COPENHAGEN – ccNSO Members Meeting Day 1 (pt 4)
Tuesday, March 14, 2017 - 17:00 to 18:30 CET
ICANN58 | Copenhagen, Denmark

PETER VERGOTE: Good afternoon, ladies and gentlemen. Welcome to the legal session from the ccNSO, the last session of today. I can see already from the people attending this session that it's the last session standing between you and the ccNSO cocktail, so we're going to do our very best not to overrun our time.

This is going to be a slightly other format for the legal session. As you probably know, for legal sessions we don't pick one kind of team. We pick a number of presenters, and they have time to share their information with you.

What we are going to do now is we're going to put it into a bit more of an interactive mode. We're going to do a panel-style session with one team to focus on. It's law enforcement in the DNS.

We are going to look at it from a multi-perspective, in a sense that we are going to have three presentations from ccTLDs across all ccNSO regions. We are going to have the point of view from the registrars and the point of view from law enforcement.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

For the TLDs, we will have Rosalia Morales, if we are able to track her, from .cr. We have Geo Van Langenhove from .eu, who is going to start off with his presentation within a minute. We have Debbie Monahan from .nz, and then we are going to give the floor to Ben Butler from GoDaddy, who will give us the perspective and the [end take] from a registrar point of view. Finally, we are going to give the floor to law enforcement, to Chris Lewis-Evans from the U.K. National Crime Agency, to inform us on his point of view.

Now, how are we going to deal with it? Well, the presenters have a maximum of ten minutes to make their points. Then, after each presentation, we have about time for one or two questions that pop up out of the audience. Then we shift to the next presentation.

I assume that, after the five presentations, we have still plenty of time for debate and discussion. If you then have questions, whether they're specific for one of the presenters, whether they are more generic for all the presenters, please fire at will.

I have some questions as well that I can use to kickstart some debate. I have some questions that can involve you in showing your cards to get the temperature of the room. We'll try to wrap up, and if we come across something that we can take away for

future sessions or to further work on, then we are going to do that as well.

Without further ado, Geo, you're up. Please go ahead.

GEO VAN LANGENHOVE: Thanks, Peter. Good afternoon, everyone. My name is Geo Van Langenhove. I'm Legal Manager at the .eu registry. I'm going to give you a little bit of insight on what we do at .eu and requests from law enforcement.

LEA stands for Law Enforcement Authorities. We get requests from them to take down domain names, to redirect domain names, to seize domain names, and so on and so on. We basically categorize them in four categories. To start, we have a very good collaboration in Belgium. We are Belgium-based with the Belgian customs. They have a specific, special cybercrime unit to seize goods at customs. They see a lot of not only .eu but a lot of websites that are counterfeit; rogue pharmacies and all the other things that are abusive.

We have a collaboration with them. In the old days, they asked us to take down the domain names. We said, "No we can't because its content." You know the discussion." So what we said is, "But what we can do is verify the registration of the holder of the domain name. If it appears to be inaccurate or incomplete or

incorrect or whatever, we send a notification to the holder. If they don't respond to it in two weeks, we have a case and we can close the domain. We take it down," or suspend it, or whatever you want to call it.

They were happy with that procedure. Why? Because it gives them to the time – those two weeks – to start making their case. They want to assemble as much as evidence as possible. While collecting the evidence, our investigation runs, and in the end, if the holder appears to be a fake registration, we just suspend the domain. You won't believe it, but there are abuses with counterfeiting on a website where people say, "No, no, no, no. it's really my domain name. Here is my ID. Here is my telephone number. Here is my real address." We send it over to customs and they go and arrest individuals.

We also have similar collaboration with the Belgian Ministry of Economic Affairs, not on counterfeiting only but on copyright and piracy, mainly. It's exactly the same procedures, so there's no need to explain it again.

We also have the – I'm going to start with the court orders, of course. That's what every registry says, "Give me a court order." Of course, that's the same here with us. If you have a court order, we'll take it down based on the court order.

Now, the very specific case in Belgium is the public prosecutor. Until 2014, if the Belgian public prosecutor asked us to take down a domain name, we refused because we said that there is not legal ground for asking us to take that action. So there was no legal ground for the public prosecutor.

We were lucky in that, in October 2014, based on another case with a Belgian ISP, there was an Article 39bis of the Belgian criminal code that was invoked by the public prosecutor, which is the same article that they based their request on when asking us to take down the domain. That Article 39bis was part of a court case before the highest court in Belgium, the Court of Cassation. And what happened? The Court of Cassation decided that Article 39bis of the Belgian Criminal Code indeed is a valid ground for a prosecutor to ask anyone to take any technical measure that he or she deems appropriate, including taking down domains.

So since October 2014, if we have a public prosecutor asking us to take down a domain name, of course based on that article and that article only, we take it down.

Of course, with law enforcement authorities' requests, we have some issues that I think we're not the only ones having them. First of all, there's the jurisdiction. As you all know, there is a legal system in each country, so the jurisdiction is only within

those territories and those boundaries. The questions are still open on what to do with foreign court orders and what to do with foreign law enforcement requests.

Let's say that one of our neighboring countries – the Netherlands or France – has a prosecutor asking me to take down a domain name. I'm not going to do it, but of course we have the alternative procedure for registration data checks.

The legal grounds? This was Article 39bis of the criminal code. So far, I have not seen any other legal grounds that really entitles a registry to take down domain names. There might be legislation coming up, but the legal grounds are always the big question.

We also have problems in the syntax. Luckily we don't have that anymore because we, let's say, hold hands with the prosecutors when they are writing the requests. But we used to have requests saying, "Take down the domain name www.___.eu." Then you need to make a decision. Do you mean the domain name, so everything? Or do you only mean the website and then you don't need to address it to us but to someone else – a hosting provider, ISPs, registrars?

We also have incomplete requests, "Redirect it to the stop page of the government." I have no clue what the stop page of your government is, so please be a bit more specific.

One of the special treatments we have as .eu being under the concession agreement and the regulation of the European Commission, it says that .eu is only to be registered by people or companies or associations who have residence in the European economic area. That means the European member states plus Lichtenstein, Norway, and Iceland.

So in case of a court order for transfer, we need to consider if, for example, an ADR decision says, "Oh, we have a complaint from an American company against a .eu domain name. Indeed, the legal grounds are correct, so the domain needs to be transferred to the American company." Well, in that case, we cannot execute the transfer because it would be against the regulation.

Just to give an example, this is, in French, the public prosecutor that we request. You see the article referenced. You see that "saisie" means seizure. "Rediriger" means redirect. It was addressed to DNS.be. and EURid ASBL. We happen to live in the same country, so this could be a copy that either DNS Belgium or we receive. This is about – I left the domain name to make my point, which is abercrombiefitchbrussel.eu. When we took a look at the registration data, we found indeed that all the things that you could expect but the correct data.

Then you see that, indeed, there are the name servers referenced and the IP addresses, so we could execute on that

one. Of course, this is then the result. If you go to that specific website, you will see in all our sites a collaboration and fighting against abuses that appear on that website.

When you take a look at – in this case, I had to take another one because the other one was seized: louisvuittonhandbags.eu – one of the domains that had been seized and redirected to that stop page, you see that what we do in our database, because we need a technical infrastructure to seize that domain name – now, in seizing a domain name and collaborating with a registrar who will then do the seizure – I'm not going to say that you can't rely on registrars; of course you can – the thing is that you need control on the domain name. So instead of registering via a registrar, the seizure happens via our so-called registrar account, which is a pure technical account, to make it happen. So we put the domain on our registrar account and we make the registrant or the domain name holder be the public prosecutor, upon their request, by the way. So we asked, "Who do you want to be there?" and they said, "Oh, it has to be us."

This is my final slide. These are some examples. You see 2014. In October, we had the court case. Before the court case, we had zero. After the course case, we already had 22.

In 2015, we had 353 takedowns. In 2016, we have 2,306 based on law enforcement authority requests. So it's not only the 39bis – I

have to say that – but it's also based on our collaboration with the Cybersquad team of the Belgian customs and the Ministry of Economic Affairs.

If you have any questions – am I taking them now, Peter? Or after the session?

PETER VERGOTE: Okay. Thank you very much, Geo. As I said, we have time now for a couple of questions that you would like to pose specific to Geo. Or you could actually wait until we have gone through all the presentations as well.

Are there any urgent questions for the time being?

I don't see any, but I have one, Geo. Because the last slide was about figures and I saw a sharp incline in the number of cases, would you happen to have an explanation for that? Is that because your level of interaction with law enforcement and the like is getting more intensive because they better know and better understand how you operate? Or is it just a kind of natural growth, like how you have natural growth in registrations?

GEO VAN LANGENHOVE: I can't say why they do it, of course. Maybe they see more abuse. I can say that the more you collaborate, of course the more you get. So indeed it's an improved interaction. That's one thing.

Of course, we're here to help them. We want .eu to be a safe and trusted space. If we really want to make ourselves credible, we need to collaborate with them, to the extent legally allowed, of course. If you give a good response to them if they ask you anything, then of course the likelihood that they come back to you is very high.

PETER VERGOTE: Okay. Thanks, Geo.

GEO VAN LANGENHOVE: I also had a question in the back, Peter.

PETER VERGOTE: Oh, okay. Jorg, please go ahead.

UNIDENTIFIED MALE: Shout.

PETER VERGOTE: Is the mic here in front working? Or else come forward and use the mic over there.

UNIDENTIFIED MALE: Here is a mic as well. You can come sit next to me.

JORG SCHWEIGER: Ooh. Scary up here. Jorg Schweiger with DENIC.de. I would be interested to get some more information about how you would deal with what I would call collateral damage. You've taken down a second-level domain and, by that, taken down a third-level that is completely legitimate. How do you deal with that?

GEO VAN LANGENHOVE: So far, we haven't had any collateral damage, so I can't answer that.

JORG SCHWEIGER: Are there any plans for how to do it? Or do you just scrutinize each and everything so fantastically that nothing like is ever going to happen?

GEO VAN LANGENHOVE: If it's the public prosecutor asking us, we're out of liability. So it's not our liability/responsibility. That's clear.

If it's our own takedown, we say, "Okay. We have reason to believe (and that's our notification to the holder) that your

registration data is inaccurate. Please provide evidence and update your data. If you don't come back (we always say that in notification) in two weeks, we suspend your domain." So suspension in the .eu space means it's still registered with you but it's no longer functioning.

If they don't come back, it's down. If they do come back, of course the deadlines are less restrictive and you start negotiating and so on. But we do have the case where we do suspend a domain based on bad registration data, and the in the end they say, "Oh, but it was the wrong data. Here is the correct data." If they update it and it appears to be correct and they provide evidence, we put it back online.

JORG SCHWEIGER: But the main message for me was that liability lies with the prosecutors when they give you the data, which is very [inaudible].

GEO VAN LANGENHOVE: Well, if it's based on Article 39.bis, it's clear. A Court of Cassation in Belgium says they have the authority to ask you to do that. If you do it, it's a pure execution of a law enforcement order.

JORG SCHWEIGER: But it's not a court order. It's just –

GEO VAN LANGENHOVE: No, but I would say it's similar.

JORG SCHWEIGER: Interesting.

GEO VAN LANGENHOVE: It has the same degree in Belgium as –

PETER VERGOTE: The same also applies for DNS Belgium of course. The difference is that it needs to come from a magistrate, so either a court order issued by a judge who is a magistrate or somebody from the public prosecutor's office who is also a magistrate. So this person does not belong to law enforcement but to the judicial power.

JORG SCHWEIGER: Okay.

PETER VERGOTE: So it means that, if a magistrate gives you an instruction and you carry it out, your liability is overtaken by the competent

magistrate that [filed] you the instruction. If whoever – because we do same as EURid – if you carry out something that has been notified by Cybersquad or the Ministry of Economic Affairs, you don't do it based upon an instruction of taking down but you operate based on your terms and conditions. You say, "Okay. I'm going to follow my procedure that I follow in case of bad WHOIS." So I think you have a bit of liability there because you could make a judgement error as a registry. That you need to calculate in.

JORG SCHWEIGER: Okay. Thanks very much.

PETER VERGOTE: You're welcome.

GEO VAN LANGENHOVE: Thanks.

PETER VERGOTE: Okay. Let's move over to our next speaker. Rosalia, who is going to present us the state of affairs in .cr. Over to you, Rosalia. By the way, we're happy to have tracked you so that our panel is complete now.

ROSALIA MORALES: Hi, everyone. I'm Rosalia from .cr from Costa Rica. I'll give you our experience in domain takedowns and our relationship with law enforcement.

For a little background, .cr has about 22,000 domains, and we've been operating for 27 years. Since 2014, we changed our policies for takedowns. Before that, we used to be very conservative in all our registrations. So if we identified any trademark that we being registered that was not being registered by the company itself – by the official owner of the copyright – we would not register that domain. Also, we were very, I think, to some extent, subjective. When identifying a domain that had bad faith in their content, we would not register it either.

Eventually, that proved to be a very difficult process, where we did not have the legal knowledge or the expertise to make most of the decisions. We decided to leave this decision on judicial and court orders locally. As such, these are our current reasons for taking down a domain.

Of course, if a title holder requests that they don't want a domain name anymore, that's definitely one reason. For non-payment. Instruction from the Court Justice of the Republic of Costa Rica – that is very similar to what Peter was recently talking about. It functions very similarly in our country as well.

So it's either a judge from law enforcement or any judge from the judicial power who can send that.

Also, we have our URDP process. Whenever we get instructions from WIPO or a similar process from a local arbitration and mediation center from Costa Rica, we also follow their instructions. We do not allow any other unauthorized commercialization of .cr, so if someone is doing that in some kind of illegal manner, which hasn't happened, that would be another reason for elimination.

When it comes to erroneous or false information, we also ask for court orders. In the past, we used to take that on ourselves as well before 2014. It also proved to be very hard to identify when a registrant was actually providing fake information, so we decided to leave that to the expertise of the courts.

The only exceptions are when a domain is going through a new RDP process, through a process in the WIPO, or through the local mediation process.

We work a lot with law enforcement, especially in the last five years. We have a very good relationship with them. Currently, as we always ask for a court order, we based this on the idea of the Tunis Agenda for the Information Society in 2005, where our local and state law in above international law in Internet-related issues. Since this is such a well-known international agreement

within the Internet space, it has proven to be very useful in applying it to our policies and our justification in asking for court orders, which I will eventually expand [on].

Whenever we have cases of intellectual property, brand registration, crimes: drug trafficking, child pornography, etc. – all sorts of crimes – we always ask for a court order. Our response to law enforcement is immediate. Usually we are aware of the situation beforehand due to the close relationship with have with law enforcement locally. We provide they information they request pretty easily. It's usually very clear what they need, and the process is very efficient.

Also, whenever we deal with cases involving URDP processes and conflict resolution related to domain names, then we follow the process according to our policies for WIPO and for the local arbitration organization.

We have a very low case of taking down domains. Usually, for the last six to seven years, we've had one or two domain takedowns per year. Most of them have been for fraud and child pornography from different criminal investigations done by law enforcement.

The first case we've had of copyright infringement was in 2016 with KAT. I don't know if I should say what it stands for. It's not

bad words. I don't know if you've heard of it. It's a well-known torrent service.

In 2016 and still in 2017, we've been dealing with Pirate Bay as well. Those are the new cases. The process has changed significantly. I will expand on it in the next slide.

The good relations we've had with law enforcement have made these takedowns very smooth and the communication has improved throughout the years. It's really good communication, which has even led to us to do trainings locally related to the issue. We also train different law enforcement officials as to the usual cases that we've gotten throughout history and how we've managed them. Even their team has managed it in the past, and it has proven to work effectively, and our relationship keeps improving.

This should say 2016, not 2015. As I mentioned before, we received our first case of copyright infringement, which was part of a global operation of different ccTLDs which were approached at the same time with a court order international case to take down the domain for KAT.cr, in our case. It was the first time we started to feel there was international pressure, other than the law enforcement involved in taking down a domain. This has only increased in 2016 and 2017.

With the new case that we're currently handling, which is Pirate Bay, we've had about one-and-a-half years of pressure from the U.S. government, particularly the U.S. Department of [Commerce], asking us not to follow our policies, not to follow our court order, but to just take down the domain without the procedure that our policies clearly state and have stated for many years now.

We have received help from other ccTLDs. Particularly, .ce has helped us a lot. They've had great experience with Pirate Bay in the past. It has been a very delicate situation locally because the U.S. Department of Commerce has involved other players locally to pressure us in taking down domains.

The interesting part is that law enforcement supports us throughout the process. However, the pressure still exists. This is a new experience for us because usually, as I mentioned, it was pretty much a process that we knew how to take care of. Our communication was great, and then all of a sudden we're having a situation where the pressure is different. The conversations are different. We feel that we're just getting extreme pressure not to follow our current policies or respect the local law.

We have decided not to bend to this pressure and stick to the Tunis Agenda. I would recommend everyone in the room who would ever be in the same position and might be to do the same

because that takes the dialogue away from a local debate or conflict to a global scale, and it's easier to handle the negotiations.

Throughout this process throughout this year-and-a-half, we've received harsh criticism from particularly the U.S. government, criticizing the ccTLD community because we have different policies, which I think is no surprise. But they seem to be upset about that, particularly the fact that it's very different when it comes to taking down domains. Whenever they ask for documentation from the ccNSO about this and there is no documentation available, they have been very clear in interpreting this as some kind of subversive behavior or that we're doing this on purpose because we don't want to provide information because we know we're guilty to some extent.

That is, I understand, a manipulation of information and also a way to exert pressure on us, but it has been hard to come up with best practices when we lack documentation that justifies that what we're doing is not exceptional.

In the case of PirateBay.cr, there are many other Pirate Bay domains in other ccTLDs and generics – about 70 or more. It's a well-known industry of torrent and copyright infringement. However, locally the pressure has been to focus on .cr itself and

make it seem like we're an exception to the rule by asking for a court order and working together with law enforcement.

So it has been a complete switch from the usual relationship we've had in the past. I think the pressure will increase with this current administration. I just want to leave this message with the community: Beware: Many of us can be a victim of Pirate Bay or any other of the many torrent domain names. There seems to be a clear agenda into exerting this pressure.

There are exceptions. We have currently received the case of Peru and Guam, who seemed to eliminate the domain a few days after receiving the demands from the U.S. government. They tried to make it seem like we're no cooperating.

So I recommend sticking to the idea of the Tunis Agenda agreement, as I mentioned in the past, so that it seems that we as a ccTLD community are following the best practices and what has been agreed on internationally in the past.

I think, with that, that will be the end of my presentation.

PETER VERGOTE: Okay. Thank you very much, Rosalia. Any questions from the audience for Rosalia?

Okay. Please come on up. Go ahead. Thanks.

[KRISHNA RAJAMANNAR]: Okay. Good evening. I am Krishna, Legal Officer for the .in registry, the ccTLD of India. I'm also doing this quite similar work as you are doing. If you can run down the slides for a moment from the beginning, I have just two or three questions on your slides. Please.

ROSALIA MORALES: Yeah, sure. Go ahead. Which one do you…

[KRISHNA RAJAMANNAR]: From the first one.

ROSALIA MORALES: The first one? From our policies?

[KRISHNA RAJAMANNAR]: Yes, this one. Regarding the current reasons for taking down a domain, the first point is: title holder's request.

ROSALIA MORALES: Yeah.

[KRISHNA RAJAMANNAR]: Which means, if I understand, [inaudible] has the right to be like a company having a trademark or something, they approach you. Is that so?

ROSALIA MORALES: Yeah. Sometimes the owner of a domain does not want the domain anymore for whatever reason.

[KRISHNA RAJAMANNAR]: I understand that comes under UDRP. I think you must have. That comes under UDRP.

ROSALIA MORALES: The what?

[KRISHNA RAJAMANNAR]: A similar process like UDRP.

ROSALIA MORALES: The domain holder would be. Actually, the domain holder requests. For issues relating to WIPO and UDRP, we would follow the procedure. We currently in our policies have a clear relationship with WIPO. We follow their procedures as to how to wait for their results before we can do anything with a domain. So that's different. We would wait for the case to be resolved

before we take any action, and we would do whatever WIPO tells us we should do.

But this is basically the domain holder. If the domain holder does not want a domain – like if you don't want to pay for that domain anymore and you want that domain to be eliminated or taken down – then we'll do it.

[KRISHNA RAJAMANNAR]: Can you give an example? Suppose I'm Amazon.com. I'm a domain holder. Can you say something like that?

UNIDENTIFIED MALE: Sorry. I think there's some confusion. Title holder? In this case you mean the domain name holder, not the IP right holder. It's not the intellectual property right holder.

ROSALIA MORALES: Yes. Maybe it's a translation issue.

[KRISHNA RAJAMANNAR]: Thanks. Can you go to the next slide?

ROSALIA MORALES: Yeah.

[KRISHNA RAJAMANNAR]: Yeah, yeah. Fine. The second question: speaking of taking down on cases of child pornography, human trafficking, and all these criminal activities, you do have terms and conditions with your registrant – that the registrar will be having with the registrant – which will be saying generally that, under certain circumstances, like in [inaudible] or any legal activities being performed in the domain, the domain will be canceled.

A similar process is in India. Our terms and conditions clearly state that, in case of human trafficking or any child pornography or any illegal activities being [carried out] under the domain name, the domain name will be canceled.

That's the reason I was asking you whether you yourself as a registry can cancel the domain name. Why do we expect a court order on that? Because we do that [inaudible].

ROSALIA MORALES: No. We wait for a court order in any case, even in these kinds of extreme cases of criminal activity, because we want a third party to make that decision. We as a registry do not take that decision.

It's also important to take into account that we started working with registrants this year. We haven't worked with them in the

past. So this presentation is based on .cr being the sole registry and sole registrant for .cr domains.

[KRISHNA RAJAMANNAR]: Okay. Because I just want to press you about that. We as a registry take action on the domains which are involved directly. So we take court orders only where it is required by law to the extent. Thank you so much.

ROSALIA MOARLES: Sure. Thank you.

PETER VERGOTE: Thank you. Eberhard?

EBERHARD LISSE: Eberhard Lisse from .na. The difference between Costa Rica and Guam is that Guam is an American protectorate. They have to do what the FBI says within American law.

For us, if they come to us like this and apply pressure to us, we tell them we have very nice places where they can go where the sun does not shine.

We will do what they want if they send it through their ministry of justice to our ministry of justice and our ministry of justice goes to the high court and the high court gives us a court order.

We have had contact with local law enforcement, with the Competition Commission, because of a particular case where a [inaudible] had weaned some locals onto a domain and then increased the prices significantly.

They found this anti-competitive and they asked us, "What can do to shut down the domain?" I said, "You must go to court." They said, "Yeah, we must go to court anyway to do any of this." I said, "Then just cite us as a defendant and just promise that you don't seek cost from us. We don't care. We do what the court says."

We would not respond to verbal or other pressure. We would tell them politely or rudely to go somewhere else. You and us are only bound by local law. There is no such thing as international law. There's international agreements. International law applies to particular aspects of the law, like marriage and things like this. It has nothing to do with this.

The FBI has only a very valid – and we have had them present here – they're very good and they're very helpful. If you have a problem, they will come and help you. But still, we have a contractual responsibility, even if they do nefarious practices.

We told them, "Take them to court. Cite us as a defendant. Don't seek costs from us." Then we will immediately respond when the court says, "Shut it down." We do it in court. We can do it from a laptop.

But less than a court case, then it opens for liability. In Belgium it's different. The Supreme Court has said, if a magistrate or a magisterial prosecutor says, "You're covered. You don't have a liability" – we haven't had this case in Namibia yet. What our lawyers say is that the best thing is a court order. Tell them, "No problem. Get the court order. We'll do it."

ROSALIA MORALES: We've told them many times, and the interesting part is that, in this case, it's not the FBI. It's from a government pressure. It's different. It's a different channel which we've never had before. I think if it were the FBI it would be a more one-to-one discussion like I've had in the past.

EBERHARD LISSE: My other –

ROSALIA MORALES: Let me just answer for comments. The other part is that I understand the situation in Guam. It's just the fact that they

tried to use cases of other countries or other regions in the world that have responded to the pressure for whatever internal reason they might have, which I do not know, as a way to increase the pressure on other governmental bodies within your country so that they pressure the ccTLD.

So we do not only get pressure from the U.S. government through the Department of Commerce, but the Department of Commerce pressures the Ministry of International Relations, the Ministry of Technology, and the Ministry of Commerce in Costa Rica to pressure us. So this strategy of pressure is new. It doesn't mean we're going to act differently from what our policies state. It's just a different way that we have not witnessed in the past and that I think might repeat itself in other countries. So it would be good for the community to know what's going on.

EBERHARD LISSE: My suggestion then is to participate in a high-level negotiation course where you learn to deal with these types of situations because this is pure tactics. They use whatever leverage they can. This is law enforcement. This is not bad, but they try whatever it takes. The quicker they get [their thing over] and they get their prosecutor, the quicker they get their own superiors on their back. We would just not respond to these kinds of tactics.

ROSALIA MORALES: We don't necessarily respond to what they do, but this is what's going on.

PETER VERGOTE: Okay. Thank you. Eberhard, one of your first questions triggered something. I can quite understand that, if you would receive an instruction from the FBI, you would say, "Thank you, but I'm not going to execute that, unless you transform it into a national court order." Now, suppose that you –

EBERHARD LISSE: No, I would not do that. I would tell them politely to go through the proper channels.

PETER VERGOTE: Okay. Meaning that, if they would be clever enough to have it translated into a national court order, then you would.

EBERHARD LISSE: Of course. I'd have to. I don't want to go to jail.

PETER VERGOTE: Now, just for my curiosity, would it make a difference if the request is not filed by, for instance, the FBI but comes from a U.S. court?

EBERHARD LISSE: It has to go from the ministry of justice in the states to our ministry of justice. Then our lawyers will tell us, "You had to abide by it, or it has to go to a local court." I'm not a lawyer in that sense. If our lawyer says you have to abide by it, we shut it down immediately. I would assume, from what my experience is, that a court order from the U.S. has to be turned into a Namibian court order. As soon as that happens, the domain is shut down.

PETER VERGOTE: Okay.

EBERHARD LISSE: We will not even enter a defense. It's not our problem. If they can convince a Namibian court, ex parte or whatever, that this is illegal – I'm not worried about assisting law enforcement. I'm worried about getting into a liability issues.

PETER VERGOTE: Yeah. Okay.

EBERHARD LISSE: As soon as I'm protected, I will assist law enforcement in any way I can.

PETER VERGOTE: Okay. Clear enough. Thanks.

Okay. Let's move over to the last presenter for the ccTLD registries, and that's Debbie from .nz. You have the mic.

DEBBIE MONAHAN: Thanks, Peter. I don't have any slides. When I got asked last night to do this, I found myself going back and looking at a blog post that I wrote in 2011, which is titled, "Takedown of Domain Names: The Rule of Law and Due Process." I find myself, six years later, reading that, and the situation hasn't changed.

Basically, to summarize the .nz position, it's very similar to what we've heard. We require a court order. We would require an appropriate court order which is quite clear about the domain name involved and the action on the domain name.

Now, one of the things we find, though, is that what we do do is take down domains names if the registrant details are incorrect. We follow a due process to give the registrant a chance to change those details. But if they're not updated, then we will cancel the name. So don't just suspend it. We actually cancel the

name. It goes through its 90-day [pending]-and-release period, and then it's released, available for reregistration.

Now, we actually have developed training courses that we give to law enforcement. When I saw "law enforcement," it's very broad. Basically, it's anybody that's enforcing anything, including health people and others. We train them on how to do WHOIS searches and look at domain names and find out information from it, and how to evaluate how correct the information is, and then we educate them about our process to follow-up on incorrect registrant details. So that actually deals with a lot of the ones that, if you like are truly, blatantly incorrect.

We would get probably one court order a month from America and every now and then from somewhere in Europe. It's enough that my lawyers have got a standard document telling them politely how to handle it, which is: go to New Zealand and get a New Zealand court order.

The other side of it, because we do require a court order, is that a number of years ago we made a decision that we would make it as easy as we could to help people get us a court order, basically. What we have is a series of standard documents. It includes an affidavit from me setting out how .nz works and what the situation is and why I won't actually remove it without

a court order. It's also got the basis for the affidavit for the true, if you like, complainant to actually file, where they just insert the relevant piece of legislation, whether it's a fair trading act or a breach of a trademark or whatever. They just put that in and complete the gaps. So those two go.

We've also actually drafted the court order. The court order names the Domain Name Commission as the second respondent. Then it says that the action of the court order is to order the second respondent to remove the domain name from the zone, from the DNS, for a period of 90 days.

What that period of 90 days does is allow us to follow through our process of incorrect registrant details because invariably they have incorrect details. The [speed of that does is], if the domain name is actually being used for something that's actually causing harm, then they will take that action.

Now, our papers have been used by some banks and some government departments. Generally they can be in and out of the high court. From the moment we provide the documents, they're walking out of the court with a court order inside of two or three hours. So it has proven quite a valuable tool to actually have those there to actually guide.

As Rosalia says, the pressure is immense to try to turn around and actually just take it down because it's clearly criminal

behavior. Well, what is clearly criminal behavior? We are a common law country, and due process is part of what we go through. We won't undermine that. We want an independent arbiter to actually give us direction, and we'll follow any court order.

But I think what we're continually looking at is: are there other options out there for a very speedy takedown or response still following a due process approach but recognizing that the Internet is a fast and dynamic tool and what used to work in the past with paper-based things isn't necessarily the best approach?

So we continue trying to think of ways that we can preserve the rule of law and due process but try to get smart about how we should work in the Internet age. Thanks.

PETER VERGOTE: Okay. Thank you very much, Debbie. Any questions from the audience for Debbie?

Seeing none at the moment – Eduardo, you had a question? Okay. Please approach the mic.

EDUARDO [SANTOYO]: Thank you, [Jorg]. No, it's not a question. Thank you very much for all of your presentations [and Debbie too]. It's just to mention that, in our case, in Colombia, we have not just a concept of the court order because, of course, if we are waiting for the court to have a pronouncement about some case regarding some cybercrime or cyber[delete] on the web, it will take a lot of months.

In Colombia, we have the statement that says a Colombian authority who can do the request to suspend a domain. We have a lot of authorities and powers to do that. For instance, in case of gaming – illegal games online – the Colombian authority ruled that games have the authority by law for ask for suspension of a domain. So they don't need to go to a court to ask for a suspension.

The Colombian prosecutor's office also can ask to suspend a domain in a case where they have evidence that the domain is being used to affect the Colombian citizens or to affect the interests of Colombia. They are not [biding] to wait until a court order has been issued.

Another example is that, when the Colombian [CERT], which is from the Ministry of Defense, is aware of something, like Colombia being attacked – some of the infrastructure – and

that's your domain, they don't have to wait for a court order. They can directly ask to execute the order.

We have agreements, of course, in order to link all of these authorities with us. Of course, we have to protect our liability on these. Of course, the liability is also on authority who gave the order is not [inaudible]. We are doing this construction of bridges between them and their registry in order to have a very [accurate] and secure e-mail account to process in a very fast way the orders. The experience that I want to share with you is not just for the court order processes because in many cases there are other possibilities in which we can collaborate in order to have a safer space in order to execute our responsibility with our registrants and, of course, with the people who are depending on the actions that we do.

In the case that Eberhard mentioned, we are doing the same. If we have a court order from, for instance, the U.S. jurisdiction, then we tell the lawyers, "Please go to the ministry of justice of the United States that has communication with our ministry of justice." Then the procedure is called [exacuatra]. They have to execute that procedure in order to transmit the court order. Of course, it will take a lot of dollars and time, but they want to do it.

Another thing that we have done on these interests is to connect the Colombian police, for instance, with the Homeland Security authorities. If they want this direct connection with the Colombian authorities and to ask the Colombian authorities to take the case, in case they consider there is some violation of something that has to be protected in Colombia, they will act.

That's the thing we are doing on those international cases that we also face. And we face a few from the U.S. because there are a lot of lawyers that get some court orders from – and we faced one from Europe last year. It was very, very strong because they had a lawyer who wanted restriction of a lot of domains – like 2,000 domains from many registries – and he wanted to have all the registries executing that domain through the Interpol, [they transmit the order] – of course, there was an order from a county from Germany – a small county. I don't know where it is. I said, "Okay. If you want to execute that order, you have to proceed through the [exacuatro] process. Otherwise, you can communicate with Interpol through the national police force. If they find that there is a way [where] there can be [involved] so we can receive an order from our Colombian" – and they [didn't] at the time.

So just to share that. It wasn't to ask a question. Thank you.

PETER VERGOTE: Thank you. Very useful. Thanks, Eduardo.

Okay. I would like to proceed now. Now that we've seen the point of the registries, now let's focus on positions of other partners in our business. We will start with the point of view from the registrars.

Ben, the floor is yours.

BEN BUTLER: Thank you. By way of background, I started and ran the Anti-Abuse Department at GoDaddy from the inception of the company. I'm still heavily involved in setting and enforcing those policies, so I have quite a bit of stories. But I won't share them here, necessarily.

I think one of the main things to keep in mind as far as a level-set here is that, as a registrar, we are contractually obligated to ICANN to provide a separate and dedicated team of individuals who are specifically empowered to investigate and take appropriate actions when a law enforcement or relevant government agency makes a request almost always in the form of a takedown request. That team reports directly to me, and we have evolved processes in that area.

I'll spend most of my comments going over that process because I think that's the one that's the most relevant to this discussion,

but it is worth bearing in mind that that is only one tool in order toolbelt with regards to dealing with potentially abusive issues. By volume, it is a relatively small tool in the tool belt.

We have existing policies and procedures that we've improved over the years to deal with things like copyright infringement, trademark infringement, spam, phishing, child abuse, malware – the list goes on and on. But those processes don't catch everything. They cast a pretty wide net, but there are always some things for which we as a registrar don't have the ability to determine whether or not something illegal is really going on. That's where this law enforcement takedown request comes into play.

I've listened to some of the comments in the other presentations and a lot of the questions that have come up, and they raise very significant points.

One of the first things we have to do when we're dealing with a law enforcement or government agency takedown request is to verify that that person making the request is actually a law enforcement agent or a government agent with relevant authority over the alleged activity because I can tell you that, on a volume that I was a little surprised at – a fairly high volume – we get a lot of people, especially once this became part of the 2013 Registrar Accreditation Agreement, who will send law

enforcement takedown requests pretending to be a law enforcement agent.

Now, sometimes that's easy to verify, but sometimes it's not. When I'm sitting in my office in Arizona and we get a law enforcement takedown request from a rural police officer somewhere in China, I have very few mechanisms that can, in a timely fashion, verify if that person really is who they say they are and if they're supposed to be doing that. Bear in mind that I'm contractually obligated to respond to that agent, assuming they are who they say they are, within 24 hours.

So this is something that we have to be on top of, and we have a large volume of these. So that's the first challenge that we have to overcome.

Once we've satisfactorily verified that they are who they say they are and they are a police officer or something similar, then we need to pin down what it is that the site is allegedly doing that is illegal. What is the law – usually a local jurisdictional law; sometimes it's a national law – that they're supposedly breaking?

Then we need them to provide some level of evidence as to how they came to that conclusion. What form that evidence takes is going to vary on a case-by-case basis and what type of law they're allegedly breaking and that sort of thing.

We're also going to find out if law enforcement attempted to resolve this by dealing directly with the registrant or the domain holder because we're not necessarily in every case going to be the best person to deal with this. And, from an evidentiary standpoint, if I own a website and someone is using it to conduct illegal activities and I feel like being cooperative, I can turn over logs and I can turn over information on what activities they've done on that site that a registrar isn't necessarily going to have.

Once we've got that pinned down, then we want to know: what is the length of time that you need this to be suspended? I emphasize "suspended" because, as a registrar dealing with these law enforcement requests, we have chosen not to permanently delete a domain name or permanently suspend it without a court order. So these are requests that are coming in absent a court order or something that final. This is us trying to be cooperative and help law enforcement with their criminal investigations. I'm willing to suspend it for a certain period of time.

Now, at GoDaddy that's currently up to 90 days. Now, if they want it down for longer than that, that gives them the ability to start that process to get the court orders that they need. There have been a couple occasions where we've extended that because of extenuating circumstances, but usually that's quite sufficient.

Once we have all of that, we also make sure they understand that, as soon as I take that site down – we suspend it – if my customer, that registrant, comes back and says, "Hey, why did you shut my site down?" we say, "We did it in order to cooperate with an official law enforcement investigation. Here is the contact information for the law enforcement agency and a specific person conducting this information. If you have questions about what they think you're doing wrong, you talk directly with them. We're simply here to try to uphold our policies, which say you can't use a domain name or any of our services for illegal activity."

If they have that dialogue – and they do – and the law enforcement decides, "Oh, well they're not actually doing anything criminal," or whatever their decision is, they will come back to me and say, "Okay. Go ahead and turn it back on. We're fine." So that absolutely happens.

Let's see. What else? Generally speaking, the biggest thing that has come out of this process for law enforcement and government takedown requests has been the realization that most law enforcement officers and government agents who request us to take down a website have not given sufficient thought as to collateral damage and the best strategic and tactical way to accomplish what they're trying to accomplish.

As an example of that, we get somewhere in the neighborhood of 500 to 1,000 of these requests per month to take down websites. We do that. We actually take the action to suspend the domain name in around 3-4% of those requests.

What that means is that, with the other 97/96% of cases, what actually happens is we help the law enforcement agent understand what exactly the services we as a registrar provide are. That might be something as basic as, "We're just the registrar. The hosting provider is somewhere over here." Or maybe we're just the e-mail provider and provide so many services. That is a big part of the question.

The other thing is to help them understand that a domain name can be part of infrastructure for any number of services that might be perfectly legitimate. So is there a more tactical way to go about getting this done? Once they understand that we are going to be turning that liability of why we took that down back on them, they're much more circumspect in making sure that this is actually something that needs to come down.

I'd love to take some questions if you guys have any for me. Otherwise, I would also like to point out that, of all the countries and all the jurisdictions and all the law enforcement agencies that we deal with, by far the best one that we deal with is the National Crime Agency in the U.K. They are stellar at making sure

we have the information we need, and we have never had a complaint from any of the registrants that they've asked us to take the site down from.

PETER VERGOTE: Okay. Thank you very much. I have a couple of questions, Ben, but unless I see urgent questions from the audience, I would like to give the opportunity to Chris to make his presentation first. Then we can have whatever kind of questions that there are remaining, and we will be more relaxed in posing questions.

CHRIS LEWIS-EVANS: First of all, thank you very much, Ben. I don't know quite how to follow that.

PETER VERGOTE: That was a hell of a [inaudible], wasn't it?

CHRIS LEWIS-EVANS: We got slides up. Sorry. To start, I'm Chris Lewis-Evans. I am the lead for the Internet and Infrastructure Investigations Team – I'll try to compete with ICANN's acronyms now – for the NCCU within the NCA (the National Cyber Crime Unit within the National Crime Agency).

We deal with serious and organized crime, so we don't get involved with any copyright issues or anything else like that. A lot of our investigations are quite in depth, quite long-winded, and last a long time.

Now our slides are [inaudible].

As it says there, the number of those serious requests that we get are roughly 50 a month. Almost 50/50 are from foreign agencies coming into the U.K., and the other 50% come in from agencies within the U.K. back out to foreign governments. Every single one gets checked and verified before they're sent to whatever company they need to go to. It's very, very important for us because I think it's been mentioned a couple of times in a couple of questions that, once we've done that paperwork, it is us that is responsible for any complaints, and that is not something that us as a police force or us as U.K. government want to be responsible for. We don't want to take down Donald Trump's site – well, maybe we might. Maybe.

So there is that litigation that we're obviously very concerned about, as much as yourselves. It's not a position that anyone wants to be in: being responsible for a takedown that has gone slightly wrong.

And it's not just domain names that we deal with as well. A lot of the times an investigation will start with an e-mail address or an

IP address. It's how we work those and explain how that's being used to commit crime.

The thing that has been mentioned a couple times – this is something I've really, really pushed within our unit – is the standardization of the communication that goes out. It's very important to get that across. It makes it a lot easier if we're dealing with someone from Costa Rica or someone in the States. They've got a nice template that's always the same. It's very important to highlight the crime type and offense being committed.

Every single request that we send out will end up as a court order, so the law within the U.K. has to be translated to the law [of the country] that we're sending it to. Obviously, the same goes for the other way.

So we do deal with a number of requests that come in from foreign countries where it's breaking the law in that country but isn't in ours. In that time, we have to say that the offense being committed isn't an offense in the U.K., and we're quite strong on that. Obviously we work around that if it is a definite criminal offense and it's just a slight mismatch in law. We're quite happy to go back to a foreign country and say, "Actually, what you're saying is an offense isn't an offense in this country. That's fine."

That never gets through to the registry, registrar, or hosting company.

Times stamps are vitally important for us, especially with some of the IP addresses that we're looking for. Again, it's just collateral intrusion. What we don't want to be doing is collecting data for someone that isn't a subject of the criminal investigation.

We're very clear all the time on what action we require of yourselves and then disclosure requirements are very important for us. Generally, it's an ongoing investigation, and a lot of the time we won't you to contact the people that we are investigating until we've properly brought the case up.

What works? What doesn't work? The top one is the big one, really. As has been said, there is no international cybercrime law, and it makes life difficult for us as law enforcement in dealing with large-scale criminal activities, generally in multiple countries. It makes life very, very difficult for us.

What helps us out is when we can get provided a little bit of information. They've got privacy protection on there. "Yeah, that looks like fake information anyway. I think you need to do this," or, "This IP relates to a VPN service. I think you need to carry on investigating and get some more information."

So we want anything that can help us out because I think, as has been rightly said, for us to get a court order out to a foreign country requires us to make one in our country and send it through diplomatic channels. It then lands in the foreign country. They need to decide whether laws match up. They have to then create a court order in their country, and then that has to get served. As you can imagine, that is not a quick process. If it happens within 90 or 180 days, then we're doing really, really, really well. So, yeah, that's definitely difficult.

Methods of sharing information I think I've touched on already. We're just trying to get some information to us that will aid the investigation. I said these are generally very serious crimes and a lot of effect. The understanding of your data protection rules and how you can share some information, especially when they are generally clearly breaking contractual issues with yourselves as well, helps us out.

Last of all is speed. Cybercrime does not stand still. I think we've actually touched on Avalanche on a couple of the cases, which might be why your numbers were so high in 2016. It was the small, German country police force that sent all the requests out to start with. They had 800,000 domains that got taken down. Not all of those were registered at once, but they had 800,000 domains that we secured, not to be taken down – sorry.

For us, the takedown is actually the last resort. It really is the last thing that we want to do. As Ben has highlighted already, for us there are so many more and better investigatory things that we can get from information within that server. If it's a compromised server, we'll do a lot of victim engagement. Can we get the logs? Can we get further information? Where has it come from? That sort of thing.

When it does work, it produces some really good results. I think three weeks ago now we arrested a subject in the U.K. that was about to fly out for holiday and who was responsible for the DDoS attack on Deutsche Telekom – a massive Mirai botnet DDoS attack. Really that was all made possible because we had I think four foreign providers giving us details to help track that down. That was all followed up with proper court orders, but [there] was a release of certain information that helped us narrow it down to the subject. So when it can work, it works really, really well.

With that, I think it's on to any questions.

PETER VERGOTE: Okay. Thank you very much, Chris. You know what strikes me after having heard three stories from ccTLD registries and then turning over to the registrars and law enforcement? We are dealing with domain names, while for you the complexity is

much greater. It's not only about domain names. It's quite the contrary. I think that, if I got you right, especially for a registrar it's far more about taking down websites than issues with domain names. They want their websites to get [rich]. We don't have anything to do with websites. The only thing we can do is perform an action concerning a domain name.

I get the same feeling from you, Chris; that it's about much more than domain names. It's also about e-mail address, IP addresses, etc.

So I think this is a very huge takeaway for us because we as ccTLD registries are so used to being with our feet in the nitty-gritty stuff about domain names that we should realize that there is a lot more going on out there. So thanks for that. I felt that it really is important that we get aware of that.

BEN BUTLER: If I could…

PETER VERGOTE: Yeah, sure. Go ahead.

BEN BUTLER: Just to add one little thing to expand on that point, as I mentioned, a lot of our takedown requests actually turn into

mini-training sessions with law enforcement on understanding the best and most tactical way to go out accomplishing what they're going to.

One of the things that a lot of law enforcement agencies – present company excepted – don't understand is that, if they go through whatever hoops they have to jump through to get a registry or a registrar to take down a domain name, that is not likely to keep the content they're trying to get rid of from being available on the Internet. It is extremely easy for them to simply point a new domain name at that same content.

I understand that there's challenges because hosting providers are not a unified group. They're not a contracted party. They don't play well with each other, and there's nothing to stop someone from being a hosting provider by sticking a Raspberry Pi computer in their closet. I get that.

So hosting providers isn't always a good option, but law enforcement understanding that taking down a domain name is like throwing a rock in a river and hoping it's going to stop the flow. It probably isn't going to, unless it's a really big rock.

PETER VERGOTE: Okay. Thanks for that. I had a couple of questions. I took some notes and I want to turn it back to the audience as well. I

particularly loved hearing you saying or stressing the importance of working with standardized documents and templates.

Now, I want to fire this question to the room. We can use the cards. Do you share the feeling that we can interact probably in a far more efficient way if we try to make more use of standardized wording or phrasing so that law enforcement is assisted in providing better instructions to us registries? I'm still having this feeling that, if I were a stubborn man and if I get court orders and it says, "Take down the domain name www.whatever.be," I can say, "I'm sorry. I'm not an ISP. I cannot take down a website, and this is not a domain name." [They withdraw the revocation of the domain name you're asking.] So I think that providing clearer instructions can help a lot.

I want to take the temperature of the room and see if you share that view also or if you think, "Well, regardless of whether we are going to work with standardized documents or templates or whatever, it's not going to change much." So which way?

I'll get to you in a second if I can.

Can I get show of cards? If you say, "Well, this is probably something that can help us forward," show me a green card. If you say, "Well, now, it won't change much," then show me yellow or red.

Okay. Interesting. All of those undecideds. Okay, well, it's surprising. I saw on this side a majority of green, while this side was more or less yellow. Okay. Interesting to know.

You had a question, sir?

GRIGORY SAGHIAN: Thank you. Grigory Saghian, .am ccTLD. You told us about a very interesting procedure that's formalized, but if you have some kind of information received by a law enforcement agency, and after receiving it, this guy, let us say, removed all the information from the website, you don't have a case in this case. Some kind of information this law enforcement agency has to provide, like [sign/print screen]. What is the situation in this field?

CHRIS LEWIS-EVANS: We have something called a preservation request that we can utilize, which effectively allows us to do a fast freeze of the system. What that allows us to do is say to the hosting company, "We want that content. A court order is on its way," and give a time and date that we want that to be carried. So we would be able to freeze that.

There is obviously a risk that they'll –

GRIGORY SAGHIAN: [inaudible].

CHRIS LEWISS-EVANS: Sorry.

GRIGORY SAGHIAN: Who will be able to freeze that? You or the law enforcement agency?

CHRIS LEWIS-EVANS: The hosting company.

GRIGORY SAGHIAN: So the law enforcement agency will also send a request to the hosting company to freeze it?

CHRIS LEWIS-EVANS: Yes.

GRIGORY SAGHIAN: Okay. Thank you.

CHRIS LEWIS-EVANS: By “freeze it,” I mean capture it as it is and still leave it running until they get a court order. In the case where the suspect might

then delete all the information, that allows us to do that because otherwise we just wouldn't get anything [realistically].

GRIGORY SAGHIAN: So the print screen only is not enough.

CHRIS LEWIS-EVANS: A lot of the time, no, because you're going to lose all of the logs, which realistically is what will give us the best investigative leads. A print screen for copyright or something like that would be fine, but realistically, for most of the investigations, we're looking for logs and who's accessed the server and maybe backend databases as well.

PETER VERGOTE: Okay. Thank you. We're a few minutes before closing this session, so I wanted to take this opportunity to have one last interaction with the audience. It's a very simple question. If you as a registry operator take action with regard to a domain name – let's say a revocation or withdrawal based upon, let's say, a court order – do you inform the registrar as well of your action or not?

Please show me your green cards if you do, or red or yellow if you don't.

Okay. Thanks. That's good.

BEN BUTLER: Speaking on behalf of registrars everywhere, thank you for notifying us.

PETER VERGOTE: That was going to be my question because, if I would be in the position of a registrar who deals with the end customer and then suddenly you realize that the registry has done an action with regard to a domain name but your end customer is going to get in touch with the registrar, saying, "What happened?" and if you then don't have the confirmation from the action that was taken by the registry, you need to phone up the registry yourself, etc.

I'm very pleased with this outcome, by the way; that we are all so careful for the registrars and that we –

BEN BUTLER: You guys have the numbers. Could you convince the gTLD registry operators to get in line with you on that one? Because that situation you described has happened multiple times, never on a ccTLD. For liability reasons, I'm not going to mention them, but there are extremely large gTLD operators who have been operating gTLDs forever who have just stuck us by shutting

down hundreds or thousands or whatever number of domain names, and the first time we hear about it is either the customer calling, really upset, or in a press release the next day. Not helpful for us.

So thank you. Honestly, thank you for doing that.

PETER VERGOTE: You're welcome. I think that Debbie was raising – sorry, Debbie. I wasn't able to see you. Then [inaudible].

EBERHARD LISSE: We are extremely strict on our WHOIS requirements. We do not deal with the end client at all. We only deal with the registrars. If we get an issue – we had a shutdown today and the end client [discussed this,] we sent him three e-mails. He must talk to his registrar. We don't deal with this. If we get a court order and we shut something down for a WHOIS inconsistency, which is an internal measure that one can always use while one is looking at things, we deal with the registrar. We do not deal with the end user.

PETER VERGOTE: Thanks. Debbie?

DEBBIE MONAHAN: I was just going to comment that the other thing we have in our authorization agreement with registrars is that, if the registrar gets issued with the takedown notice, they are to send it to the Domain Name Commission, and we will take the liability. We will pick it up, and we will make it quite clear to whoever is threating the registrar that that's actually on us and then tell them the process for .nz [inaudible].

We also take out an insurance policy which covers registrars with respect of their .nz activities. So we take out public liability insurance. We get one policy that covers all our authorized registrars, and that's to encourage them, if they give us any notices that they get like that, that then they will be covered under our regime and we'll look after them.

PETER VERGOTE: Okay. Well, with this, I would like to bring this session to a close. I would first of all like to thank all my panelists. Thank you very much for your presentations.

Thanks to the audience for helping make this session and interactive one. As you know, at the end of the ccNSO meetings, there is always a survey. Since we slightly changed the format for the legal session, please give your feedback, your opinion, about how we structured this session. Do you think it's beneficial compared to how we previously had done it? Would

you like to repeat it? Would you say, “No, please revert to classical presentations –25-minute presentation and a Q&A”? Feel free to give us your feedback, please.

Thanks. Let’s enjoy the cocktail now.

[END OF TRANSCRIPTION]