP addresses and blocks of IP addresses play in the Internet space in terms of being able to find bad actors.

So it's just a comment or an observation that I think we need to really think about the policies around WHOIS and make sure that we're not leaving out what's really important. On a cyber crime level as it rises, from a business level's perspective, the fact that WHOIS can be spoofed and what it offers is limited as opposed to querying DNS and understanding about the significance of IP block ranges, etc. Thank you.

Emily Taylor: Thank you for that point. Shall we move onto the next slide?

Unidentified Participant: So I'm not familiar with that. Can you provide an example of a spoof to WHOIS? Are we talking about a whole other database if you went to the wrong --

John McCowski: I'm not an expert in this area, but I do know that to some extent you have to be able to be able to find authoritative in records. And in order to find authoritative records, if you're in old query DNS, and go from the top down -- that's very difficult to spoof. Because IP block ranges are delegated from the top down from our end. But when it comes to WHOIS, and I'm not an expert in spoofing, but it can be spoofed, even when you talk about it on a cyber crime level with credit card data, I mean from the information that can be provided is minimal relatively speaking. So to catch bad actors, WHOIS is not the answer. And it's --

Emily Taylor: Thank you. I think that might lead on quite nicely to the next question which is about accuracy and what steps could be taken to improve accuracy. And are there lessons, are there good practices out there from the CC world that can help us to think about (inaudible)?

Marilyn Cade: As part of our initial work in the early WHOIS task force, we went and interviewed a number of ccTLDs. And this was a few years ago, but subsequent to that the OECD also did the report that you guys probably have. And the interesting thing that we learned was that many countries do authenticate. And I also know that in the sponsored TLDs, the sponsored TLDs require authentication to prove that you belong in the sponsoring community. And our view at the time in the BC was that this was a major positive contribution to use that authentication to make sure this is a real entity, belongs, blah, blah, blah.

I do think that a form of any kind of authentication at all would improve the accuracy. But the reality is that the registrars who take credit cards have all the authentication information. They have accurate, they have the equivalent of accurate WHOIS data or the ability to get that accurate WHOIS contact data because they use credit cards. They maintain apparently a separate database that has all the accurate information in it. So one thing I could do is to basically say that the registrars have to provide the accurate information. It isn't that they don't have it if they accept credit cards.

Unidentified Participant: I think it's important to note that on a cyber crime level, RFC channels, it is very easy to get credit card information. And web sites stay up for days, sometimes seconds. They get moved around between IP blocks. And the nature of the integrity of the data that's given to the registrar has been really meaningless when it comes to what really counts on a very deep level in fighting cyber crime. Because anyone who is engaged in that kind of activity doesn't use accurate credit card information. So what are they verifying except for the fact that they bought some credit card on an RFC channel.

Emily Taylor: Yes, thank you. I think if we sort of take the -- oh, sorry, Sir.

Unidentified Participant: I'm (inaudible) with the (inaudible) obviously. And I would like to add, there is a -- we are supposing that bad actors are not good payers. And this is not a supposition that is founded. And also I would like to add the experience of Brazil with dot BR. There is the validation that is required to have a dot BR (inaudible). It is not difficult as a domain name in the dot BR. I don't know if you have an equivalent in the US of the numbers -- so it would be a social security number, but it is not something to pay the taxes, it's a number that is owned. But even though everybody is recognized and gives this information, it's not checked. It's just junk, the checking that is done. It is that this number exists, not if it belongs to the person that it is saying. So it's wrong also. It gives us a little bit more validation than is done in the GTLD arena, but it's not guaranteed that their efforts will be left out of the domain space. So I think all these law enforcement agencies will have a hard job despite the WHOIS that we can provide.

Emily: Sahed?

Sahed: I just wanted to mention the good work that RISG is doing, they are the Registration Infrastructure & Security Group, and you may want to speak to them about how to deal with and collaborate with law enforcement also. I think there are two different types of bad actors we could sort of speak of. One is the bad actor which does a cyber crime for which you would need to go after the IP addresses. And that's very useful there.

But then there are the bad actors who do cyber squatting and those sort of infringements where law enforcement will only sort of go after them and after IP addresses and take down those websites. In order to do that, it's where UDRP and now hopefully we can do it in RFS, you will need to have accurate and good WHOIS information. So I think the value of the WHOIS record is actually -- both of them are there -- the IP addresses as well as WHOIS record needs to be accurate.

Emily Taylor: Thank you. Any more comments on this one? Steve?

Steve Metalitz: Yes, just to pick up on that, cyber crime is of course an extremely important issue and WHOIS plays an important role in that. But let's remember that WHOIS has a lot of other important purposes other than tracking down the worst cyber criminals. Sahed just mentioned some, and I think, again, there is some data on what people use WHOIS data for. Again, just to find out who they're dealing with online to see which sites their children are visiting, and who is operating those. So those are much less high profile in many ways than the worse cyber crime. That's one of the reasons and perhaps in terms of number of WHOIS look ups that are made, that may be the vast majority of them. And the small cyber crime may be a very small subset.

Unidentified Participant: Yes, just very quickly, (inaudible) from the BC. (Inaudible) assume you're checking some of the different ccTLDs and their systems. Coming from Spain, I remember the days when you certainly had to, to make a domain registration, you had to fill in all the paperwork and really prove your identity. Of course it's been liberalized now, but it might be worth doing some checking at some point and seeing the perfect system from an integrity point of view and looking at the mess from the business point of view of the work involved across the spectrum.

Emily Taylor: As you quite rightly -- well first of all, to answer your question, we've certainly asked the CC community within ICANN to help us and so we'll await their input. I was going to come back on Marilyn's point where you've made it very nicely that since the -- in the last ten years a lot of CCs have liberalized and actually slackened their requirements because there's always a balance between having a healthy database in terms of accuracy and having healthy business in terms of aside. So yes, thank you for raising that point. Shall we go onto the next slide? Oh yes, sorry, we're just going to leave now because we have another meeting at 3:00. I was just enjoying the conversation so much I lost track of time, Steve.

Steve Metalitz: I just wanted to thank you on behalf of the IPC and also thank the BC for sharing their meeting space with us. We really appreciate the opportunity to talk with you. We are going to be submitting responses and encouraging our members' responses to your paper.

Emily Taylor: Thank you very much. And I'd like to in turn thank you all and I really appreciate the joint session with you all today. And please do stay with the process and help us out with your insights and your experience. Thank you.