HYDERABAD – ccNSO Members Day - Day 2 (pt 1)
Monday, November 07, 2016 – 09:30 to 10:30 IST
ICANN57 | Hyderabad, India

PETER VERGOTE: Good morning, everybody. Can I ask the presenters for the legal session to come upstage, please?

Good morning, everybody. We are going to start with Day 2 of our ccNSO Member Meeting. I'm going to be your Chair for this legal session of this morning. In the next coming hour, we will have four very interesting presentations. We are going to have Hiro from .jp and Vika from .za who are going to share some insights on the recent changes in the legal framework and how this is affecting their Registry. Erwin from .dk will share with us the result of a public consultation on how to fight cybercrime. Last but not least, we are going to have some cross-community engagement here while we have Thomas Rickert and Michele Neylon with us who are going to take us through a number of issues regarding data protection and privacy.

Without further ado, because we are already running late, I'm going to ask Hiro to kick it off. Just for a sense of efficiency and in order to get us smooth through this session, I would like to ask you to hold on to your questions or remarks until all the presenters have finished their presentation. We take questions

and remarks at the end, depending on how much time that's left. Hiro, the floor is yours.

HIRO HOTTA: All right. Thank you, Peter. I'm Hiro from .jp. I'll, today, talk about the Amendment of the Japanese Telecommunications Business Law. May this year, an amendment of the Telecommunications Business Law executed. I will briefly talk about the background and who will be affected by the law and how our Registry JPRS goes with the law.

This is the background. In 2015, last year, the amendment process started. In the government document, these are set, Growth of the Internet and DNS usage from 2005 to 2013. The Internet user penetration, of course, it grew and DNS queries, five times more.

Number of TLDs, as you know, that before that, 300 including gTLD and ccTLD. In the time of 2015, it was 900. Of course, at this moment, there are more. TLD operators with less experience are emerging as new gTLD operators. Complexity of DNS operation grew as bigger zone, more frequent zone update and more DNS server instances and more cautions are needed in operation such as due to DNSSEC.

This is a contractual framework of .jp management. In the past, before the amendment law, we, the private company, have contracted with JPNIC which is a membership, nonprofit organization that we report our activity to JPNIC. JPNIC checks whether it's good or not. JPNIC consults with the government whether we do good or not. JPNIC and government consult with each other whether JPRS is a good guy or not. Of course, we have a contract with ICANN.

On and after 21 May 2016, the contractual framework of .jp management is little bit changed. The government and JPRS has a direct relationship of this amendment of law. We report to the government as well as to the JPNIC. The government checks whether we do good or not.

Telecommunications Business Law, before May 21st this year, there was no reference to domain name registry. No action needed to the government under this law. It means that no laws applied to us. However, by the amendment of the law, ccTLD Registry and Japanese geo-TLD Registry are under this law. We have to notify of our business to the government. It's just notify, no permission. It's just notification.

Obligations of TLD Registries. Who are named by the amended law? It's the ccTLD Registry; us, .jp; and the geo-TLD Registries which reside in Japan. It's the nagoya, .tokyo, .yokohama,

.okinawa, .osaka, three new registries. What obligations? The principal ones are documentation of our administrative rules for the telecommunications facilities. It means domain name facilities and reporting it to government.

We provide neutral universal services without refusal to users. We report significant accidents to gov. if it happens, and the significant DNS failure at the time of accident without delay. For the less significant failure, we report it to the government quarterly. We publish financial accounting statements every year.

How we contend with the obligation. First one is the documentation of administrative rules. We clearly document the administrative procedures, such as operation in usual situation and operation in emergency situation, namely accidental situation, and preparation for the system considering future demand and possible crisis. For example, disaster recovery, and security policy and implementation. This documentation was not a big issue for us because they are currently all or almost documented already.

The second one is the designation of responsible persons and reporting it to gov. Who's responsible for the service? Who is responsible for the reaction to the accident? Top responsible

manager of telecommunications facilities. We named our CTO as the responsible person.

Okay. Next one is how we provide universal services without refusal. The law says Registry must provide a fair service to the registrants. Of course, this is not a big issue for us because we operate neutrally to the registrants and applicants for registration. It's documented as a policy.

However, definition of fairness is not given by the law or decree. For example, it is not defined whether deleting a DNS entry from the zone file due to abusive Web content is against the fairness to the registrants. Why not? It's not easy to decide. Even the government does not have an answer to the above at this moment. Registry, registrar, and government, and maybe registrants cooperatively need to work on the definition of fairness and how the registry should respond to that.

The third one, reporting significant accidents to gov. What are significant accidents defined in the law? At this moment, 1,000,000 domain names influenced for one hour is significant. For example, JP has 1,500,000 domain names. If the DNS stops entirely, of course, it's a significant accident if it takes one hour to restore.

Thirty thousand domain names influenced for two hours. We have to report our outage with huge influence. For example, DNS failure, every time without delay. Of course, we didn't have this kind of experience but we have to prepare for such reporting system.

Registry needs to make outsource DNS operators formally report the outage of their DNS service to the Registry to collect them and report it to the government even if the outage is tinier than the significance threshold criteria.

Registry must define the workflow and the scope of information collection and reporting. Contracts with outsource DNS operators need to be amended for Registry to be able to impose SLAs and the reporting responsibility on them.

Publication of financial accounting statements, we hate to do this but the law requests us to do that. Basic financial information, P&L, BS, and supplementary statements for P&L and BS. They are published. Domain name related services are considered to be a single business unit in the statements. This is not a big issue for us because, of course, we do make this kind of spreadsheet on our site. However, we don't like this because it is not defined about what are domain name related services.

Exposure of the financial status of domain name related services nearly equals to exposure of the financial status of our other business and may negatively impact the market competitive power. Usually, the transparency leads to the demand for more transparency even if no one thinks about how to use the disclosed information. Okay. I think this is the end. Thank you.

PETER VERGOTE: Thank you very much, Hiro. In order to keep track with time, I would move on to the next speaker. Erwin, the floor is yours.

ERWIN LANSING: Good morning. I have to admit I am not [prepared for that] either. I don't have any famous quotes but I do have a cartoon later on so stay tuned.

First off, a little bit of background of why this slide say Danish Internet Forum. Usually, you know me as DK Hostmaster. That's because we're two different companies. There is Danish Internet Forum which is a membership based nonprofit with a broad range of members from the Danish Internet Society which is appointed by the government to take over responsibility of the .dk zone. DIFO owns DK Hostmaster which is a limited liability company. That's just there to operate .dk. It's just an operation, not a company.

I think you get the same thing as we have. There are several forces in our constituency that want to do more about crime and abuse on the Internet. Of course, with the unique position as a registry, they want us to do more as well. Without being very specific, we thought let's ask back what you actually mean by that. What should we as a registry do?

We held a public hearing with oral events in June and then there are written open hearing until August. We have three specific topics in mind. I'll get more into what they are in later slides: the suspension of domain names, disclosure of registrant information if the registrant has name and address protection so they're not public in WHOIS, and validation of the registrant's information.

We were positively surprised by their replies. There are from just about everyone in Danish Internet Society, from consumer organizations, rights holders. Lots of domain and registrars came back. It was really positive to hear.

I don't have to tell you, people did disagree. They did not agree. On the first topic of the suspension, we have two different processes. We have an Independent Complaints Board which basically takes care of the use of the domain name itself and does not really look into the content of how the domain is used.

Then we have, as DK Hostmaster, there are certain provisions in our terms of services that allow us to take action which we basically only use for two cases which is typosquatting and malware hosting.

The question we posed was: should we establish a separate complaints board that looks more into the content of how a domain is used? Several people replied that it might be a good idea. The current process of going through the police, then having to go through a prosecutor, then having to get a court order takes a lot of time and especially with phishing, etc., it really is used in hours and not days or weeks. We should have a way to do it more quickly.

But of course, we get quickly into the discussion of what is "obvious" more, what is obvious crime. This also make the complaints boards, judge, jury, and executioner. People were very afraid of going through that direction. That was also the decision by the board of not going through the direction but to create a better cooperation with law enforcement and the judicial system to make it easier to use the current system and make it faster.

On the disclosure of registrant information, by law, we are obliged to make all registrants public in our WHOIS and our websites unless there's a specific provision not to make it public

which means for private persons, you can go to the local council and get name and address protection. Then we have to hide you in our WHOIS.

We have a best practice on how to get that information if you really need it. It's very specific on what you have to provide to us. Be very specific about what do you need, why do you need it, and why do you think you're allowed to get it. The conclusion here was that current rules are quite sufficient and we should just stick to those.

On the registrant validation, we have, by law, again, a very strict provision that we should validate all registrants against either the Civil Registration System or the Business Registration System.

For foreign registrants, we send a paper letter. If it comes back, we take away the domain name. But of course, you can see that lots of countries, the letter just get lost and doesn't actually return. This is very easy to circumvent.

What should we do more about that? In Denmark, we have a governmental ID system called NemID, easy ID. Should we use that for Danish registrants? Because what we also do right now is that when you register a domain name in Denmark from a Danish registrant, we check that the name and address actually

fits with one of the registries but we don't check that is actually you.

Should we use the login procedure of the governmental system to actually check that is the right registrant, registry domain name? What should we do more about foreign registrants? What we got back was basically that NemID is used in so many places already that it should not be a big burden for anyone to use so that we should go in that direction.

Foreign registrants is quite hard. There's no real registry, civil registry or business registry to ask, and we should figure out something. That's all I have.

PETER VERGOTE: Okay. Thank you very much, Erwin. [Nigel], I saw that you were waving your hand. Is it point of order or is it question or remark, because question or remarks, we are deferring them until the end of the session.

Good. Next speaker is Vika. Vika, you're up.

VIKA MPISANE: Good morning. My presentation is about the Changing Regulatory Landscape in South Africa. That's [operating] also the Domain Name Regulatory Landscape.

I'm running two screens here because I'm not wearing glasses. As much as I can see there, I see the pictures, not the words. Right.

The .za Domain Name Authority has its own mandate defined in the law, the Electronic Communications and Transactions Act of South Africa. Its responsibility are listed there. The management and administration of .za; licensing .za registries and registrars; best practice compliance; policy guidelines; importantly, public awareness; research in South Africa; and advising the Minister of ICT in South Africa on related policy issues. That's the current mandate, and that is what this ongoing ICT policy review framework is reviewing.

Now, this ICT Policy Review Process of the Government of South Africa started in 2013. It's ran until early 2015. The reason behind this ICT Policy Review being there was no holistic ICT Policy Review since 1996, so almost 20 years later.

Then the reality was the current ICT laws were no longer are talking to each other well. Based on the '96 interventions, the appreciation over time was that ICT regulation spread across different regulators. For example, .za Domain Name Authority for domain name regulation and the Independent Communications Authority, ICASA of South Africa, responsible

for the broadcasting spectrum networks and so forth, the bigger part of the ICT value chain, if you want to put it that way.

There's an agency called USAASA, Universal Service and Access Agency of South Africa. That too is responsible for universal access establishment of ICT hubs, digital terrestrial television, and so forth.

Then there is also the Film & Publications Board that's responsible for content regulation. That was the appreciation really that prompted the need to review the ICT policies with the view of harmonizing them.

In addition to that, of course, there are gaps in terms of our [due diligence] of Internet research or technical development and Internet governance. Those were not allocated to any particular entity.

This Policy Process, when started in 2013, had the Minister of communications establish what was called an ICT Policy Review Panel which at its end in 2015, released a Green Paper calling for integration across the regulators and especially the Independent Communications Authority and then the Universal Service Agency, ICASA and USAASA.

But this current process did not make any conclusive recommendations on what to do or how to change or affect

ZADNA. It did urge the minister to consider expanding ZADNA's mandate to do deal with other broader Internet issues or Internet governance, Internet security, and so forth.

The Green Paper also concluded with a call on government to proclaim clear Internet governance principles. Also, the same Green Paper also advocated that there must be a clear domain name regulatory framework covering both .za and generic top level domains that exist in South Africa like the three, such as .durban, .joburg and .capetown.

Now, from that policy, from the Green Paper, the government moved then to what is called the White Paper which is now the policy decisions based on that process. In the White Paper, the government made a firm and they've taken up decision. The White Paper came, I think, last month. No, sorry, on 8 September.

It calls for the integration not only of the Independent Communications Authority and USAASA but also even of ZADNA, the Domain Name Authority. The idea being to integrate the regulatory framework into one what is called Integrated ICT Regulator. This integration though excludes issues of broadcasting, and that's because there's a specific law that will make it difficult for them to be moved to this integrity of regulator.

This White Paper, these policy decisions that the Ministers now made, means that there will be significant amendment of laws. That's about to begin. In fact, government is working on that. Those are the types of laws that will be affected: the ECT act, the Electronic Communications Act, and so forth.

There is, however, willingness on the part of government to receive expert advice on how best to implement this. As a result, we've been talking to our government and with a couple of other entities and especially from the local Internet community.

There is also an appreciation in the South Africa the government that the pursuit of integrating the regulatory framework may need to be done in a phased manner so that there are not disruptions across the whole ICT spectrum.

This is just a mind map extracted from that policy that shows that this now new integrated ICT Regulator will be responsible for a couple of other areas that will bring together for missions of competition, regulation, numbering resources, innovation, open Internet, equipment approval, spectrum allocation, Universal Service and Access, and so forth. It's a measure integration.

Notably, at the bottom there, there's the blue part which is the Internet and Digital Authority. This, in itself, is interesting

because it's a reflection of how the government grappled with the issue of how to best deal with Internet governance and so forth.

There were calls that there should be a separate entity built on what ZADNA is or converting ZADNA into that entity. That entity should ideally be outside this integrated regulator because of the multi-stakeholder nature of the Internet but eventually, [the designated standard is .za] and it will still be part of the integrated regulator. It may well be a subsidiary of this regulator.

Now, what does this mean then, this decision? It means that here, .za Domain Name Regulation that ZADNA is responsible for. The management of second level domain registries, you'll see with .za and so forth. The registrar accreditation, Internet governance, and the operation of registries for the three cities will all move into the new integration ICT regulator.

Now, what is driving the government to make this decision is that they're trying to eliminate duplications across the entities. They're also trying to deal with the gray areas that have been left hanging in our ICT value chain, like I said, issues of Internet research and governance and so forth. They want to achieve coordinated and effective governance and regulation of the ICT as a sector.

One of the drivers of this integration also is the fact that government wants to accelerate rapid deployment of ICT infrastructure in a country like South Africa, developing economy. Then also, one of the drivers is they appreciate the convergence of technology that they can't allow the entities to be existing in total siloes as if they are not related.

It's also important that, and this is acknowledged in the Paper, that the government wants to have flexibility to allow for new entities to exist if they have a clearly defined mandate. Then of course, the issue of being effective in cost of ICT regulation. Those are the key drivers behind this.

The question has been what will be the best means of achieving this integration that the government is pursuing. There are at least two similar options, but they differ at the end goal. We [had consultations] last weekend a couple of ICT industry consultations and workshops about how best to implement this.

What has come to the fore is there are, as I said, two options. Option 1 has been to say the industry back home appreciates that the Internet is founded on an openness and multi-stakeholder collaboration and so forth.

The feeling is that as Option 1, the management of Internet resources be integrated first under ZADNA. What that means is

that you do not take ZADNA immediately and absorb it into a new entity but that the management of Internet resources be moved under ZADNA. This allows at least government to have a phased integration. That will allow the government to learn as they go with these integrations. It. allows also for quick wins because it's easier to integrate certain sections of the Internet value chain into ZADNA as an Internet authority in a way.

Thereafter, you can then take this as the "new ZADNA" it's called also and integrate it into the new integrated ICT Regulator. But there's Option 2 which is really similar to 1. The only difference with Option 2 is that the goal is that you do not take the new ZADNA or the Internet resources management agency and absorb it into the bigger ICT regulator but you let it exist separately.

This Option 2 has received greater support from the industry last week in the consultations that we had. Then also we had the government, the [inaudible] those consultations, and it looks like we are likely to have a scenario where ZADNA will be expanded in terms of mandate but not be integrated into the new ICT Regulator.

Sorry. I'm not sure. Okay. I don't know if you can see that. That's just a map out of what the new ZADNA – here it's called the Internet Resource Management Agency – just for argument's

sake, what its functions will be. One being the current functions as allocated by the ECT Act of what ZADNA does. Then two is the management of Domain Name Registries which currently sits under entities under us and the policies calling for them to be elevated to this new regulator.

Three, this new entity, the new ZADNA will be responsible for multi-stakeholder governance, Internet governance. Then four, Internet policy and research. Five, issues of emerging Internet technologies, protocols and standards and how they're related to the effectiveness of the Internet in South Africa. That's a broad scope. I heard they Nominet presenter yesterday talking about the issues of Internet of things and TV White Spaces and how they relate to the domain name infrastructure. This entity will actually be responsible for such things.

Then skills development, number six. Seven, accreditation and compliance, so for authentication of service providers and so forth and then Internet security. That's just a map of what this new entity or what the ZADNA will tend to be is part of this process is.

Now, way forward, obviously, is that then government is now working on turning this ICT Policy into specific legislation. It's likely that process may be prolonged because there are a number of acts of parliament that will need to be changed. The

process also is substantially political. It may not be as easy and smooth as it appears.

That's why, of course, government started to appreciate that it may be easier to expand ZADNA into something else on the Internet side and that could be a quick win. The reconciliation of the other ICT Regulators is a highly political matter.

We want to be proving value and benefit in separating Internet governance framework from the Integrated ICT regulator. We're working with a number of entities in South Africa. We will also be having provincial workshops of this ICT Policy review and also advocating what we think is the best means of implementing it.

That's, in a nutshell, the process and the development in South Africa as far as ICT and especially domain name regulation is concerned. Thank you.

PETER VERGOTE: Thank you very much, Vika. That brings us to the last presentation of today. If I have understood it correctly, Thomas, you're about to kick this off. Then Michele will take it over or add a few points.

MICHELE NEYLON: Or just disagree with him or something.

PETER VERGOTE: Or sing a song. Okay.

MICHELE NEYLON: You don't want that.

PETER VERGOTE: Okay. Thomas, go ahead.

THOMAS RICKERT: Thanks very much, Peter. Good morning to all of you. My name is Rickert. I represent eco, the Internet Industry Association, and I brought with me Michele who is with Blacknight which is one of our members and he's also on the i2 Coalition Board. I guess you will see us collaborating more in the future. We shared the podium yesterday already, but the idea is that we would do more initiatives together between the two organizations.

I came here to discuss or hopefully start a discussion with you. I didn't bring any slides, so I will try to make my introductory remarks as shortly as possible and then hopefully we will have some space for discussion.

I want to discuss data protection and privacy with you. If you look at WHOIS which is not the only data protection related part

of what we're doing but it's an important one, certainly, you see the CCs running their WHOIS according to local law. At least that's what they should be doing. They should be compliant with their local applicable law.

The customer these days, at times, is quite confused because in the country that I come from, they have .de. I'm looking at Peter over there. They have .de which runs WHOIS in a certain way. Then they have .berlin. I see [Diac] at the back of the room. The WHOIS regime is entirely different. From a user experience perspective not even talking about compliance, that's sort of a weird thing.

If you look at Gs, it's sort of funny because there, U.S. law is the starting point for everything. While this is a globally applicable conversation, let me just highlight one thing, which is safe harbor. I mean you are familiar with safe harbor and that the European Court of Justice invalidated the safe harbor principles and thereby making it illegal to use safe harbor for an exchange of data between Europe and the U.S.

Then there was a political wish to fix that issue briefly so they came up with Privacy Shield. But the underlying concerns with safe harbor are the same for Privacy Shield. Experts in the field believe that Privacy Shield will be invalidated sometime soon. There are people gearing up to take Privacy Shield to court.

When I speak about these issues, I tend to tag Privacy Shield as a cliff hanger between now and the time that it's being invalidated. Can it be a solution for us to do everything under U.S. law and to ship all the data to the U.S. in the long run given this complexity? There seem to be irreconcilable gaps between the legal systems.

What do we do with that? Shouldn't we consider to rethink this whole thing, particularly since the CC world and the G world is converging? Many of you are running gTLDs as well. Many of you are running backend for Gs as well, so you have the technology in place to do certain things for both worlds. I think that the Gs can learn a lot from the CCs in this regard.

My take on it is that it is quite outrageous that a registry operator or a registrar in a certain jurisdiction needs to go to a private entity in California and ask for permission to be compliant with the local law. You can ask for your WHOIS to get an exemption to run your WHOIS according to local original law. You can ask as a registrar to get a data retention waiver. But these are cumbersome processes. These are costly processes. These are time consuming processes. I think it's not really appropriate that you need to apply to get an exemption to be compliant. You should be able to be compliant by default.

Shouldn't we think the other way around and for WHOIS or for data protection or for certain contract law matters to make local or at least regional law the default? Let's maybe not take U.S. law as the default and try to change that but reverse it to have a better customer experience to make it easier for the contracted parties to be compliant.

I do know that this is not an easy task, but I think that it's high time to think about that. Certainly, ICANN legal will not like the idea of honoring as many jurisdictions as we have globally because that would be a costly thing to do for them. But maybe we should think about ICANN offering local or regional laws, let's say one legal regime in Europe that you can do contracts under, at least something that is better or easier for customers to understand and for the contracted parties to operate on them.

Certainly, we do need standardization at the technical level to the best possible extent. I will invite Michele to talk to that in a moment because he was member of the EWG looking at WHOIS successors and he also, as you know, is a technical guy which I'm not. But I think that we should all think about how could this work and start a conversation about that which hopefully we're going to kick off today. Then maybe we can take some of that to the jurisdiction debate that we have and work stream too of the accountability discussions.

I will leave it there. Just as a takeaway message, main idea is paradigm shift, not U.S. law as the starting point for everything but maybe local law is the starting point for everything. Then make it match what we have at the global level to the best possible extent. Over to you, Michele.

MICHELE NEYLON: Thanks, Thomas. I know many of you have had the pleasure of coming to the ccNSO once or twice in the past. Plus, I know some of you via CENTR and some of you, of course, have had to deal with me as one of your dirty, filthy registrars who asks you all sorts of awkward questions.

Okay. This entire discussion around data protection and privacy, I think for those of us based in Europe, it's a hot topic. That's not something that we're going to debate. As Thomas rightly points out, safe harbor is gone. We currently have Privacy Shield. But there are multiple people who are trying to invalidate that. When that happens, it's going to cause a lot of problems for a lot of people.

My own company is based in Ireland which, of course, is part of the European Union and is not leaving, just so we're clear. What we're seeing in lines of the context of what happened in the U.K. with Brexit is we are seeing companies actually coming to us and

looking to put data physically in Irelands because we are the only English speaking country that is going to remain under that privacy regime.

Within the context of ICANN, as Thomas points out, there are a lot of issues. There are several of the other European registrars here in the room. I know several of you are offering backend services to gTLD registries. ICANN legal only understands U.S. law. They are very happy to say to everybody in public that they would never ever ask a contracted party to break the law. They will say that until the cows come home. But the reality is they will ask. Actually, no they don't ask. They will demand that you break the law. They make it very hard, if not impossible, to comply with the law.

There are two things that as a registrar for gTLDs that we've had to deal with. Well, actually three, I suppose. One is the data retention requirements under the 2013 contract. There are ways to get a waiver but it's very, very complicated. You end up having to have a ridiculous argument with somebody about privacy who doesn't actually understand how privacy works.

My company applied for this as soon as ICANN made the process available. It took us I think ten months before they finally let us have it. That was very nice of them. The WHOIS waiver process that Thomas mentioned exists. Yes. However, it is so

dysfunctional that nobody has been able to use it. Not one registrar it has been able to trigger that process. Because it is so backwards in the way it's setup that's it's just impossible.

Why would you guys care? I suppose part of this conversation is for many of the country codes, you've solved this. You are running your WHOIS, or at least as Thomas says, you should be running your WHOIS under the correct regime and under local law. From a technical perspective, I know some of you are looking at different solutions and some of you are moving to technologies such as RDAP which you've probably heard is being adopted by the numbers community and is being adopted, well, will be adopted across the gTLDs.

I served on the EWG within ICANN for about two years where we came up with all sorts of interesting ideas of how to potentially solve all the WHOIS issues. I know some of you have read that report and hated it. I didn't write all of it, swear to God.

Now, over in the GNSO, we are still working on WHOIS and we still haven't fixed it. I suspect that I'll be back here talking to you in about another two or three years' time, and I'll still be saying it's still not fixed. Maybe the answer is to actually just remove WHOIS completely. That's quite a nice idea.

Anyway, I'm going to shut up now. If anybody has any queries for me or for Thomas, we're happily to answer them. If you don't have time to ask us now, just grab us at the hallway. Normally, I'm the one wearing a T-shirt. Thanks.

PETER VERGOTE: You're a bit in disguise today. Or did you dress up for us?

MICHELE NEYLON: Well, I thought it was only respectful for the ccNSO.

PETER VERGOTE: Thanks so much. Okay. We have a little less than 15 minutes for questions and interactions with the various presenters. I already had [Nigel] on the queue. Young-eum, I'm going to put you on queue as well and Rieke and Christian.

But just as point of information, what Thomas and Michele have been touching upon, there is a high interest topic this afternoon where there is a meeting scheduled with the legal counsel of ICANN. If anyone would feel compelled to dive deeper into the issue of data protection and privacy, we can always take it up during the high interest topic session of this afternoon.

Now, I'm going to open for questions and observations. [Nigel], you have the first call.

[NIGEL]: Thank you, Peter. I put up my hand or I think it was as much as raising an eyebrow, in one of the early presentations so the comment is going to be about that. I've got something that comes up over what has just been said, but like I would like to put myself at the end of the queue for that one. I'll just deal with the one that I've put my hand up to give everybody else the opportunity to do the 15 minutes.

It relates to validation of particular natural persons as well as legal persons. I got involved in a case recently, not to do with my registry but to do with another registry, were these domains are registered because of a former colleague who had the problem and he called me.

It turned out this registry is doing validation. This gentleman found he had about 30 or 40 domain names registered that he had never heard of. The reason for that was that these domain names had previously been registered, been caught by drop catchers, and the drop catchers were using them to settle counterfeit goods. Because of the validation, I don't know where they got his personal data from, but they fastened on his

personal data, registered these domains in his name in order to pass the validation checks which check that this person is a real person, that he exists, and that he is resident at the address that's in the registrant.

He found out about this when somebody phoned him up and tried to buy one of the domains off him. We managed to get the domain names. Well, they don't need to be transferred into his name. They were in his name. We got the registry to recognize that, although he was not really the person who had registered them, he should be the person who registered.

We got control but not too quickly because he then got the summons from a very big U.S. law firm acting for a very big U.S. brand naming him along with a lot of other people in a very scary lawsuit. He got then involved. We had to get a friend of mine who's a practicing lawyer to negotiate with the brands and persuade them that, although they tracked this guy down and he was a real person and so on, that he wasn't really. Eventually, it was dismissed with some not inconsiderable legal costs to the innocent party.

My comment is really this. Be careful what you ask for because the law of unintended consequences does come to bite you. If you are validating in this way, you are going to get strange and unusual problems, and really how can you go any further than

this? You want people to appear in person at the registry offices? I don't know.

YOUNG-EUM LEE: I would like to ask a question both to Hiro and Vika because I found an element in both their presentations that were very similar which is that in your recent legislation, the laws seem to have included these generic names which are names of cities or geographical but also fall under the GNSO rubric. I would just like to hear your opinion on what you think is the potential effectiveness of the law in enabling the government to have such control or such regulatory power over these G space geographic names. Question for both of you. Thank you.

HIRO HOTTA: Yes, from .jp or the Japanese situation, I think the amendment of the law comes from the implementation of public good on the geo gTLDs as well. The government said that they have a kind of responsibility for such geo gTLDs because the geo gTLDs are in a format supported by the city or the prefecture or some local government. They want to be assured that they are running well by their report. I think that's the only aim for the government. It seemed that they don't want to regulate the registries.

VIKA MPISANE: I think I'll add to what Hiro just said but just point out that I think in our case, this particular ICT Policy is clear in accepting and appreciating the role of other entities including ICANN to say that ICANN has a responsibility of the gTLD regulation and it appreciate those parts. But as Hiro says, then there's the local part of it that says how to use this particular geographic TLDs must be in line with what government perceives to be correct approach because there are names belonging to that particular jurisdiction. It's really not transgression or a rejection of ICANN's role, but it's simply saying at a local level over and above your responsibilities to ICANN, this is what should happen.

YOUNG-EUM LEE: Yes. I'm not saying that the Japanese or the South African is trying to overrule ICANN's authority, but what if something happens in those regional names that the government sees as not appropriate? Then what do you think the government will or can do?

VIKA MPISANE: We'll have to cross that bridge when we get there. It will be nice to set some precedent and find out how to reconcile those conflicting interests. We are learning for us. In the case of .africa, we were involved to that. It's also becoming a very good

precedence setter to have a string that is belonging to a particular continent being held in a court in the U.S.

It seems that development is coming through and there's an appreciation in the U.S. that maybe the U.S. courts are not appropriate to be resolving this matter. We will have to take it as it comes, but at least as we anticipate from South Africa, we do not foresee it to be a likely major hurdle in the sense that we accept what ICANN does and that ICANN allows this flexibility in how you run your geo-TLD.

The government is really looking into that to say, for example, in the future, do we apply for an additional geo-TLD? If we apply, the government or this particular ICT regulator will be the one responsible for endorsing that and for setting up the operations of that in within the ICANN regulatory framework.

PETER VERGOTE: Okay. Rieke or Christian.

[CHRISTIAN ARMAND]: Hello. My name is [Christian Armand]. I'm from [inaudible], a registrar company in Denmark. I have a question for Erwin from Danish Internet Forum, or I have two questions. Now that so many organization spends time on answering or making

comments for your public hearing, here in India today on this public meeting, we had the conclusions from the Board. My first question is on your website in September, you wrote that you would make the decisions public on the website when they were available. I'm a bit surprised that now that they are public that they are, first, not on the website yet and, second, that all the organization that spend time on giving comments that we haven't got a reply yet.

ERWIN LANSING: There are people working on the official report that will be public. Yes. I'm not sure about the date but it will be soon.

[CHRISTIAN ARMAND]: My second question is that now that you are making it so hard for Danish registrant to register a domain, I know that a lot of my customers, they will use my service of a nice address in the U.K. or Norway to register domains. Aren't you afraid that you will get bad WHOIS in the future of all these Danish registrants that suddenly moved to the other countries?

ERWIN LANSING: Great question. It's not up to us. It's decided by law that we have to do this for Danish registrants. To me, it also makes no sense.

It's only 20 kilometers to Sweden. It would be easy to register a postbox there and avoid the law [by that way]. We are just upholding the law for Danish registrants.

For the foreign registrants, we can see that, to me, it also makes no sense because the real abuse is not coming from Danish registrants. If you really want to do anything about abuse, you should look into the foreign registrants so that's what we are going to look at.

[CHRISTIAN ARMAND]: Just a quick follow up comment. It's not in the Danish law that you have to use NemID for the registrations.

ERWIN LANSING: That's correct. That is correct. That will be because right now, as [Nigel] pointed out, there is this loophole where the name and address of the registrant is public, again, by law. You can find out the name of a natural person and just register a domain in his name.

We will send a paper letter to the registrant but then depend on the registrant reacting to us and saying, “I did not register this domain name. Someone abused my name and address.” That would be a way to close that loophole.

RIEKE POPPE: I also have a question. I am not as lucky as Michele that everyone knows me and I know every one of you. I am Rieke Poppe. I work at One.com. We are also one of the biggest registrars in Denmark. We also participated in both the oral and written hearing.

I have a question which is, what will the process be to find that better solution for foreign registrants? Will the registrars and/or the advisory board, which I'm also in, be part of this process?

ERWIN LANSING: Quick answer. I don't know and yes. We just know we have to do something, and we're not sure what it will be yet. Of course, we will talk to the registrars what we can do.

RIEKE POPPE: Great. We are very interested in participating. Also, is there a timeline for the implementation of the forced NemID?

ERWIN LANSING: No.

RIEKE POPPE: Thank you.

PETER VERGOTE: Annebeth?

ANNEBETH LANGE: Annebeth Lange, .no. I would like to follow up on Michele's and Thomas' privacy stunt.

MICHELE NEYLON: Stunt?

ANNEBETH LANGE: I think it's a really interesting idea because we have been working with WHOIS. The first time I remember was in Luxemburg in 2005. It was a really big meeting with the law enforcement. Since then, we have been working with WHOIS and never find out how to do it and then RDS and it's complicated, complicated, complicated. Then safe harbor, and now we have the shield.

We know that especially for Europeans, it's a big problem. I think it's a really interesting idea to turn it around and try to work on some other way to do it if we need WHOIS at all. That's also a question that we are discussing in Norway. We have too many

data. That makes problems and it creates more and more problem. Thank you for raising this. It's very interesting.

THOMAS RICKERT: Thanks very much, Annebeth. That's very kind of you. Many of you, I think, have been in the room when Fadi Chehadé did his first opening speech. He was addressing WHOIS as well. He was saying that there are two issues in the world that seem to be unresolvable, that's the Palestinian conflict and WHOIS. I'm not sure whether I think that's politically appropriate to say, but I guess it clearly demonstrates how tough this is. We've been struggling with WHOIS for ages.

I do agree. I've said it on other fora; I will repeat it here. I would like the idea of shutting down public WHOIS. The two customers of public WHOIS are law enforcement and the IP lawyers. They tend to take what's in the WHOIS at face value and start investigations, sometimes even go in and arrest people or so based on the information in there.

We heard from the example that [Nigel] was making that WHOIS is not and never was meant to be a reliable source of information about registrants. Even the registrar accreditation agreement with the validation requirements only helps a little

bit because sophisticated folks will be able to bypass that anyway.

I think we really need to rethink this and adding to the – I was about to say stupidity of the process and I don't mean it, but I do mean it.

MICHELE NEYLON: No, I'll say it for you, Thomas. It's okay.

THOMAS RICKERT: When we have WHOIS exemptions, these are made subject to public comment. Then you have IP lobbies – I have nothing against intellectual property – speaking against what's required by law. This is nothing that contracted parties can negotiate over. They have to be compliant, period. I think we need to find ways to make it easier for contracted parties to be compliant who all want to be good corporate citizens.

MICHELE NEYLON: I'm waving at the ccTLD people down the back who arrived in late. Roelof, looking at you. The WHOIS debacle, like you, it was the first topic that attracted my attention when I came to an ICANN meeting back in 2007. I made the mistake of opening my mouth, and I've been coming to ICANN meetings ever since. I feel

like this is like an alcoholics anonymous scenario like, “Hey, my name is Michele. I talk about WHOIS.”

It is a ridiculous situation that registrars and registries and backend providers have to negotiate with a California corporation to be compliant with their local law. It's absolutely ridiculous. In what reality do I negotiate with a private company about Irish law? Unless that private company is an Irish company, okay, maybe we can discuss some subtleties and maybe we can lobby the government together to get stuff changed. But no, it's nutty.

There are only two gTLD registries at present who have managed to fix the problem, .cash and .tel. .tel, as we all know, is a resounding success with millions of registrations. The guys from .cash spent years fighting ICANN before they were able to get it fixed. Maybe removing public WHOIS would solve a lot of things. I honestly don’t know. But I agree with everything that Thomas said which for Thomas is good. It’s like I'm agreeing with a lawyer.

PETER VERGOTE: Vika, was your question regarding WHOIS?

VIKA MPISANE: Yes, very much along the same question that they were answering. I wanted to find out from them, how do they think we should reconcile at least in the meantime these two conflicting situations? So, I'm covered.

PETER VERGOTE: Could you repeat that, Vika?

VIKA MPISANE: No. My question would have been, I would have asked the question in a more hypothetical to say, what do they think should be the appropriate model to this debacle of WHOIS?

MICHELE NEYLON: Remove public WHOIS, problem solved.

THOMAS RICKERT: If I may, I think as much as some might like to remove public WHOIS, it's likely not feasible. But I guess the solution would be to allow for contracted parties to run WHOIS according to their local law. Eurit does it in compliance with the European data protection regime, so that's perfectly possible. It's possible for other regions in the world.

We certainly do have the issue that a contracted party might have customers from other countries registering through their system. That's highly desirable. At least for Europe, we have court decisions for that as well. There was a decision by the European Court of Justice saying that even though Google doesn't have a fingerprint or might not have a fingerprint in all countries, they need to be compliant with the law their customer sits in.

I think law should be the starting point, and it should not be the ICANN contract being the starting point. I know contracted parties that receive breach notices, or TLD applicants, because they were saying that they plan do WHOIS in compliance with local law. Then ICANN said, well, do you really want to infringe on the contract? I guess that's a predicament.

PETER VERGOTE: Thanks so much. Roelof, the last question or remark is for you, and then we break for coffee.

ROELOF MEIJER: If it's inappropriate to ask questions, then I'll refrain.

PETER VERGOTE: Excuse me?

ROELOF MEIJER: Okay. So, I can ask a question?

PETER VERGOTE: Sure.

ROELOF MEIJER: Can I also make a remark? I agree with Michele about what he said of having to negotiate with ICANN. We are in this problem with .amsterdam, so I recognize what he said.

I don't recognize what Thomas says about solving the problem is getting rid of public WHOIS. I completely disagree with the notion that there are only two customers in public WHOIS and that's law enforcement and IP lawyers.

THOMAS RICKERT: Primary customers. There's statistical data out there.

ROELOF MEIJER: Those are what's primary there. Okay, because law enforcement and IP lawyers have separate WHOIS entrances for .nl, and our public WHOIS is used a lot. I'm sure, if we kill it tomorrow, there will be attempts to kill us the next day.

MICHELE NEYLON: I think, Roelof, when Thomas or myself say things like, “Let's kill public WHOIS,” we both know full well that it's never going to happen. It's more to provoke a reaction from somebody like you. You actually have solved – now, hold on. Don’t get upset with me. You can get upset with me later. You have solved the issue because you have a process in place in .nl that addresses the concerns of law enforcement. But there is nothing under the current WHOIS regime and the gTLD space that allows for that. There's no differentiated access. It's all or nothing.

That's the problem because, as an Irish company, I don’t want to end up in a situation where I am being forced to break the law. But every single time that somebody registers a domain name with us, that's effectively what we're doing.

Iron Mountain with the escrow provider that all registrars use with one or two exceptions, do not have any serves in Europe. All of the servers are in North America. At the moment, they're finally covered by the Privacy Shield.

ROELOF MEIJER: Michele, I get you. Let me make my final point. I don’t think it's good for a discussion if you come up with statements that you

know are not true or won't work but it's just to draw out a reaction. I think that's not a very useful way of moving forward.

PETER VERGOTE: Okay. Sorry to [head off] a very interesting debate, but we are going to break for coffee now. I would like everybody to be back in the room a bit before 11:15 because next sessions are going to start 11:15 sharp. Thank you. Thanks to all my speakers for their time and their dedication.

[END OF TRANSCRIPTION]