KOBE – ccNSO: Members Meeting Day 2 (3 of 4)
Wednesday, March 13, 2019 – 13:30 to 15:00 JST
ICANN64 | Kobe, Japan

EDUARDO SANTOYO: Good afternoon. Thank you, all of you, for being on time for this session. This is going to be a new session about legal topics. We are really lucky because – I am really lucky because we are having now a session with many things in common for most of us as registries, as ccs, that we are leading. Now we have one of our presenters coming here.

So we're going to have four presentations for different topics, legal topics, topics that have to be [day-to-day for] many of us. Please don't be shy. Participate all the time. You can ask questions to each one of the presenters at the you want. No need to wait until they end. Of course, share also your experiences in the topics they are going to present.

I think for us, I as the Chair have no incentives to offer to you more than sharing, of course, the knowledge and the experiences of our presenters. Thank you to all of them for collaborating with this specific session.

Now, without any more to say for now, I'm going to give the floor to Patricio, who's going to share his experience or their experience on transparency law and the .cl registry database.

Patricio, please.

A mic.

PATRICIO POBLETE: Thank you, Eduardo. My name Patricio Poblete. I'm Director of NIC Chile, the registry for the .cl top-level domain. I'm not a lawyer, and I never thought I would be one day speaking in a legal session. But anyhow, I'll do my best.

The topic is transparency law and the .cl registry database. What's the legal context there? NIC Chile is part of the University of Chile. It's not a separate entity at all. It's just a unit within the university. The university is a public university. It is autonomous but it is a public university. It belongs to the state.

They've researched transparency law in Chile since 2008, and that law was welcome by everybody. Its intention was to let the citizenship have access to the information related to the decisions made by the government – the procedures and the formation held by the government.

Well, there's a list in that law of all the entities that it applies to – all the ministries and such – and the public universities are not on the list, so we did not have to comply with the law for a number of years, until there was litigation on that.

Somebody asked to know the information about the salary of the Director of the University of Chile, citing transparency law as the basis. The university fought that for several years. It went as high as the Supreme Court and finally lost. So by interpretation, we had to start complying with transparency law with the university, starting in 2011.

Transparency in Chile, probably in other places also, can be active or passive. Active means that the university, in our case, has to publish certain information without being asked. It has to be done. It's published on the institutional website: salaries of everyone, financial information, procurement information, and so on.

There's also passive transparency. It means that anybody from the citizenship may ask for information and the university is under an obligation to provide that information.

But there are some exceptions that the law includes; things that have to do with national security or personal or sensitive information or when the cost of providing the information is disproportionate, is way too high. So there are, as I say exceptions.

Now, what does this all have to do with NIC Chile? Well, after a while, somebody realized that we were part of the university and therefore they could use transparency law to get the information

from NIC Chile. That's interesting to people there because .cl domains are highly visible in Chile. Close to 90% of the domains used in Chile are .cl. So it's an interesting target.

So, in 2014, we had the request from somebody who asked to please give him the full list of domain names, registrant .cl, plus the tax ID of the registrant , which is information that we had for everybody back then. We don't have it anymore for everybody, but at the time it was universal.

Now, at the time, our WHOIS was giving out much for information than it does today. So, basically, having the domain name and the tax ID could be used to get basically all of the database, and also, matching the tax ID, [you] could be connected to lots of other databases that were out there.

So we really thought that, if we said yes, we were putting a lot of our customers/users under a lot of risks that we could envision. By the way, if a request could potentially affect somebody in their rights, like privacy or things of that sort, we are also under an obligation to notify that third person so they can object. We have to do it within 48 hours and we have to do it by certified mail.

Well, at the time, we had, like, 300,000 customers. The thought of mailing 300,000 letters – actual paper letters – for certified mail was something that I couldn't even imagine how to do within that timeframe.

So we decided to send e-mail instead, which was something that we debated a lot because the law didn't say anything about e-mail notifications. But we did that anyway because we thought that was the only way to approximate complying with the law.

Then all hell broke loose. The thing became a big topic in the news/social networks, and somehow the person who made this request – which, by the way, had all the looks of a spammer – was outed. So people started harassing that person.

So, after a couple of days – well, because of our mass e-mailing of the customers, about 30,000 replied immediately, saying no way they would ever allow their information to be provided to this person.

So after a few days, the requester withdrew the request. Also, the same thing was done by several copycats because, after this became news, we also started receiving similar requests, "me too" requests. "I also want a copy of the full database," and so on. So they also withdrew their request and the thing died then.

In the years since, we have received similar requests, and we have denied them. In some cases – well, always the person who presented this request has a right to appeal in case of denial to the Transparency Council. In other cases, the Transparency Council agreed with our position.

Except now, which is the reason I'm talking today. At the end of 2018, we received a request for the full list of registered domain names, and nothing else. We refused, as we had been doing before, and there was the appeal, the complaint to the Transparency Council, and this time the council found for the requester and ordered us to provide the full list of domain names.

Well, providing the full list of domain names is something that we have avoided doing ever. We feel that there are many reason for not doing it, so we looked for ways to get out of this situation. We also had the right of appeal this time in the courts, but before doing that, why did the Transparency Council change their mind?

Well, for one thing, the people in the Transparency Council change all the time. They're political appointees. So maybe the people that are there now have a different idea. The reasoning was that there could be no possible harm if the list contained only the domain names and nothing else. That's what they said. "Just the domains. What's the problem?"

The users need not be notified because they had already authorized the sharing of their information as part of the registration process. So that went out with the mass mailing. And NIC Chile was already publishing a partial list of domain names, so why not publish it all?

So let's go one by one. What, is there really no harm if we only give out the list of domain names and nothing else? Well, our WHOIS is much more restricted today. Still, someone having the list of domains can get information and that can be abused. We also provide an interface for contacting the registrants. That can be used for spamming them and can be used for phishing. So feel there is a risk there.

Also, if someone has the list of all the domains, it makes life much easier for a potential attacker who could walk through the whole zone, looking for vulnerable servers, guessing server names – that's not too hard – and trying to find vulnerabilities in the configuration of those servers. It's not a big problem if they only have a few names, but it's a big problem if they have all the names.

We remember when NSEC3 had to be introduced, and that was because of exactly the same risk: having the possibility of walking through the whole zone, getting all the names.

So we certainly disagree with this reasoning that only the domain names is not a problem.

They also said, "Well, but users have already authorized data sharing." They cited part of our terms and conditions. The registrant authorized [Thick] Chile to make public the information of the domain name.

But they cited it only partially because the full clause says that this is exclusively for purposes related to the management of the .cl registry and the operation of the DNS. So it's not for anything. Just for things related to the operation of the DNS.

Now, it is an essential part of transparency law that the requester doesn't need to state why they want information, nor what they're going to do with it. It's supposed to be public information, after all, if it's under transparency law.

So giving it out without a condition that it be used for these specific purposes would be, for us, certainly a violation of the agreement that we have with each one of our users.

Third, what about this thing about the list of domains already being published? Well, there is something in our dispute resolution policy that encourages that complaints be brought early in the life of a domain, within the first 30 days. In order for that to operate, the list of the most recently registered domains is published – the last 30 days – and that is about 2% of the database that is published.

But we feel that it's hardly a basis to conclude that 100% should be public based on the fact that 2% is published. The abuses that could be done on the 2% would certainly be much more serious if done on the 100% of the database.

Certainly, we do see abuses on this 2% and it is a matter of concern. [We] would probably change some things in the future because, even if it's a small fraction – and it's mostly domains that are not yet operating because they're freshly registered – we do see abused on that small fraction.

So, in order to prepare our presentation [for the appeals], we did a quick survey, and many of you replied. I thank you very much because we asked you to say, "We're in this situation. Please help us out." We got 50 replies in just a couple of days, and we said, "What would you do if you were asked for the full list of domain names?" 82% said that they would refuse absolutely, like we were doing. 16% would accept with conditions. 2%– and that was actually one TLD – said they would give out the list without any conditions attached.

Now, for those that said that they would accept with conditions, what kind of conditions? Typically if the list was requested by a court or by law enforcement, which is something that we would also do. Our issue is with giving out the list without any conditions. If it is requested by a court of law, we would certainly be obligated to comply. But this was not the case in this situation.

Also, if it is for academic research. We also do that. We provide the list to the CERT, for instance – .cl CERT – for their research in

computer security/cyber security. But we have an agreement with them on how they can use that information.

Or if it was after signing an agreement to guarantee there would be no misuse of the information.

Well, those conditions to us of that 16% seemed eminently reasonable, so we wouldn't have a problem if it was like that. The problem is that there are no conditions in this case. The one reply that said, "We would give it out unconditionally" was certainly very firm in that position. They would give out anything that they have, no questions asked, no buts, no ifs.

So where are we now?

UNIDENTIFIED SPEAKERS: [inaudible]

PATRICIO POBLETE: No, I'm from Chile. Anything that's less than a 7 I don't feel.

EDUARDO SANTOYO: [inaudible] just to see if you are awake.

PATRICIO POBLETE: Yeah. And the building is designed for this. Like I said, I'm Chilean. If it's less than a 7.2, I don't feel it.

Okay. Are we …

EDUARDO SANTOYO: Yeah. Please.

PATRICIO POBLETE: Okay. So where are we now? We filed an appeal at the next higher level, which is the Court of Appeals. The court could have refused to hear the case. Why? The law makes it very hard – it's an uphill battle – for the part of the government to fight an order from the Transparency Council.

There are many conditions on that. Apparently, we managed to fulfill all those conditions because the court accepted it and put it in this docket. In itself, it was a small triumph to pass that hurdle.

Now we're waiting for a date for the case to be heard. If we do not succeed there, we could potentially go to the Supreme Court. It depends. We have to see. We are preparing for our day in court. We hope [they will] agree with our reasoning.

The Transparency Council filed, just a couple days before I traveled, their reply to our case. All the things that had to do with risks to the cyber security of our customers they didn't say anything at all about. They ignored that part, which is something

that we feel, when we have the opportunity to present the case in front of the court, is something that we will have an opportunity to stress. Cyber security is a matter of great concern in Chile. Recently, there have been several cases of attacks to banks or other institutions. So we feel it's something that we have to stress.

That is the situation at the moment, so there's nothing else I can say now, except that we're mildly optimistic that we will have the Court of Appeals agree with us.

That's it.

EDUARDO SANTOYO: Thank you very much, Patricio, for sharing with us this interesting case. I just want to ask for the audience, what do you do? If you are in the [eager] opposition, not in Patricio's position, because, of course, Patricio was [inaudible] governmental institution. But now we have different conditions in our different organizations. Then it is important to see what should Patricio should do, but what do you think you have to do according to your [honor]? You [provide an answer for this guy?] Or you will expect to receive for an order from an authority to proceed?

So raise a hand, those of you who normally could proceed giving a list of domains under your registry.

Okay.

UNIDENTIFIED MALE: [inaudible]

EDUARDO SANTOYO: Okay. Now are you hearing me?

UNIDENTIFIED SPEAKERS: Yes.

EDUARDO SANTOYO: Okay. What do you do? You've been a registry who has been requested to give a list of domain names registered under your domain. You will provide that list?

PATRICIO POBLETE: Eduardo? If you want to put them in our exact position, I have to stress that that request comes without any guarantee that that information will not be misused. So it's just a request that doesn't carry any non-disclosure agreement or anything at all. Just unconditional.

EDUARDO SANTOYO: Yeah. Okay. But we are not all [polling] institutions or governmental institutions. So I want to ask if some of us will proceed with giving the list of domain names, as in [the situation] presented to NIC Chile.

Anyone? Raise your hand.

Nobody – ah, yes. Thank you. What do you think will happen at the end? I wish I had a crystal ball. You don't?

That is an interesting case because I guess that probably not for the full list of domains but everyone, of course I guess, in this room has received at some time a request for information about the registration update of your domains, probably in some cases with their personal data included or, in this case, just, for instance, the list of domain names registered under your registry.

Vika?

VIKA MPINASE: [inaudible]

EDUARDO SANTOYO: Yeah. Please.

VIKA MPINASE: I think we have had requests from time to time for the list of domain names in .za, but that was not based on the law. It was somebody who said, "I would like (maybe) the zone file or the list of domain names," and so forth.

For us, exactly based on the law, we say, "We can't give you that list because there are issues of privacy." Before GDPR kicked in, we already had in South Africa the Protection of Personal Information Act, which required us not to disclose anything unless there was a clear reason. And it also provides mechanisms for people if they wanted that list to not resort to courts to compel us.

So we fall in a legal environment that tends to protect more the individual than the commercial interest when it comes to personal data.

So we would definitely be standing exactly as said on [cld], saying, "No, we can't disclose that."

But quickly also, one thing I would like to ask from Patricio is, did you check any case law in Chile with regard to such a request, maybe not the domain name list because that [inaudible]? Have their been cases where, for example, a certain public authority was required to disclose full information on something that you could rely on?

PATRICIO POBLETE: There are precedents going one way or the other. The one that went the way we wouldn't like was with the querent of the IRS. They had to release the full list of properties, real estate, and their owners a few years back. And there are other cases that happened the other way. So it's hard to tell from the precedents.

There's no such things as precedents. Each case is decided on its own merits.

UNIDENTIFIED MALE: [inaudible]

PATRICIO POBLETE: Yeah.

EDUARDO SANTOYO: Okay. Thank you. There are more questions for Patricio or more things that you want to share with all of us?

Okay. Thank you, Patricio. Thank you very much. And thank you all who replied to our survey.

Now we are going to have Peter sharing with us a very brand-new procedure they have in .be to notice and take action for domain names.

Thank you, Peter, for coming here to share your experiences.

PETER VERGOTE: You're welcome. Okay. Sorry, but after four days of ICANN, my voice is starting to break up. So some among you might even like that thought, but I'll still try to hold on to give my presentation.

Next slide, please. So what I wanted to share with you is somehow a bit of a plunge in the unknown because I think that, for a very large part, our approach is similar. If somebody comes up to us and asks us, "Please take down this domain name," or, "Please redirect this domain name to (whatever-kind-of-[warning]) page," I think our reaction would probably be similar: "No, we are not going to do that unless you provide me with a valid court order."

So what we have been doing is we have been negotiating with what we call the Federal Public Service of Economical Affairs. It's probably equivalent to your Ministry of Economical Affairs and Consumer Protection. But it's a government agency. We have been negotiating with them a procedure that would provide them with a possibility to give us direct instructions without having to go through law enforcement and to provide a subpoena or a warrant. So basically that's the essence of what I wanted to share with you today.

It has been formalized in a cooperation charter so that we have certain guarantees, certain rights and obligations, for each involved party. This is something that obviously comes on top of our other procedures. I think nearly all of us have some equivalent of a bad WHOIS procedure; if the registrant data are manifestly incorrect, we can revoke the domain name. I think all of us try to assist in the execution in local court orders and subpoenas and similar things. Some of us probably have specific procedures to deal with malware abuse, phishing – those kind of things. So we have that as well, but this comes on top of that.

Next slide, please. So you probably have been hearing this before from me. A large chunk of our legal policy is based upon risk analysis. As you can see on the left side, you have interactors. You have consumers that are victim of a fake e-commerce site. You have IP rights holders that have been victimized because somebody else abuses or infringes on their trademark. So you have interactors from that side that could levy pressure on the equivalent of your Ministry of Economical Affairs and Consumer Protection. They interact with the registry, asking a certain action. You would refer. You would deflect. You would say, "No. Go to the top of the pyramid. Go to the public ministry. Provide me with the necessary documentation."

And the biggest risk you have there is the lightning bolt. It's delay because it's a kind of a black box. You don't know what's on the

urgency list on the agenda of the public ministry. It could take weeks and weeks before they provide the subpoena. But of course, if you're dealing with something like a fake e-commerce site or a phishing attack, it continues to do the damage to your consumers and whatever kind of other Internet users.

Next slide, please. So what we did is we tried to come up with a solution, which is that notice and action procedure. So how does it go? Well, basically, we get a notification from the Ministry of Economics. As soon as we get it, we process it in within one working day. We do not revoke the domain, but we disengage the name server functionality and we redirect it to a warning page that we host on a server. But the content of that warning page is actually a warning from the Ministry of Economical Affairs.

This triggers our standard 14-day period for the registrant to respond to it. Let's assume he doesn't respond. So after that 14 days, we send up a follow-up reminder to the ministry, asking them, "Have you received any word from the registrant? What should we do?" It's important that they need to reconfirm that the breach is still ongoing. [After] any kind of step in this procedure when we do not get the necessary reconfirmation, automatically the referral to the warning page will be disengaged.

So suppose that we get a confirmation. We – well, the FPS economy has two weeks to deliver us that confirmation because

they probably have to re-examine if this breach or infringement is still going on or not. So suppose we get the confirmation. Then we will keep the redirection active for another six months. Then we area simply going to revoke the domain name. It will go in our standard 40 days. What is the equivalent in gTLD Land? It's a grace period or something like that? Anyhow, it's a state where you can still reactive the domain name. Then it gets finally deleted.

Next slide, please. Important. This is not something that can be activated like this. It's a last resort procedure. It means that our counterpart from the governments has to exhaust his own procedures. If the application of those procedures does not help to remedy the situation, then they can activate this procedure.

Second important remark. This is not for everything. This is not for minor things. This is not about an e-commerce trader that happens to forget to put his [fee-A-T] number somewhere on his website. It's for things that are connected with distortion of the market's equilibrium or when there is a menace, a real and imminent menace, to consumers and so a threat to consumer protection.

Why do we do that? Well, first of all, because we think that, as a registry, we have a fiduciary duty to try to uphold the quality of our zone and to exclude it from abuse in the best way we can. So

it fits within our mission and within our goal as a public trust company, if you want.

But we need it to have certain guarantees before diving into this. The guarantee that we got is that, although we cannot prevent somebody from suing us – suppose that the registrant says, "Well, I do not agree that you have redirected my domain name to a warning page. You're hurting my business. You're causing damage," so we cannot prevent that person from starting litigation to us. But as soon as this happens, in the notice and action charter it is stated that the government will step in. And if ever we got convicted to pay damages, they will compensate for it.

So, basically, this procedure is layered. It's proportionate. We do not go as far as to revoke the domain name immediately because, if we revoke it, if we delete it, and a couple of weeks afterwards there is a litigation that is started against us, the damage can already be considerable. So we prefer to have something that is reversible.

Also, we do not make it dark. We redirect to a warning page. We have sufficient stop elements in the procedure that can return to the original direction and the original linkage with the website.

Next slide, please. Okay. A small word about legal liability. How am I doing on time? Good?

UNIDENTIFIED MALE: Good.

PETER VERGOTE: Okay. Thanks. So why did it take us so long? Because we have been negotiating this for at least five years. Well, obviously, things got complicated and blocked – okay; thanks – when we started discussing legal liability. So we managed to remove that, and now we get a sort of coverage when we execute the instructions exactly as they have been delivered.

This of course covers us not if we do something wrong. If we get an instruction to redirect ABC.be and instead of that we are redirecting CAB.be, well, clearly we're not covered for that.

But if we stay within the boundaries of the instructions that we receive, our legal liability is covered by the notice and action charter.

Next slide, please. Okay. Cases. Well, the notice and action procedure has been activated on [4th] of December. In December, we didn't receive any cases. We received two in January. None in February, and none in March so far.

As you can see, in total, we have two batches, with the second one being the most significant one because it was more than 100 .be domains in one single case.

As one might expect, reaction from the registrant? Zero. It's typical cases. It's about deleted domain names that get re-registered and directed to a fake web shop.

I think the last two slides are just screenshots. There you have it. That's how your typical fake e-commerce shops look like. They're getting better and better, so obviously the threat for consumers are getting more and more significant as well.

Next slide, please. So what do we do? If we get instructions for a domain name that is pointing to such a website, we redirect it to a page that looks like this to alert the Internet users.

Final slide, please, if you can. So next steps. Well, it's still early days of course, and we only have had two cases so far. But we would be willing to look to enhance this procedure with other government counterparts, like – I don't know – the Ministry of Finance, the Ministry of Public Health. But of course, under the same conditions. I mean, also they have to accept that we want coverage for our legal liability. And our counterparts, being whatever kind of government agency, need to have the competence to actually do something with the infringements. If

they cannot act upon it themselves, if they lack that competence, we are not going to step in and dos something on their behalf.

That's it. Any questions?

UNIDENTIFIED MALE: [inaudible]

UNIDENTIFIED FEMALE: Thank you very much, Peter. I actually have three questions, but if you decide that it's too much, you let me know and I will finish later.

EDUARDO SANTOYO: Please proceed.

UNIDENTIFIED FEMALE: So, first, what is the Public Ministry on this slide with a triangle [inaudible]?

PETER VERGOTE: It's your public prosecutor, the one that sets in public prosecution for criminal affairs but also for civil affairs.

UNIDENITIFIED FEMALE: Okay. Second, you mentioned that there might be serious and minor infringements. Who decides which infringement is serious and which one is minor? Who and how?

PETER VERGOTE: Thanks. An interesting question. Well, the first filter obviously is public service itself, the Ministry of Economical Affairs. They have to assess, "Is this something that we can deal with based on a notice and action procedure. So they're the first filter, but obviously, if something comes in, we are going to do a quick check as well: does this fit the parameters? As parameters here, I have limited myself to a couple of bullet points. They're more elaborated in the notice and action charter itself.

UNIDENTFIED FEMALE: So if DNS Belgium finds this infringement minor, you would start discussion with the authority?

PETER VERGOTE: We could, yes.

UNIDENTIFIED FEMALE: Okay.

EDUARDO SANTOYO: Okay. Thank you very much. [Nick?].

[NICK]: Hi. Hi, Peter. Thank you. Very interesting presentation. I'm interested in the redirect page most specifically because it's something that we are working on. I wanted to understand more the legal basis for the changing of the name servers of the registrant's domain name. That is in the law. Is that right?

PETER VERGOTE: No. It's actually in our terms and conditions.

[NICK]: Okay. Thank you. Secondly, obviously it needs to go through a live website page. I wondered whose name servers are there? Who's hosting that page? Is that your—

PETER VERGOTE: We are.

[NICK]: So you decided to host it. And it's the same language for all your suspensions. You don't differentiate for any reason. You just have a set page.

PETER VERGOTE: Yeah.

[NICK]: I'd be interested in an English translation. My Flemish isn't very good.

PETER VERGOTE: Ah, I think it was in English as well.

[NICK]: Oh, is it?

PETER VERGOTE: Yeah. I think we have four languages on there.

[NICK]: Okay. My eyesight is obviously not good enough then. Okay, thank you.

PETER VERGOTE: Only [West] Flemish is lacking, but we've been working on that.

[NICK]: Thank you.

EDUADO SANTOYO: Okay. Thank you. Okay, last two questions from Vika and [George].

VIKA MPISANE: Sorry. Peter, in one of your slides, when you said that this is a last resort measure. Once the FPS economy is exhausted, it's internal steps. And in one of your slides, you then stated two things or I suppose two crowns that they must first exhaust it before they refer this to you, which was distortion of market equilibrium.

PETER VERGOTE: Sorry. Come again?

VIKA MPISANE: You had one of the crowns of the areas that FPS economy must prove in referring a matter to you. You had the distortion of market equilibrium and then if it's [managed by] consumer protection.

PETER VERGOTE: Yeah. That was basically the two large type of situations of abuses that can be used to deal with this.

VIKA MPISANE: Are these defined in any law in Belgium?

PETER VERGOTE: Sorry? No, this is defined in our notice and action charter.

VIKA MPISANE: Yeah. I'm saying for FPS. Who determines if it's a distortion to market equilibrium? Is it DNS .be or is it the FPS economy?

PETER VERGOTE: The first filter is themselves. They have to evaluate, "Is this something that we could deal with based on our notice and action cooperation with the registry?" If they say okay, it takes the box. They give us the instruction, and we do the same kind of evaluation. We check, "Is this following with the scope of our notice and action cooperation?"

VIKA MPISANE: So my question then is the definition of what distorts market equilibrium. Is it defined in a policy or law?

EDUARDO SANTOYO: From the institution. From the ministry of that.

VIKA MPISANE: I would suppose at that ministry level, but the question is, is it based on a law?

PETER VERGOTE: Yeah. It is based on the – how would I put it? – the [courdic] of economical law.

VIKA MPISANE: Okay. Because that was worrying me a bit. At least if it's defined in the law, at least gives me comfort that it does not lead to subject assessments of what distorts the market.

Okay. My last question is, you touched on the issues of risk to DNS .be. Does this mean now in your budget you have to have provision for potential legal risks on these matters, assuming somebody may come and sue the FPS economy and join you to the action?

PETER VERGOTE: No. It's not that much tied to budgeting and to finances. It's more the philosophical approach. As a legal, you could do two things. You could say, "My primary function is to try to shield off from liability as much as I can." Basically, that would say, "For everything that they come asking me, my preferred answer is, "No. I'm not going to do that because this is going to bring liability to my doorstep.""

We do it slightly different. We balance legal liability on one hand and the risk tied to it. So if the benefits are far outweighing the legal liability, we would take the proactive part.

VIKA MPISANE: Okay. Thank you.

EDUARDO SANTOYO: Thank you very much. Last, a very short question and a shorter answer. [George], please.

[GEORGE FIGER]: All right. First of all, thank you very much, Peter, for a very interesting presentation. I wish I had a ministry like this, taking the liability. That is key to all the solution of the problem.

You've been stating that you do not get any reaction from registrants. Probably the reason for that is you do not properly reach them. So what I would like to know is how do you make sure that you've got the right address for the registrant? Are e-mail addresses mandatory? How do you contact your registrant?

PETER VERGOTE: Well, we send them an infringement mail. So—

[GEORGE FIGER]: Snail mail?

PETER VERGOTE: No, e-mail. If that e-mail address is not correct, which could be true – I don't know any figures by heart, if we had generated bounces for those hundred and – what is it? – fifteen cases that we treated so far. But even if the e-mail address would be incorrect, or terms and conditions very clearly say, "Your registrant contact data should be up to date in case the registry wants to reach you," it's both written as a general obligation in the terms and conditions and more specifically in a separate article. It has been in there since the earliest versions of terms and conditions. It says, "You need to have a working functional e-mail address so that we can …" So if he hasn't done it, he is yet breaching the terms and conditions through another article. So I would say that we're pretty covered.

[GEORGE FIGER]: Thanks.

PETER VERGOTE: You're welcome.

EDUARDO SANTOYO: Thank you. Thank you very much. Thank you, Peter.

PETER VERGOTE: You're welcome.

EDUARDO SANTOYO: Thank you. Now we're going to have Ann-Cathrin sharing with us this piece of dealing with the illegal content in .no.

Please.

ANN-CATHRIN MARCUSSEN: Thank you.

EDUARDO SANTOYO: Thank you.

ANN-CATHRIN MARCUSSEN: My voice has also reached the almost-end-of-ICANN status, if I'm starting to cough, you will bear with me.

We can put the next slide up. So, for several years, we have been working with our own view on how should we deal with illegal content. It's complicated and it's something that we started already back in 2016. So the heading here was what we called our first national Internet Governance Forum. There's something – a line – that we don't like. That was the first time we actually got

our law enforcement agencies, the government, and stakeholders in Norway together to discuss this.

I can click? Ah, okay. Thanks. You will see some Norwegian headings here as well. This is media, of course. They were very interested.

So back then, in 2016, we started out and we didn't have any clear view of where we were going, how we were going to do it, except we didn't want to judge content. We didn't want to do anything with content. So that was our basic starting point.

So of course we tried to give information about what happens if you take down or block or redirect domain names, trying to give all the stakeholders out there in the society the message to: "Try to go to the source. That's always the most effective thing." But of course that is an increasing pressure; to go to the domain name, dealing with the infrastructure, instead of going to the source.

So … here, yes. So, basically, the legal background for domain names and our Criminal Act and the Criminal Procedure Act in Norway gives us two possibilities. One is to seize a domain name while law enforcement is actually investigating a criminal case. Then there's also a possibility to make a final court decision, if the court would like to do that, to forfeit the domain name.

Now, we tried to work hard with the society and the governments to underline that, in our view, the domain name sort of exist does not exist before it is held by someone. So, as a starting point, it's always the domain name holder that should be the subject of a criminal case. We as a registry should not be involved. We should not be under litigation or sued – anything like that. We should not be a part of the criminal case. So that was also one important measure for us: to try to achieve that in our relationship to law enforcement and the rest of society there.

We also have this nice Supreme Court decision from 2009. We've been actively using that for as much as it's worth. That was a case of seizure of a domain name. The Supreme Court says … I'll go here … oops. Sorry … yeah, I think that slide is … yes. No, there it is. This is quote on the top there from the Supreme Court. "Norid does not undertake any control of the content of websites, nor does it have any mandate to react to websites that may appear to violate the law. It is up to the police and the judicial system to do this." So that was basically another good starting point for us, we think, but it's hard to get that message through to stakeholders, which I'll come back to.

So we've seen some cases where law enforcement starts an investigation. So we then entered into contact with them, had meetings, brought our tech guys, and invited ourselves to them. I think we actually managed to get their trust, so they actually

asked us to advise them. So that was a very good start for the final case that we now almost didn't do, coming back to that.

So, basically, what we tried to do is get law enforcement, on a voluntary basis for them, to enter into the domain name registration. The thought behind it was that we wanted to get paid. We didn't want the domain name to be just there in the hands of the criminal or suspected criminal. We wanted someone to pay because we had a lot of cases where the domain name holder was under criminal investigation and he didn't pay. So it took us two, three, or four years with loss of income on that little domain name. So that was one of the background thoughts for trying to get law enforcement into the registration holder as domain registrant.

We also had the thought that, when a domain name has been seized, it has been subject to criminal investigation, it might not be nice for future registrants to immediately go into and buy that domain name or hold it. So we were thinking of a quarantine period. So, basically, we landed on two years, but that might change. We're not quite there with that.

So here we see the Supreme Court quoting again and then also, of course, the cooperation. We want to be helpful, like Peter's approach, as well, but we have to make sure that we don't get

into liability problems with economic or other [reputation] … here.

So we tried to provide as much information as we could. We tried to reach out to the Judges Association, all kinds of law enforcement agencies, and this is the handbook that we've made. I think also it's translated into some more general thing on the CENTR webpages. So you're all free to copy it or use it for yourself if you would like to. It's explaining how it functions and also stressing of course that if you do take down or block or somehow take away one domain name, you take away everything that's under that domain name.

So then we had the first court case of confiscation here. I'm not quite sure if it's final yet because there was an appeal period of 30 days. So it is running out in these days. It might be final. But this case was about the popcorn-time.no, which was used to host a website – not host, but the domain name was linked to a website where there was information about how to reach popcorn-time, which is of course viewed as an infringement of copyright.

So if was a challenge, I would say, to – we were contacted by the law enforcement agency and the prosecutor and tried to assist them with facts. You could see the quote is there in the middle. "If a domain registration is forfeited, the domain name will be transferred to Norid." That was the judge's take on it, which was

back to zero. Back to square one. So that just shows how extraordinarily hard it is to get the message in.

Now, luckily, the verdict itself says that the law enforcement agency should just handle the forfeiture in some practical ways. So we were happy with that.

So, basically, the end of the story is that they are now – law enforcement – per the day of the verdict are the domain name holder and they may then continue to be so. Or they may want to – let me get it – yeah. They may delete it if they want to. Then we will keep it for two years in a quarantine after deletion.

But they may also sell it. That's according to the Criminal Procedure Act. So, basically, forfeitures [as] the result of illegal criminal actions, back to the state, doesn't very fit very well on domain names. But anyway, they can choose to terminate it, but they have to pay us every year. And of course, we will then keep it, as I said, for two years.

So this last slide. These are links that you can go into and click on if you want to. You see the third bullet point there, Routines and Procedures. There you will find a description of the procedures that we have. So far, law enforcement follows them. I don't know if they think it's law or something. I don't know, but we are very, very pleased that they are listening to us and with the good

cooperation with them. And we hope popcorn-time is final and that would be our first confiscation of a domain name.

Thank you.

EDUARDO SANTOYO: Thank you, Ann-Cathrin. Questions for Norway?

How many of you are familiar with [Configure] Operation or Avalanche?

Yeah, there's a lot. Because I agree. There needs to be more activity from law enforcement authorities in order to protect people from abuse on the domain name system. Then it is an invitation for all of us to think how to establish procedures in order to collaborate with the system. That's good examples we had here with Norway, with Belgium. Of course, the other one is [Configure] or Avalanche. They are operations where the law enforcement authorities is asking to block the domain names before they could be registered by anyone.

Vika?

VIKA MPISANE: Thank you. To .no [operator], you said an alternative is you could sell the name on behalf of the law enforcement authority. Is that

you selling the name or the law enforcement agents that sell the name?

ANN-CATHRIN MARCUSSEN: You mean sell it? The procedure goes like this. If the police want to seize the domain name, they will enter into the contract, find themselves the registrar first, and then do as a normal registrant will do. Then they may put up a warning site. They might do whatever they want with it. Then, if the final court case says this will be forfeited, the police may then still choose to stay on as a registrant, or they can sell it.

VIKA MPISANE: Oh. It's just the police that may sell.

ANN-CATHRIN MARCUSSEN: Yes. The police may sell.

VIKA MPISANE: [inaudible] some form or a registrar or a sale of some sort.

ANN-CATHRIN MARCUSSEN: Well, they choose a registrar like anyone else.

VIKA MPISANE: Okay. Then the last one was, in terms of your policy, you also stated that these types of names are quarantined for two years. Any prohibition against the same holder after two years re-registering the name?

ANN-CATHRIN MARCUSSEN: The police will know that, if they choose to delete immediately after the course case – for example, we don't do know what they will do, for example, in this popcorn-time case. They might choose to hold it for two more years. Then, when we get deletion, if they want to delete it or not hold it any more, we will keep it in quarantine two years after that.

VIKA MPISANE: But there's no prohibition of the same guy now re-registering it?

ANN-CATHRIN MARCUSSEN: Yes. In these two years. It's no revenue for us or payment for us.

VIKA MPISANE: Okay.

EDUARDO SANTOYO: Thank you. Now we have a dual Abdalla and Barrack, who are going to share some legal issues for the ccs in Africa. The floor is yours.

BARRACK OTIENO: Thank you very much. Good afternoon. Barrack again Abdalla. We are not lawyers. So when you're not a lawyer, you need an alibi to assist in your defense. But of course, we have learned friends like Vika from the African continent on the floor, who I'm sure will help chip in from time to time.

So the presentation we are going to give is based on some interviews we did with AFTLD members that we chose across the sub regions and not east, west, and south for purposes of this presentation. The reason why we would registries from the sub regions is because we have varying legal environments across the different sub-regions on the African continent, or regional economic communities, if you may.

Again, let me say that, in the past five years, AFTLD has been working very closely with the Africa Union, ICANN, and the Internet Society in helping to build a harmonized legal and regulatory framework across the African continent. But for purposes of time, I'm just going to touch on some of the issues that we have been handling jointly.

Most of this has been around capacity-building, training of law enforcement officers, and training of lawyers. We don't have as much capacity as probably Belgium or the European Union has. That is a legal mindset, to really understand and appreciate some of the issues that ccTLDs are concerned with.

So, basically, we'll touch on some of the work that we've been doing and the trends we've been seeing on the legal front, and then Abdalla will talk about some of the practical issues that are affecting country code top-level domain registries.

For starters, let me say that, right now, we have approximately 450 million Internet users on the continent. I'm using statistics from the Internet. Wild stats. That's between 35 and 40% penetration on the continent.

The other thing that I would like to say is we are noticing a trend. Most multinational organizations – the social media giants, so to speak – are right now in investing in a lot of policy and legal officers on the continent. So it is an area that is actually growing, or there's a lot of interest, largely because most of the Internet users access the Internet or use mobile phones to access the Internet.

So in 2014, the Africa Union members adopted the Africa Union convention on cybersecurity and personal data protection. It's

referred to as the Malabo Convention. I touched on this in my earlier presentation.

So the main objective of this convention is to establish essential rules for the digital environment, as well as a harmonized legal and regulatory framework across the African continent.

Of course, not all countries have ratified this because, again, it's a political process. Also, Internet penetration in the respective African countries is a bit slow. But this convention, once ratified or acceded by most of the African countries, is going to have a profound effect on the domain name industry or the country code top-level domain name registries on the continent.

So the convention is open to all member states of the Africa Union for ratification. So, currently, we have just a few countries, most of which are members of AFTLD. That is Senegal, Guinea, Mauritius, and Ghana that have ratified the convention. When I say they have ratified the convention, at least they have a data protection commissioner or commission in place. Of course, other countries, like South Africa, [again], have legal instruments in place for personal data protection. Nine countries have signed the convention. I have listed the countries there: Benin, Chad, Comoros, Congo, and the rest of the countries that I've listed there.

So, for those that have been following cybersecurity and legal developments, this convention has borrowed heavily from the Budapest Convention. There's a lot of work being done by the Council of Europe, supporting the African Union in capacity-building efforts.

So the main parts of the convention are basically listed under the categories that I've put up there: electronic commerce, protection of personal data, promotion of cybersecurity, and combating cybercrime. Then we have additional provisions, of course, that also address the area of electronic commerce.

So we tried to compare – again, as I mentioned in my earlier presentation, for those that were there, most of our registries have also had to comply to GDPR provisions. Of course, because a significant number of registrants in the region are from the E.U., I don't want to belabor the point on GDPR.

So what are the similarities between the E.U. convention and cybersecurity and the African convention? Both seek to harmonize data privacy laws across Africa and Europe. When I looked at both conventions, this is what came out prominently. They also seek to protect and empower Africa and of course E.U. citizens' data privacy. They also seek to reshape the way organizations across the African and across the E.U. region approach data privacy.

Again, some of the key issues that are driving these legal and regulatory developments are that many African countries have signed economic partnership agreements with the European Union. You can check the EPA fact sheet on that website, Europa.eu. Again, a significant number of registrants in African ccTLDs. And of course, the gTLDs are from the European region, and thus the ccTLDs are actually compelled to be GDPR-compliant. From a political standpoint, soon, as more countries ratify the Africa Union convention, they'll also have to comply to provisions of the convention.

So Abdalla will take up the next part, which speaks to the trends.

ABDALLA OMARI: Thank you, Barrack. We did a survey from AFTLD members, about 15 registries, where we had to do Skype calls with them so that they respond. Among the 15 whom we contacted, 13 answered all the questions.

The findings from the survey were that the majority of ccTLDs have a legal resource on the Board. The reason is that a good number of ccTLD can't afford to have a legal officer on their payroll. So what happens is they do it on a volunteer basis so that a legal officer can join the Board and assist the ccTLD from the Board level without pay.

Also from the findings we found that, when the number of domains increased their zone size, some of them now start to creating a small legal resource within their ccTLD. So the smaller the number of the zones or the domains, the more likely there'll be no legal officer. But the big registries, like South Africa and Nigeria, and Egypt, have started developing a legal department in between.

So the smaller ones have contracted legal services by way of having a legal secretary attending Board meetings. So you can see that the access to continuous legal advice for most ccTLDs is a challenge. Hopefully, the ccTLD across Europe and America may assist AFTLD to update our legal capacity within our registries.

The common legal issues which came out of the survey were trademark infringement, dispute resolution, and handling requests for registrant information.

Now, on the third bullet point, usually for most registries in Africa, an election year is a very fearful year. That's the year when you get a lot of requests to bring down domains and so on. Any person who has dealt with the high offices will know, when they are dealing with the high offices, their legal processes don't matter. So what matters is how good you are in leadership and the ability to negotiate with them, telling them it will not benefit the country

if you bring down certain domains which are perceived to a threat to the processes.

Although some countries, like the DRC (Congo) – a month ago, when they elections were there, there was a complete Internet shutdown for about three weeks? Yeah, for about three weeks. So you can imagine what happens to the ccTLDs. And a few other countries.

So those are the semi-political/legal challenges which are there. So election years are fearful years for ccTLD managers because you really need to be in a position to protect your registrants.

Cybercrime. Current challenges are there, but I think it's not a very big issue because of the number of domains in the continent. And we don't hold a lot of content, so they're not as serious as they are in the other parts of the world.

We have had some ways of addressing the challenges. Especially we'll thank ICANN. ICANN has come to Africa and has had a few conferences for capacity-building. There was one in Cotonou, Benin, and there was one in Harare, Zimbabwe, and there was one in Nairobi. Those workshops, although they are far and wide, have really assisted to increase the capacity of legal knowledge within ccTLDs. More needs to be done, but the few players who have come to hold our hands we appreciate.

The other challenge is the lawyers in the continent, and I think Vika can attest to that. Understanding ICT issues is a big problem. So you may get a legal expert to assist you, but being able to put ICT challenges into a legal context becomes a problem.

An example is the elections we had in 2017 in Kenya. Somebody contested to have the data downloaded, but a lawyer convinced the judge that it will take over a month to download data, which can take only a few minutes. They got the [injunction] to hold the process for a month. ICT players found it a big joke. But, you know, it's the knowledge gap. So it's a serious issue across the continent.

So that's it. If you have questions for us, we'll be glad to take them.

EDUARDO SANTOYO: You don't have lawyers, but you have lions there.

Okay, Abdalla and Barrack. Questions for guys from France and Africa?

[ABDALLA OMARI]: Questions or additional comments from Vika. And he will answer himself.

UNIDENTIFIED MALE: That's the problem.

EDUARDO SANTOYO: Thank you. Thank you very much. Additional questions for our presenters? We have a couple of minutes that we can use to share more information with them.

Leonid, please.

LEONID TODOROV: Leonid of APTLD, just for the record. When talking about UDRP, I think that's a very, very important issue Asia-Pacific as well. In this regard, I just want to tell you that there is an excellent expert with whom we have actually held a webinar for our members. Unlike many experts, he's not only talkative, but he also knows how to deliver material in a very consistent manner. I didn't know if there is anyone from the Serbian registries because these guys – yes. So you better contact Vladimir because that gentleman is associated with that registry. Absolutely excellent walkthrough. Then everybody is perfectly aware of how to address that issue. Just a quick comment. Thank you.

EDUARDO SANTOYO: Thank you very much. And thank you very much for the offer.

Okay. As I see it, it is really important to have this new session on cc meetings. Legal issues are really important and, every day, have more importance in our organizations. Then sharing experiences about how are we dealing with these issues has become and will become really an important thing in order to have a better performance in our activities in our own organizations.

Thank you very much. And now we have a break until 15:15.

Okay. Thank you. Thank you, all. The earthquake's epicenter was 20 kilometers to the south of Kobe, and it was 5.2.

UNIDENTIFIED FEMALE: Nothing to worry about.

EDUARDO SANTOYO: [inaudible]. Thank you, all of you, for standing here for this session. Thank you.

[END OF TRANSCRIPTION]