

20130822_EWG

Michele Neylon: (Audio in progress) the reasons why and if they've got suggestions for alternatives, share those with us. What else? Okay, that slide says questions by 12 August because we actually pushed that out until what's the date in September, ladies? ICANN staff people who have better memories than me? The second week of September I think it is.

Since Durban, just to give you some concept of what's been going on, we have been receiving info. We did talk to a lot of different groups in Durban and since Durban. We're aware that there's a lot of areas that we need to do work on, so over the last few weeks what we've been doing is working in subgroups, sub teams, dealing with specific areas that we felt needed extra work. At the moment what we're trying to do is -- okay, comment deadline has been extended to 6th of September, 2013, at 23:59 UTC. Thank you, Denise.

The -- we've been working forward on this trying to get the final report ready before the ICANN meeting in Buenos Aires which will be held in November. Assuming that we're able to meet that deadline, then the report would be handed over to the ICANN CEO, Board of Directors, and then at some point further down the line, that would then be fed back into the ICANN policy process. It will probably end up triggering several PDPs, policy development processes. And then we've got a bunch of discussion questions which I won't really go into. Those are backup slides which is very nice. I think that's the main job. Do any of you from law enforcement have any questions or anything you need clarification on now or should I just hand it over to Margie?

No problems? Okay, Margie, over to you.

Margie Milam: Sure. Hello, everyone. And in case you're not familiar with the Adobe Connect Room, if you have questions, you have the ability to raise your hand. At the very top of the screen there's the ability to raise your hand if you have a question and we can manage the queue that way. Essentially the reason, first of all we're very happy that Bobby reached out to us, was because the expert working group has several questions for law enforcement and I circulated them yesterday by email. And you can see it pulled up right now. And I'm not going to read them all to you, but I think if you take a look at them you can see the types of questions that the expert working group is really trying to focus on as we try to finesse the recommendations of the report.

Particularly, I think the area where your expertise is most helpful is to really provide us explanation or understanding of how there might be some sort of accreditation process for accessing the system itself. One of the aspects of the recommendation is that various types of users would go through an accreditation process so that they can have the ability to access data in the aggregated system. And particularly with respect to law enforcement, they're very interested in understanding whether there's any work that has been done in your community with respect to accrediting law enforcement or identifying who is considered law enforcement. And I think that's a general area of concern and I think it would probably be best now to open the floor for you all to see if you have any input you'd like to provide.

- Bobby Flaim: Okay, Margie, this is Bobby. Unfortunately I didn't get your -- I'm just seeing your list of questions right now, so I haven't had a chance to review them. I'm just looking at them right now. So I don't know if the other law enforcement on the line have seen them and they have a response to them. But I think I may just have to look at them and --
- Richard Leaning: Bobby, it's Rich Leaning here from EC3. I'm like you, Bobby, this is the first time I've seen these questions and I'm just very quickly scanning them now. Margie, when would you like a response from law enforcement to those 20 questions? Is that by the 6th of September as well or is there a bit more time for us on this?
- Margie Milam: Yeah, that's not tied to the comment period we discussed earlier. This is really more for the various groups to understand the law enforcement's perspective. And I'd like to at least ask some of the expert working group members, the ones that came up with these questions, whether they want to provide more background or explain the questions in any way so that law enforcement can think about this. This is clearly not meant to be something you need to answer today. We do have additional meetings in Washington, D.C. for the expert working group next week. And we can certainly talk about when's a reasonable time to try to get answers to some of these questions.
- Michael, I see your hand is up. Do you want to provide some more background?
- Michele Neylon: I think you mean Michele.
- Margie Milam: Sorry, Michele.
- Michele Neylon: That's okay. It's not that we've never met or anything. What I would say, just with respect to responding to these, rather than you guys trying to answer all of the questions and just kind of working away on this like crazy and presenting us one big reply for every single question, personally I think it would be more helpful if say for example the guys in our CMP go, hey, for us we find that this particular thing, this is our answer to question two or question three or whatever the hell it is. And then if you want to come back again with answers to the other questions later on. It's just -- what I'd be afraid of is that you can focus on trying to get every single, give an answer to every single question, and you might not have very strong feelings about some of those questions, if that makes sense.
- Richard Leaning: Yes, Michele, because some of the questions will be easier to answer than others. From my position, I'm going to have to reach out to 28 member states. And in itself, that is going to be very time consuming in trying to drill down into the data.
- Michele Neylon: Absolutely. That's perfectly understandable. I think some of the questions are probably easy for you guys to answer. We don't know. One of the things we've been trying to avoid is trying to kind of second guess you to kind of think, oh yeah, law enforcement obviously get really, really hands off about particular things. But it could turn out that realistically you guys don't give a damn about that particular data element. It could be something else that we're not aware of.
- Margie Milam: It looks like we've got Interpol Singapore with a question.
- Rebecca Ledingham: We can provide a brief overview. We've seen your questions and we can provide a brief overview to you tonight on particularly the questions surrounding investigations and the steps that are taken and what data that we look to obtain, or Natalie from domain searches, if that's of any use.
- Margie Milam: Yes, that would be very useful to hear your views on that. And then Bobby, did you want to jump in?
- Bobby Flaim: Yes, I'm sorry, I apologize. I'll hit the man on the screen next time. Why -- a question. Why are these ranked in level of importance?

Michele Neylon: They're not.

Bobby Flaim: Okay. So what was the thought behind the question, since it says please rank by level of importance questions 10 and 11.

Michele Neylon: Within those questions, sorry.

Bobby Flaim: Right. So what was the reasoning behind 10 and 11?

Susan Kawaguchi: Bobby, this is Susan Kawaguchi from Facebook. Those two were some of my questions. And it would just be interesting to hear from different law enforcement members if they use some of the elements more than others. And that was my whole idea of asking it in that way. Obviously the whole new structure is important. But I know in just my limited intellectual property enforcement that I use some elements a lot more than others. I'll start doing my research with a couple of different of the data elements and then I'll often times quit, I don't need the rest of it. So I was wondering if that was true for law enforcement also. And if there is something that's of absolute critical importance, like email address for me is probably my number one, it would be interesting to know if that was true for law enforcement, too.

Bobby Flaim: Well the only -- I think I understand the point of priority because I think maybe some of the fields are looked at, but my only concern would be if we start ranking them, then people may get the idea that we may not need the others and may cut them, when sometimes those other fields are actually important to an investigation. If the other fields that we deem are more important are not accurate or false, sometimes some of the other fields provide clues to accuracy or will lead to another point in the investigation. So that's just my only hesitancy in ranking. Because then once you start to rank, people may get the impression that the other ones are either not looked at or could be cut or not shown. That's just my initial reaction.

Susan Kawaguchi: Well we could have an informal discussion about it on the phone here, too, if that's helpful. We are trying to decide what is freely available. And so knowing what's most important to law enforcement would be helpful. But I understand your other concern, too.

Bobby Flaim: Do you want us -- we had, on the US side anyway, we had come up with some things or questions that we had about the paper or the draft. Is it okay to bring those up now?

Margie Milam: Yeah, absolutely. If you've had a chance to look at the report and have initial comments, we'd certainly love to hear them. Then I think we'd also like to go back to -- Interpol Singapore wanted to give us an overview of some of their perspective on some of these questions. But if you feel like you have some thought you'd like to share on the report before we delve into these questions, that sounds great, too.

Bobby Flaim: Okay, whichever you prefer. I don't want to -- whichever is going to work out better. I'm flexible.

Margie Milam: Why don't we go back to the report? I'll pull up the slides because sometimes to answer the questions we might want to refer to those slides. And then we'll go back to the questions after you've gone through your point. Does that sound fine?

Bobby Flaim: Yeah, that's okay by me.

Margie Milam: Okay, perfect.

Bobby Flaim: I guess one of the major concerns that we had was the authentication of the users. Because for law enforcement, I think we've talked about a tiered system, so it is going to be a very big challenge and I did see that referenced in some of your questions. So that is going to be huge for us because in the US alone we have about 20,000 law enforcement agencies. And just one of the concerns we

have is that we may -- if we were going to be -- the FBI who I represent, is going to be selfish. Everyone knows who the FBI is and it's quite easy for us. But we're just concerned about the state and locals and how that would work. So having a closed system by default and then trying to get people into it is definitely going to be a challenge for other law enforcement.

The other thing that we noticed was the validation of the data. So we're just trying to figure out how that's going to fit in with -- we just spent 4 years with the RAA and the RAA for the new one. So we just want to see how that is going to, the new system, will compliment as opposed to kind of supplement that.

Another issue is the notification of the WHOIS search to the registrant. That is huge because if we're doing a criminal investigation and the criminal is notified of the investigation, obviously that's going to run into huge, huge problems.

Some of the other things was having a centralized system who is going to -- you say a third party, but would that not be the kind of direct responsibility of ICANN? Would that not kind of tie in maybe more with ICANN compliance? So the third party issue, that's interesting. And if we can get further details on that, that would be good.

I think that's it from my perspective. I don't know if Terri Stumme from the DEA has anything to add.

Terri Stumme: No, Bob, I think you covered all the things we discussed.

Bobby Flaim: Okay, Margie, that was kind of just our off the top major concerns after we read it.

Margie Milam: Okay, sure. From the expert working group, would anyone like to take up any of those questions and provide more background?

Michele Neylon: This is Michele, I'm happy to if nobody else puts up their hand. Thousands died in the rush. Hi, Bobby, how are you?

Bobby Flaim: I'm good, Michele, how are you?

Michele Neylon: Just dealing with a couple of these queries, with respect to say some of the questions we're asking, it's not a case of us even suggesting that certain elements are going to disappear or anything like that. I think it's more to do with what are the concepts we have of differentiated levels of access. One of the things that we've also been looking at is access for a random punter who just wants some kind of data from the system through to access for a governmental body, law enforcement, whatever. Now in terms of the accreditation type of thing, I can understand that it might be complicated for you, but I'd hope you'd understand that if this system were implemented in the spirit of what we're planning, the overall accuracy of the data that you would be able to get out of us would be significantly better. I mean under the current system, we can argue about this, but we all know that the level of accuracy is flaky at best and that's being polite. Under this system the level of accuracy should in theory be moving much, much closer to kind of 90% plus, that kind of way. I would love to say 100%, but let's face it, that's just not going to happen.

So the idea behind this accreditation of law enforcement and other agencies would be that if you're going to hand over the crown jewels, whatever they are, because there could be a lot more data in here than the data that is currently available to you. In theory. We don't know for sure because we're still kind of working our way through this. Where we'd want there to be some kind of give and take. So the thing is that if you are a genuine law enforcement agency or acting for a genuine law enforcement agency, then you should have access to more data than some random punter who just wants to know who registered a particular domain. Maybe Stephanie or Rod might want to add something on this to explain some of the rationale behind this.

- Stephanie Perrin: Hi, Michele. This is Stephanie and I was just typing something. I think we need to stress at this point that more or less the price of greater accountability on the part of the system and the members of the ecosystem and greater accuracy is more responsible application of applicable privacy law and procedure. That's not to say that registrars in jurisdictions that have privacy law don't comply with law, but the entire ecosystem needs to sort of up its game a bit in terms of how it processes the transparency of personal information. And that's really -- it's not that law enforcement won't get the data elements, but if they normally would be protectable under data protection law, then there may be more process to getting them. Is that a fair description of how we feel about this?
- Michele Neylon: This is Michele. Yeah, I think you're kind of directing some of our thoughts. Rod, are you going to say anything?
- Rod Rasmussen: The -- I guess one of the key things to think about here as well from this concept of accreditation is really more -- it's framing it more as an existing framework of access. In some instances, in many instances we think that access granted to probably the general and anonymous public will probably be sufficient for most of the investigative purposes that you may have. But if it starts getting into some of the data that may be protected or what have you, whatever reason, there may be an increasing level of rigor of (inaudible) and perhaps level there of then going into if you want to get this kind of information, there has to be a way of determining that you actually are a law enforcement person. Being able to determine if you are a person or bonafide law enforcement officer or whoever you are, I think is a little bit different than pre accrediting the entire, every kind of county, every province, every whatever. One of the things we want to understand is how law enforcement can do that today as far as getting a request in from somewhere (inaudible).
- But just in general, how does one go about getting that process done? We don't actually have it in the real world every day, it's not a new problem understanding how it works (inaudible). We also understand that there are some places like Interpol for example where there are some clearinghouses of information so that people can see the communication between law enforcement and how that works and how that might be packaged potentially in something like this.
- That's what I wanted to talk about, is that area, how we go about that.
- Michele Neylon: Thanks, Rod. Richard, you had your hand up. Sorry, I kind of skipped over you. It wasn't intentional, I swear to God.
- Richard Leaning: That's okay. All I was going to say is if we could just wind back slightly, on the question as to law enforcement, Bob's concerns, Bobby's concerns were about the grading if I can call it that, concerns that we would have as well. And investigations are like a jigsaw puzzle. We don't have the pieces in the same order every single investigation. It's the pieces that are available that gives us the overall picture. So I'm with Bobby, I'm not keen on grading information 1, 2, 3.
- Michele Neylon: Well if that's the case then, what I would say to you then is it's perfectly acceptable from our perspective for you guys to come back and say look, we do not want to grade this and this is why. That's perfectly acceptable because ultimately from our perspective, what we want is your input. For you to say, look, this is what we're doing. Now we may think some of the things you might be doing might appear strange to us, we might not like them, but that's not -- that's moot in many respects because we just want to have a better understanding of what you want, what you need.
- There's a couple of other questions that we have there, so don't forget, this is a reboot of the entire system. We're looking at departing from what's there in the past, etc., etc. So in a kind of utopian reality, to quote another famous Irishman, which data elements might you like to see in WHOIS? I'm not asking you to answer that now, but that's the kind of question we're looking at. Would other data be of use to you? Bearing in mind, some putting in their preference for tea over coffee isn't going to be particularly useful in a domain context because we won't know. But are there other data elements that we might be able to put into something. That we might, as registrants and

registrars and others that we might be able to collect, that we have already collected that we could share? I mean another question we're asking you is, if the domain, if you were able to get the domains disabled much more quickly, would you still need the same kind of data that you need now? And maybe in some cases you maybe don't. We're just trying to get you to give us some indication of what you're doing with domains. [cross talk].

Margie Milam: One of the key -- an example would be financial data. Obviously you can't show transfer of funds unless you get access to financial data. From a data protection perspective, that's one of the hardest things to get access to. Banks do not just let you cruise through their system randomly I think. Unless I'm missing something. And we have had discussions about where the financial data would be held and what the threshold would be for getting it. So if you absolutely can't get X types of convictions without a data element such as that, we need to know that so that we can place it in the ecosystem and figure out the threshold.

Richard Leaning: Okay. My second observation and there's a few questions in there, is we, the EC3, could, and I put the emphasis on could, act as the gateway for the cybercrime units, law enforcement within the 28-member states. But once you've had the 28 member states, and not just law enforcement, because this is the bit we're concerned about, is it law enforcement as in police officers? Or is it people or individuals or entities that have been legislated by their own countries to enforce the law? So are we talking like traffic wardens, are we talking litter -- how big is the law enforcement community if we're outside of the traditional police?

But we could act as a gateway for that because that's a unique thing that we could do as EC3. But the spin of that question is, do we know how many inquiries the current WHOIS has daily? And if we do, this third party who will be looking after the new system, when the EC3 for example make a request of the system, how -- I know I'm trying to get into the detail now, but I don't particularly want to, but is it an automatic type thing or would it be a human interaction? And if it is, how long do you wait for the reply? There could be hundreds of thousands of inquiries going in weekly. Now how is that going to be processed? I know that may be too much detail at this very early stage.

And my last point is, and it's a question again, I understand -- I'm just trying to work out the process that you get the comments back by the 6th of September, it goes to the board in Argentina in November, then it goes into the policy process. So what sort of time scale do you see from now to, if everything goes smoothly, for this actually being in place? Are we talking months, years? What sort of time scale are we looking at? And that's me finished.

Michele Neylon: Okay, thanks, Richard. Let's see, you actually asked quite a few questions. In terms of -- that's okay, I just wasn't taking notes as I probably should have done. I'm renown for not being the best at some of these things. Okay. In terms of the timelines, Rome wasn't built in a day and a lot of this stuff is -- we're talking about seismic changes in how a lot of things would be done. I don't think anybody here is going to be confident to give you a firm timeline. But we would be, for the entire thing, you're talking years, not weeks or months. For various aspects --

Richard Leaning: That's what I wanted to hear was that. That's good.

Michele Neylon: Honestly, and if anybody were to say otherwise, I'd have to wonder about their sanity. In terms of the number of queries that WHOIS gets at the moment, since the bulk, the largest volume of domain names are using thin registries, in other words .com and .net, which is where WHOIS data resides with the registrars, there is no central database for WHOIS queries for .com and for .net. So the number, the exact number of queries per day, per hour, or whatever, I wouldn't know and I don't think anybody would know. I'm sure if we were to poll a couple of the largest registrars, you could probably extrapolate from that some kind of figure that would give you some concept of it. Lisa, do you have any numbers on that? Or is what I'm saying correct?

- Lisa Phifer: Yes, that's true, Michele. There are some statistics maintained on the ICANN website, reports from the registries on the volume of queries. But I would point out that that might not be the same as the new system either, but we can provide more concrete answers on what's going on with WHOIS today, but there is no central location and it does require accurate reporting on the part of registries about what they see.
- Michele Neylon: Okay. Thanks, Lisa. Anything else from Europol? Or are you okay for now?
- Richard Leaning: No, we're good for now.
- Michele Neylon: Interpol Singapore. I'm sorry, Margie. Go ahead, Margie.
- Margie Milam: Sure. One of the things I wanted to point out with this chart that we have on the Adobe Connect Room is that to answer one of the questions about accreditation of law enforcement, you don't need accreditation for this. There would be a basic level of publicly available data that is available to anyone and not expressly in our model. And that if you want to go deeper and get beyond what's publicly available, then you would need accreditation. So I just wanted to clarify that because I'm not sure that was clear in the documents and the presentation we made earlier.
- Michele Neylon: Okay, thank you. I see Rod has his hand up and I want to go to Interpol in Singapore. Rod, go ahead.
- Rod Rasmussen: Yeah, two things (inaudible). Without having to be accredited or validated with like biometrics or what have you or maybe even law enforcement and being able to state a purpose and get some more data. That's one of the things that we're looking at. But the other part that I wanted to get back to Richard on was he asked one of the questions we have there is figuring out what kind of agencies would come under the broad law enforcement environment. The -- (inaudible) or are we good? [cross talk].
- Michele Neylon: Your line is breaking up on me. I don't know if it's just on my end.
- Rod Rasmussen: So is this any better?
- Michele Neylon: Yes.
- Rod Rasmussen: Sorry, somebody was programming a microphone. So the point that Richard was asking about, other agencies, it's one of our questions there is what type of agencies would make sense or do investigations that are in terms of policing there, use the registration data for investigations? So for example, in the United States an organization like the FTC, which is kind of a quasi-law enforcement type of agency, at least for certain particular laws, obviously the DEA who is on the line would be another one who looks at particular laws and would be interacting with the system. So it would not just be "traditional police" or even if you can call it a term, traditional cyber police. But anybody who is using the system to do an investigation that would touch on domain registration data. That's my bit.
- Michele Neylon: Thank you, Rod. Interpol Singapore, I believe you wanted to add more detail to something? Or had some questions?
- Kimmo Ulkuniemi: Yes, good evening from Singapore. My name is Kimmo Ulkuniemi, I'm Director of Strategy and Outreach. And yes, we've got questions today, afternoon, and we had some time to go through them just briefly. And if it's okay, we can go through this question by question. Starting from the first question about the accreditation procedures and implementing mutual assistant packs. We think it's in every country there are their own procedures for legal assistance, mutual assistance in these kind of matters. So it would be quite difficult to form one level of accreditation process. But Dick from EC3 suggested that they could be part of the accreditation process. I think that's a very good initiative. On the other hand, we at Interpol, we would have also our secure channels

and now 190 countries. So I think we could work together with the EC3 to have some kind of accreditation process for law enforcement together.

And this number three, so what would be the entities that would be willing to provide a bidding service for ICANN? We think that all the law enforcement offices, they have imbedded already in their home country and it would be quite difficult to provide some kind of bidding service in general for ICANN. So while one solution for that could be that we as Interpol or in the EC3 they would know exactly what contacts are appropriate and which channels those contacts are approaching, Interpol and EC3, which we can then forward to ICANN or registrar.

And yes, just a moment -- are there any amulets which cover access to data such we need them to be holding RDS, #4. Yes, if you mean -- that wasn't quite clear, the question. So while, we didn't know if you mean with the amulets like agreement, bilateral and multilateral agreements, or just amulets to different countries. So that would need to be clarified also. But if it means in general, multilateral agreements, at least in Europe, we have in the European Union and also in Council of Europe agreements on mutual legal assistance which also covers cybercrimes. So that shouldn't be a problem.

On the other hand, mixing operational work with the police and then traditional legal aid, that can be more complicated. So yes, I think that's from the first part and I'll let Rebecca continue.

Rebecca Ledingham: My name is Rebecca Ledingham. I work in digital crime for Interpol in Singapore. I can probably give you a more practical element as to the application of the data that we use in investigations, why we need it, or what it is that's actually most crucial to investigations. The WHOIS data is helpful for as long as it is correct. Quality assurance is probably the biggest issue with WHOIS data. And I think some of your questions are probably overlapping so I'll try and answer them a couple at a time.

From an investigative point of view, in terms of data elements, I agree with what you say about you can't right structure them. However, there are things like name and address, telephone number, email address and creation data or new data are really important. The reason something like creation data is quite important is because quite often domains are registered either on the day or the day after the criminality is first committed. So it's a good way of giving law enforcement a timeline for investigation.

For question 13, if the data in the registration record were for the most part accurate, would that change our needs? It probably would change our needs because quite often we do find the data is inaccurate because there's no quality assurance on the WHOIS data. So therefore if the accuracy was better, then we wouldn't probably require as much detail because we would be able to find who we were after in the first instance.

What type of crime, question 14. We investigate all types of crimes from child protection to fraud investigations that use WHOIS and domain registration data. I'll give you an example of a case that has been investigated that's in the public domain that relates to carbon credit hacking. The perpetrators had actually direct registered a number of domains which they were using as false businesses to contact genuine carbon credit brokers. And we were able to find out when they had registered the website and it tied in with when the companies were contacted. It turned out it was actually registered to India. We were able to get payment information from India with regards to the domain registration.

It's not the smoking gun as WHOIS data and domain registrations, but it's a lot of circumstantial evidence that strengthens a case. And that's why it's so important. So in terms of investigator respect, essentially you are looking to the central ops or max mine data in the first instance to see if any of it is correct. However, I will say that from a law enforcement perspective, my heart absolutely sinks if I see privacy.org as one of the registrants because I know that they have an address in Noni beach which is not real. And there are so many websites that are registered

against privacy.org and they claim to have servers in the Netherlands and then you get bounced back to Russia. And you never find out who is behind the actual domain registry. And they are a big problem for law enforcement.

In terms of question 18, how important is your anonymity or protection? It's really important because quite often, in terms of an investigation, you will need the inquiry of the WHOIS or the domain registrant data firstly. And quite often we will go after the server where the domain is actually registered. We do not want that information disclosed as part of an investigation.

Let me see -- again, the domain registration elements are typically used as circumstantial data in question 16 to back up other pieces of data. So quite often it's used as collaboration for other elements that you have in an investigative case. So I think that's all I've got to add unless anybody's got any questions.

Michele Neylon: Thank you. Does anybody from the expert working group have any other queries, specific queries for law enforcement? Going once.

Stephanie Perrin: Michele, it's Stephanie again.

Michele Neylon: Why does that not surprise me? Go for it, Stephanie. Go for it.

Stephanie Perrin: Just a general question. (Inaudible) on the specific investigations, but can you tell us how much you use the WHOIS data, or should I say you would use it were it to be accurate, for general surveillance and what you might call intelligence crime prevention?

Rebecca Ledingham: I personally, when I'm doing an investigation, I do about 25 look ups per day.

Stephanie Perrin: So I guess what I'm really asking is, would -- how much would you be moving towards automated surveillance using predictive analytics and these kind of things on the data? If, as you say, you can time your investigations based on creation date, then clearly some kind of risk analysis of new domains could be in the future. I mean I'm assuming some resources on that one.

Bobby Flaim: At this time, this is Bobby from the FBI. At this time it really isn't used for surveillance. It's really used for investigative which means past crimes and research. So I don't see it as a surveillance tool. If you're talking about complex investigations where it's organized crime or maybe a botnet and there's algorithms involved in which they create domain names, that could be something that's used or equated into the investigation. But insofar as a surveillance tool, no.

Stephanie Perrin: Thanks.

Terri Stumme: This is Terri from DEA. I'd like to add that in our section we do online pharmacy so we look at thousands of domains a week and we do thousands of look ups per month. Our domains actually - it's random. I mean they go up and down, but there's also some that have been around for years. So the WHOIS data that we look at is actually all important, but we also do reverse lookups, WHOIS lookups, are very important to us. It's the start of our investigation, WHOIS data, and determines who we send a subpoena to. Afterwards to obtain additional information such as who paid for the domain, the account holder, and not the registrant, because sometimes those are not the same. So for us, it's a little different with pharmaceutical affiliate programs. And we do monitor the domains which is helpful. Which is why we use WHOIS so often is that when they do change, we get alerts for the domains that we're looking at.

Michele Neylon: Thank you. Richard, is that an old hand or a new hand?

Richard Leaning: New hand. Just from listening to my law enforcement colleagues, I mean already from very small snapshot of our investigations, we're talking thousands and thousands of lookups a week and that's only from three, four different agencies. One of my questions earlier was, this third party, how are

they going to process the requests from law enforcement when we make the request? Whatever mechanism we use to make the request, the request has been made, how is that third party going to process and get back to us the results?

Michele Neylon: Thank you. I'm not actually answering that because we haven't got that answer to some of these questions, Richard. I mean, the thing with a lot of this, as we've been trying to do, it's working on a framework. We're diving in to a certain degree in some areas, but not in others. I don't want to tell you one thing and then discover that in five years' time the system comes at the far end of a process and it's completely different. Margie and then Rod.

Margie Milam: Yes, this is Margie. I wanted to first provide additional information on the particular issue with regards to privacy services. Part of the recommendation that the group is working on is trying to identify the principles and standards for privacy and proxy services. And that's part of what the expert working group is spending some time working on. But I also wanted to point out that that work is also being done because of the recent adoptions of new provisions in the 2013 registrar accreditation agreement that just got approved by the board in July. As part of that, there's a new specification about privacy and proxy services. And so I just wanted to let you know that there's a lot of work being done both by the expert working group in terms of the future service, but also in conjunction with the current service to try to deal with some of the issues that everyone has seen with respect to the privacy services and the ability to not get information.

Michele Neylon: Thanks, Margie. Just actually on that note, with respect to the 2013 RAA, the way that those contracts work, it means that all ICANN accredited registrars will be on the 2013 RAA at the latest by 2017, it's a 4-year contract. Is that right, Margie? Or am I missing something?

Margie Milam: I think that's right. I don't know the exact outside date, but at some point most of the registrars are moving over. And most of them sooner because of the obligation if you want to sell new gTLDs, you have to be on the new agreement. And ICANN trying to find a way to bring on the registrars sooner than that.

Michele Neylon: And my comment on that is please don't poke the beast. Rod, go ahead.

Rod Rasmussen: Responding to Richard, most of the queries I assume are still going to be answered in real time. Then beyond that, we're looking at ways of providing mechanisms so that you have some sort of pre-validation, pre-accreditation, what have you, that you would also probably get a real time answer. But there may be a path where if you aren't accredited or you're asking for something that needs to be accessed in a different method, where you would get an asynchronous response. But I think the intent is still to have real time access to the data. That actually provides for an interesting path that I actually hadn't thought about where you might -- I'm seeing the microphone ping again, can you guys hear me?

Michele Neylon: Yes, we can.

Rod Rasmussen: But that allows potentially for a path where you may have a request come in from a non accredited type person or unknown entity that claims to be law enforcement where you can then delay your answer until there is a process where somebody can slow down the chain and see, okay, this is a legitimate request from a legitimate police officer or what have you. So that might actually be a really interesting path to look at for some of these data elements or someone first accessing the system or something like that. Thanks for that input.

Michele Neylon: Thank you, Rod. Thank you, Richard. Susan, go ahead please.

Susan Kawaguchi: Thank you. So I'm wondering how important is for law enforcement the investigations that non law enforcement do in cases and then deliver them to law enforcement. So we have a pretty big team at Facebook that investigates issues that go on on our sites, (inaudible) and fraud. And then I know we work with law enforcement very closely. So those teams need the same access almost as

a traditional law enforcement. I was wondering how important those investigations are to all of your work.

Bobby Flaim: This is Bobby from the FBI. Actually organizations like that are extremely important because a lot of times the information that we get from the outside community in particular organizations like that, are critical to starting investigations or getting other information such as yours, such as Rod's with Internet Identity, such as Spam House. There's lots of other organizations out there that are non-law enforcement that are key and critical to the whole industry of solving domain name abuse. So that is something that is very important to law enforcement and that's why with the validation and who's going to be in the closed system is actually an important question for law enforcement in and of itself but also our partners.

Susan Kawaguchi: Thank you.

Michele Neylon: Okay. It's now ten past four in my time zone, which is the only time zone I really care about. For others, it's ten past the hour, whichever time zone you're in. Are there any other issues or queries from either members of the expert working group or from our law enforcement guests?

Faisal Shah: Hey, Michele, it's Faisal. I just have a real quick answer to one of Bobby's questions. I think, Bobby, you were talking, you were asking about the management of the RDS? And I just wanted to point out that it's going to be similar to the trademark clearinghouse where ICANN will contract with a third party and I think the clearinghouse, the contract is IBM and Deloitte, so it will be very similar in content to that with the compliance hammer being (inaudible). So I thought I'd clarify that.

Michele Neylon: Thank you, Faisal. Okay, anybody else have any comments or anything else you want to add or any other questions for either side?

Terri Stumme: This is Terri from DEA. I'd like to point out another concern we had was any cost associated that might be associated with the new system is something that would be of concern to our government.

Michele Neylon: Okay, thank you. Just one query though, I mean if the data you are able to access was significantly more accurate, would that, would the potential cost still be an issue for you?

Terri Stumme: Yes, Sir.

Michele Neylon: Margie, go ahead.

Margie Milam: One of the things I wanted to follow up on was very interesting comments about Interpol and I think it was the EC3 perhaps working on how to identify law enforcement. I think that your expertise in that area is very important and to see if there was a way to perhaps follow up on that particular topic at another time. My thoughts were since we have our meetings next week in Washington, D.C., and Bobby and I had talked about whether it might be appropriate to have some of that time be to follow up on some of these law enforcement issues, my question is, would that be an appropriate topic for some follow up in Washington, D.C. next week?

And Bobby, I don't know if you've had a chance to confirm whether there's several of you that are available to meet either Wednesday or Thursday next week. Either remotely, we can set up a conference call, it doesn't have to be in person.

Bobby Flaim: Yeah, I did send out the notification to all the people that were on that email list. So I don't know, they haven't let me know if they're available. I'm available, so I plan on being there. But maybe the ones on the phone now can -- I think Dick Leaning said he may, from Europol, said he may call in. I'm not sure about Interpol or the others.

- Richard Leaning: I can call in. Unfortunately I won't be able to make the meeting in person. It's in Washington, but it's not in Europe, so the chance of me being there next week are nil. But I will definitely phone in. And on that, just on the meeting, the face to face meetings, is that the only face to face meeting you're going to be having with this type of topic? Or are you intending to hold similar face to face meetings in different parts of the globe that we can find it easier to attend rather than flying to the States?
- Margie Milam: I don't think there's been any plans for that, but that's something we could certainly explore if there is a reason to have a meeting. I think that's something we would probably take back and consider, but at the moment we don't have anything scheduled with respect to that.
- Kimmo Ulkuniemi: From Interpol, it would be possible for us also to call in next week.
- Margie Milam: It would be possible?
- Kimmo Ulkuniemi: It would be possible to call in next week. I think it's not possible to attend a meeting in person on such short notice.
- Margie Milam: Right. Okay. So I'll try to work with Bobby on what the best time for that would be. But I think that exploring further the issue of law enforcement accreditation and how to identify law enforcement I think is probably a good issue given the kinds of work that the expert working group wants to follow up on. I guess I'll ask the group, do you expert working group members, does that seem like a plausible use of our time?
- Michele Neylon: And thousands died in the rush. Stephanie agrees. She's put up, she's given us a positive tick.
- Margie Milam: Oh, that's right, use your little signature boxes on the right.
- Michele Neylon: Faisal agrees, Rod agrees. Does anybody dislike the idea? Okay, I'll take silence -- they all love the idea because they haven't bothered saying otherwise. So just work on the basis that they all love the idea. Richard, also Richard, if you or any of your other European colleagues have any concerns or queries or anything else you want to talk to anybody, there's a couple of us within the EWG who are in time zones that are more, what's the word I'm looking for, civil? And you wouldn't be very good law enforcement if you weren't able to find my contact details. But myself, Michael, who else is in Europe -- Jean-Francois some of the time. What's her face, Nora. I think that's about it. We're all on either Irish/Dublin -- well Dublin/London time or Central European time. So if any of you want to query us about things, you always can.
- Richard Leaning: Thanks very much for the offer. There's no immediate rush for it but I can say as this issue progresses over the next months, years, that face to face meetings with the law enforcement community of the EU would be something good and if we can get countries there who themselves would have a diverse view on WHOIS and what they would like from it. So sometimes it's a better dialogue when everyone is in one room rather than having 15 law enforcement officers trying to stick their hand up on a teleconference.
- Michele Neylon: Okay, thank you. Does anybody have any other issues they want to raise at this juncture or shall we wrap up the session with law enforcement? Because I'm aware of the time. We've still got one or two items we need to deal with internally I believe. Okay, I will take the silence to mean that you're all happy and at this juncture I will thank the law enforcement for joining us on this call and we look forward to discussing with some of you in person next week or via other communication methods. And of course if any of you have any further input, queries, questions, need clarification on anything, you can reach out to either us individually or as a group. And as previously stated, if any of you have difficulty finding contact details for any of us, I'm sure others within your section of the world would be able to help you with that. So I'm going to hand this over now to -- we're going to dig through some stuff internally within the group, so thanks to law enforcement again.

Thanks guys, and leave you go. Charla, you wanted to talk about logistics for our meeting next week in Washington, D.C.

- Charla Shambley: Yes. There's -- Alice was kind enough to send out another email with details on office locations, hotels and each of the meetings, dinner locations, etc. If you have not received confirmation on your hotel, Michele and -- well I think you're the only one, Jean-Francois as well, but I think you're the only one who needed follow up from the hotel. You should have received that by now?
- Michele Neylon: I did, yes. Thank you.
- Charla Shambley: Okay, great. Other than that, the appointments for the sub teams should be on your calendar and then invites to those groups' Tuesday working sessions. Anyone have any questions on D.C.?
- Michele Neylon: What's the weather going to be like?
- Charla Shambley: I don't know yet. I haven't looked at the forecast.
- Michele Neylon: I'm shocked, disappointed and depressed that you don't know this.
- Charla Shambley: I'm not packing a suitcase, so --
- Michele Neylon: You're not packing a suitcase? What are you going to do, you're not going to wash?
- Denise Michel: Michele, your question assumes that we're actually going to let you outside rather than in the conference room working. So bring an umbrella.
- Michele Neylon: Okay, bring an umbrella. Thank you. Denise, I made sure of this I would have non ICANN time while in D.C. So I'm not flying over, doing EWG, and then falling out of bed the next morning and jumping on a plane.
- Denise Michel: Good for you. Do we have anything else we'd like to follow up on before we close the call?
- Michele Neylon: You may have noticed in your inboxes there was a barrage of emails from Cathy Kleiman and her cohorts who are a subgroup of the non-commercials. They have submitted a number of comments and queries on a variety of aspects of our work to date.
- Charla Shambley: (Inaudible). So give some thought to whether or not you think we'll actually have time for that when everybody has had a chance to read that input and can appreciably discuss whether it would be feasible to meet with a couple of them in D.C. next week or have a phone call or whether we should just handle the response like we are handling the other inputs to the working group. So we'll give team members a chance to look at that input perhaps and sent out an email Friday or Monday. Would that work?
- Michele Neylon: I'll say potentially since everyone is rushing to answer as usual. Michael was saying on the chat it would be good to meet them. I'm not sure if that refers to LEA or the non-commercials. Michael, are you talking about the non-commercials or the law enforcement?
- Michael Niebel: Non-commercials and law enforcement.
- Michele Neylon: Okay, so Michael's being very sociable and wants to meet everybody.
- Charla Shambley: Okay, well let's -- we'll look at the schedule and follow up online and see if there is something that we can work out for both groups.

Michele Neylon:

Okay. Just one question, I'm just asking this because somebody was stupid enough to give me control of this, so I decided I was going to ask questions. I know that Susan won't be in D.C. Is there anybody else who – (audio ends abruptly).