BARCELONA – ccNSO: Members Meeting Day 1 (5 of 5)
Tuesday, October 23, 2018 – 17:00 to 17:45 CEST
ICANN63 | Barcelona, Spain

PETER VERGOTE: Alright. Ladies and gentlemen, can I ask you to take your seats, please, so that we can start with the last session of today which is going to be mildly focused on GDPR. I say mildly because two of the three presentations are directly involved with GDPR while we took the advantage of bringing a very recent privacy-related case in dot-NZ to the attention of the membership. So, that was an opportunity we just could not let go. So, it's GDPR and beyond. We'll start within one minute.

Okay. Let's start the last session of today. The first presentation will be around the WHOIS/GDPR survey that CENTR has been carrying out and Peter is going to show us the conclusions and the results of that survey. Over to you, Peter.

PETER VAN ROSTE: Thank you. Good afternoon, everyone. My name is Peter Van Roste from CENTR. I presented 80% of the slide deck about two hours ago in the GAC meeting. I assume that quite a large number of you were present there. I'll go through it, but I'll go fast and then we can take questions at the end. For those who had already seen it, there's a few extra details that I'm going to share during this presentation.

So, as most of you know, CENTR is an organization for and by European ccTLDs. What we do is we provide, amongst other things, but we provide our members with a platform in which they can exchange data information. Part of the exercise is we run regular surveys, about 15 per year, and this one was on the impacts of the GDPR, on WHOIS.

It was more to get a snapshot of what happened in June, of what the situation was in June, rather than see a historical evolution. That said, and very importantly, for most ccTLDs, no dramatic changes took place on May 25th. It was fine-tuning of their policies. It was making sure that their backend processes were compliant with GDPR. And for quite a few, it also meant having a good discussion with their registrars on how the data exchange is taking place.

So, a good response rate to our surveys. Typically, it's between 20 and 25. This one matches that. As you'll see, there's a few CCs that are not European but that still responded to it and that gave us some insight on how European regulation had affected them.

A couple of things we're going to cover, what data is published, what mechanisms are available for those who want to have access, how is accuracy verified. What is that problem with registrars refusing to transfer personal data? How [inaudible] data subjects safeguarded, average response time, and differentiation between individuals and companies.

Don't worry about not being able to read some of the details of the slide deck. All the information is available on our site, on Twitter. CENTR News just shared the links to both the report and a publicly available

dashboard and you can find it there. If you have problems finding it, just ask me afterwards.

Importantly, in that survey, we made the distinction between individuals and legal entities. As those of you who are familiar with the GDPR would know, this is about personal, identifiable information, so we need to make that distinction.

When we look at – and this is the highest-level overview of the information. But when we look at these different columns, what do they tell us?

Well, first of all, there is quite a difference between the information that is collected and here is the registrant contact information that is highlighted there, and the information that is published. So, from 74% of information collected, 74% means 74% of ccTLDs on average collect data in that category. I'll explain a bit more in detail in the next slide.

So, there is a big difference there and that's important because in many of these discussions that I'm following in ICANN, some make it sound like that information is disappeared or gone. It is not. Registries do collect it and they have plenty of contractual reasons to keep on doing that.

Another important thing to notice on this highest level is that if you look at this particular column, 10% of registries publish some sort of registrant contact information. Compare that with the information published from legal entities, there is quite a big difference, from [10-50%].

This gives you a bit more detail. Again, the full dashboard is available on our site and there you see what we mean with these averages. Obviously, the registrant name of individuals, for instance, it's 100% of the registries that collect [that]. But, if you look at the registrant [facts extension], that's only 26%. If you add up all these numbers, that's how we got to the 74% on the previous slide. It gives more an indication than exact reference.

Then, information is available on stats.centr.org and there you will find a drop-down list, the WHOIS dashboard.

Not [discussed at the] GAC, but if we look at verification, how many registries verify the information that they get? 52% verify after registration, 32% do not verify at all, and 16% during the registration process. Typically … Well, a good example I think is some of the registries that use EIDs to verify that.

The level of verification, as you see in the last bullet point, partial verification of the accuracy is automated for 40% of the registries. I want to make sure that the expectations there are set right. That can just be as simple as does this postal … Does the post code for a particular region exist? So, it's checked with databases that are publicly available. It does not necessarily mean that the accuracy of the identity is verified. That's an important distinction.

Sources for that verification are business registers, supporting documents, still scanned PDFs, e-mailed in some cases, even faxed information.

In the CENTR community, there has been quite a lot of discussion on registries that receive partially obfuscated data from registrars.

What does that mean? That rather than transferring the e-mail address of the registrar, because that' typically, in 50% of the cases, the problem. Rather than transferring the e-mail address of the registrant, what the registry gets is a hashed address that will still lead to that registrant but is unrecognizable for the registry. It is still in a means to reach the registrant but it doesn't share any information about the identity.

In other cases, it's a general address and that's even worse because then it's not identifiable. It's not a specific name. It is an info@registrar.whatever.

25%, so a quarter of the registries are facing that problem. That seems high. When you dive into the details of that, it typically is about the same registrars. Some registries have been able to fix that problem at the registrars by assuring that the information that they receive is not published any longer, and then registrars felt comfortable again transferring it. It solved most of the issues, but not all of them.

So, we also investigated into what are the legal grounds for both collecting and publishing data in the WHOIS. This is the publishing part. Legitimate interest, contractual terms, consent. A couple of things that were mentioned by registries.

What I personally think is a quite interesting one is those registries that do not want to publish personal identifiable information through the

WHOIS protocol, some of them – [eleven] – offer opt-in services. So, if as a private individual, you still want your data to be available in the WHOIS, or truly WHOIS protocol, then you can tick a box. And that is a very popular box to tick. Those that offer that service signal that lots of registrants actually do prefer to have their data published. Quite a few more are planning to offer that service as well.

Data retention requests. Majority of registries keep data for more than five years and in about 32% it is kept forever. From a legal perspective, that's an interesting observation because, in Europe, European registries will soon – say, end of next year – will soon have to deal with the [e-evidence- directive, which will allow law enforcement agencies to send preservation orders to, amongst others, registries and registrars are specifically mentioned in that regulatory instrument.

That basically means that the anonymization that most ccTLDs have been planning for following the GDPR will need to include some exception rules in case you want to keep specific information. So, it's conflicting rules that will give I think our technical departments quite a headache.

Most registries do not implement the right to be forgotten for registration data.

I think the registries in this room probably have had the discussion internally. There is not one single department within a registry that typically deals with these requests. It's customer service, legal department, and/or the data protection officer if they have one.

And here we're back to the presentation I gave at the GAC. If you do not publish information to a public WHOIS protocol, how do you allow access – do you allow access? 85% said yes. How do you provide the access? 75% of those do that via e-mail and individual requests.

SIDN mentions in the GAC session that they have an access protocol where law enforcement agencies can have access to the database directly and that is covered by an agreement that they have with the law enforcement agency and law enforcement agency takes full responsibility for how they deal with that data.

So, those that to provide access [inaudible] 75%. Partially it's … Well, 90% [inaudible] identified in court orders. Law enforcement, 100%. IP rights holder and other stakeholders, 40%. Then, a quite significant category, anyone with legitimate interest at 60%.

So, how do we define what legitimate interest is? Typically, it's just by the legal department. That's the majority of those responding. A few [judged] by the customer service or by third party which turns out to be external legal counsel.

At the moment, there is no accreditation service that is used by any of the European ccTLDs. There's quite a few in the making that I'm aware of. But obviously these typically focus on the G world and not on the CC world.

Timeline for responding to those requests. The important one is about 65% is responding within three working days. 33% does within one day.

How do we make a distinction between individuals and organizations? 10% doesn't. Those that do are spread between self-select and other. The other category, if we dive into the details, it is kind of self-select, too, by asking the registrant in the registration process to add a VAT number, a company registry number, anything that identifies them as being a legal entity rather than an individual. And that's it. Thank you.

PETER VERGOTE: Okay. Thank you very much, Peter. Questions for Peter?

ROELOF MEIJER: Thanks, Peter. That was an excellent overview. Very useful. Just a comment. You mentioned the verb identifier or the word identification a few times. I think very few registries actually wish to identify the domain name holder. We want to be able to contact the domain name holder. There's a difference.

So, the WHOIS data can be completely correct, but it will not identify the domain name holder. It will just be data which we can use to contact him or her. I think we should make the distinction because identifying, you can only do that with an identifying document, either electronic ID or a paper one like a passport. But there's no other way to do that beyond any doubt. In that context, I think using EIDs to buy a domain name which normally costs something like, on average something between 5 and 10 euros a year. Sounds a bit heavy for such a thing, unless it is what you would call an attribute-based electronic ID that only gives certain of your data to the registry when you want to buy

a domain name but I don't think they exist in many countries yet. So, a complete identification is a bit strong, I think, to get a domain name.

PETER VAN ROSTE: That's a fair point, Roelof. I'm not sure. I don't think we are prepared for that, but I know that DK is verifying the identity through an EID system. I don't know if, Ali, if you want to share a few words on that. But indeed it is still quite a [inaudible].

UNIDENTIFIED MALE: I think paper, mail, letter to the address that the registrant gave and then ask for a reply. You're referring to [inaudible] something like that, I think.

UNIDENTIFIED FEMALE: Firstly, I think it's a good thing to do, to make it a difference between the two, because it is, as Roelof said, it's not the same, but once that's set, we do go for the identity check of the registrant by electronic ID, if possible, and if not, by other means. And it is heavy, but that's the way of the world as far as we are obliged to do [inaudible].

UNIDENTIFIED MALE: Okay, thank you. I have a question for you, Peter, if I may. It might be a difficult question. You might not have an answer. I was quite struck by the number of registrars that is obfuscating data. Although it might be primarily a problem or an issue for European ccTLDs, I think there could easily be a spillover effect to other TLDs as well because if I am a

registrar, I want to keep my processes aligned and as simple as possible, so why would I then differentiate between, I don't know, a registry in New Zealand and a registry in Belgium, for instance.

But, I think for us registry operators, it's really key that we have the data in our database. It doesn't necessarily have to be in the WHOIS, but I can see an important for us having it in the database.

Is there a way that we, as a community, could actually try to bring out a message that it is not necessarily from a GDPR point of view that they obfuscate, for instance, the e-mail address?

PETER VAN ROSTE: To put that 25% in perspective, as I mentioned during the presentation, it's 25% of registries that are affected by it, but this can be by a handful of registrars. We don't have the data on that, but from hearsay, it is restricted to I would say three or four large European registrars that have that practice.

In terms of as a community providing an answer to those registrars that have probably genuine concerns that we can mitigate and respond to from a legal perspective, I'm not sure if he was in the room but Jorg succeeded to convince the registrars – or at least a few of them – that [inaudible] obfuscated data, that this data will not be published. It will be protected under all safeguards provided by the GDPR and that seemed to have calmed down that discussion. So, probably Jorg could share some of that logic and that might be helpful for those other registries that are facing the same problem.

PETER VERGOTE: We're on the same track. We have been discussing this with registrars. We agreed to it and if we remove e-mail from the WHOIS, they will start sending, again, the real data and obfuscate the data, so we might do an effort in that perspective as well to share our experience. Hilde, could you just hang on for a second? Because I think we have a question from remote participation.

UNIDENTIFIED FEMALE: Indeed. Thank you, Peter. So, Ryan from SGNIC is asking, "How is the right to receive personal data in a structured, commonly used and machine-readable format being implemented in European ccTLDs?"

PETER VAN ROSTE: Could you read it again? I didn't get everything.

UNIDENTIFIED FEMALE: Certainly. How is the right to receive personal data in a structured, commonly used and machine-readable format being implemented in European ccTLDs?"

PETER VAN ROSTE: I think this situation will defer from ccTLD to ccTLD. I'm not sure whether every registry already has an operational way to deal with this. So, I think we better take that question offline and think about it before providing a more detailed answer.

UNIDENTIFIED MALE: It was for sure another question in the survey that I'm presenting, so from that survey, there is no data to respond to that question, but as Peter mentions, I'm happy to look at it offline?

PETER VERGOTE: Okay. Hilde, over to you.

HILDE THUNEM: Yes. I don't have a question, but just a comment that will unfortunately complicate the picture of obfuscation of e-mail addresses a little bit more, because what you're talking about is that it is a bad thing if somebody puts in an e-mail address seeing info@mydomain-dot-something. That's an obfuscation or a hashtag type of thing.

At NORID, we do not consider that a bad thing. What we require is that the e-mail will reach the registrant, but we have taken the [inaudible] point of view that the e-mail address should be available to the public to be able to contact the registrant, and thus any means that the registrant then wants to take to anonymize it so that they are not identified as a person through the e-mail address is perfectly okay with us. We know that other registries are in the other area, but when you do follow up on that and if you want to do more of a survey on that, you might want to provide the option of people saying, "Yeah. We get obfuscated data in this specific regard and we don't consider it a problem." Bogus data, people giving us a postal address that is non-existent, etc. is a quite different thing and that's where we tell the

registrars that if you do that, we will not have [inaudible] registrar. But anonymizing the e-mail address is, for us, a quite okay thing.

PETER VAN ROSTE: Thank you, Hilde. The problem here is that it's a bit of a mixed bag. Indeed, as you mentioned, in some cases, the e-mail does get through. In other cases, it ends up with the customer service department of a registrar.

PETER VERGOTE: Okay. thank you, peter. Moving up to our next speaker, we wanted to share with the membership the practical experience from an actual ccTLD in how GDPR affected their processes, their procedure. So, I'm very happy that Jorg volunteered to give us the practical experience that dot-DA encountered while implementing GDPR. So, over to you, Jorg.

JORG SCHWEIGER: Thanks very much, and hello, everyone. Thanks for the opportunity to present what we've been doing with respect to GDPR. So, to say from the hot land of data protection, at least we are within the European Union.

Basically, it already has been said, but I want to state it again. GDPR does not start with WHOIS. GDPR starts with data collection and that is the first thing we need to take a closer look at.

What we do is we collect full registrant data sets. So, name, address, you name it. But, the only reason we do do that is because we do have a contract with the end user. As to this, we are entitled to collect those data. If you wouldn't have a contract, we might have a hard to time to even collect such data.

Come into Admin-C data. As you see, this is crossed on the slides. We are not collecting Admin-C data anymore. We wish we could because it makes life within our registries so much easier. But, it is not. It is not needed for our core business of registration and of making names available. So, if we don't need it, we just simply can't collect it, full stop.

So, we even changed our policy and I think this is one thing that is really remarkable. Due to GDPR, we changed our registry policy. Prior to GDPR, we had the requirement that domain name holders not residing in Germany had to provide an Admin-C contact. Nowadays, we don't even collect it.

Tech-C, once again, very interesting and very useful concept. It does make sense that one could very easily contact a person that is running a name server or that is, in a certain way, technical responsible for a domain. Yet, would I need it for the registration business, for the registry? The answer, once again, is no. I do not need it. And as I do not need it, I just can't simply collect it. So, we don't do it anymore. And exactly the same thing applies for zone data contacts. We do not collect them anymore.

So, everything we do is driven by data minimization and the reason why we are doing it is because we feel that GDPR is going to be interpreted.

It's like labor law. You got all the letters, all the language, that is written down, but it is going to be interpreted by courts. Or, in this case, it may be interpreted by the European Data Protection Board.

So, I think that we will see different kinds of interpretations on how we and everyone that is affected by GDPR has to implement it. And we just wanted to make sure that we do not have to change things overly and overly again. So, do it once and do it right. Even do it in a more rigorous way than is probably necessary in the first place.

That said, pretty easy. What you do not collect, you can't publish. So, our WHOIS looks quite narrow. Narrow means we only do publish whether or not a domain name has been registered, and if it's registered, we provide all the technical data like name server, name servers, DNS keys if applicable, but that's it.

That leads us to a situation where we leave a couple of parties behind who certainly still do want this kind of information. For example, we have public authorities, we have names and trademark owners and all that. So, what are we going to do with them? Because as I said, they only get the information a domain name [inaudible].

So, what we had to do is we had to provide access for those parties who can prove that they do have a legitimate interest. We tried to do that twofold. One, for sure we wanted to do it in a way that is as much and as mostly automated as possible.

So, for domain owners, we decided that they just have to give the e-mail address that has been used at the point of registration or they could

provide the postal code and they will get sent their domain information to their e-mail address and that is the e-mail address that had been given at the point of time of registration.

All other interested parties, they have to prove legitimate interest. What we do is we vet those inquiries with our staff, so we really look into each and every request coming from, say, trademark owners. And just to give you a couple of numbers because I think that might be interesting, as you may know, we currently have 16.2 million domain names under management, and for those, we got prior to GDPR, roughly 10,000 WHOIS queries a day.

After GDPR, we get 1,000 queries a day, but very interestingly so, out of those 1,000, only 35 have to be vetted for legitimate interest. So, the number was way less than we feared that we would encounter.

So, that more or less is the current state and it leaves us, or still leaves us, I think, with a couple of challenges because, for example, [inaudible] lists do not understand why they do not get the data just because they want it.

We have consumer protection organization who really do want the data straightaway without providing any legitimate interest. We have to tell them, no, it's your consumer protection [inaudible], you do not get your data.

It is getting a bit worse because those consumer protection organizations refer their consumers to our WHOIS telling them, "If you want to verify whether or not a certain website is not malicious, well

then, go to WHOIS of DENIC and take a look at the WHOIS data." Now they can't do that anymore because we are not publishing any data.

So, there's some friction in what consumer protection organizations do and what we are doing post-GDPR implementation. And while for sure legal authorities or law enforcement agencies want access, they do not want to prove that they have a legitimate interest, but they feel that they have a right, per se, which we neglect and we vet all their inquiries as we do with any other person. And that's basically it. Questions?

PETER VERGOTE: Okay. Thank you very much, Jorg. Questions for Jorg? I have one. I needed one point for clarification. Suppose that I'm a company like ABC GMBH and I have abc.de, so also my company name doesn't appear in the WHOIS anymore.

JORG SCHWEIGER: Yes, that's correct. It's correct because, within our database, we just simply could not distinguish between a company or a legal entity and a domain name holder. We could in, let's say, 60% of all cases, but we just simply can't be sure about the rest of the 40%. And as we can't be sure, we choose not to do it.

PETER VERGOTE: Okay, got that. Can I opt in?

JORG SCHWEIGER: Yeah.

PETER VERGOTE: So, I can-

JORG SCHWEIGER: Okay. Now I understand. I thought you want opt in with another question. No, you can't opinion. The reason for that is we do not want to handle a lot of requests and changes back and forth. It would be very serious and very problematic to handle opt-ins and retractions of those which is a lot harder across, say, reseller chains. So, you can probably do that quite easily with respect to our members. So, the registrars that is more or less in the first place of that chain. But, it's that registrar working together with resellers and they were working together with resellers as well, so you never get traction on any retraction of an opt-in, so this is why we choose not to provide opt-in.

PETER VERGOTE: Roelof?

ROELOFF MEIJER: It's just we're sitting here, might as well do something. How did you say? You said we want to do it once, we want to do it good, even if that means that we may be going a bit too far for the present situation. What is your main drive to use that approach?

JORG SCHWEIGER: Well, exactly as I stated. To be compliant. To be compliant with—

ROELOF MEIJER: As you suggested yourself, you're being over – I don't know if the word excess. But you suggested yourself that you're probably being over-compliant.

JORG SCHWEIGER: No. We have been confronted with a lot of different opinions that we are too restrictive.

UNIDENTIFIED MALE: It's always an opinion. Even if you're in court, it's still the opinion of the judge. Do you think that you are doing more than what would probably be necessary or not?

JORG SCHWEIGER: For sure, what we did, we did consult with our membership before we implemented and we had a couple of members, for example, saying they don't feel that we have to change anything. And in a very first place, actually, we thought so ourselves because going very much into detail, the [inaudible] – that is the German law that was in place before GDPR – is almost as strict as GDPR.

ROELOF MEIJER: Yes, the same [inaudible].

JORG SCHWEIGER: What is. And under the [inaudible], we did publish and we did collect all the data, everything. So, there happened to be this situation where we made a complete change due to GDPR, even though we feel GDPR and [inaudible], they are quite similar.

ROELOF MEIJER: You're kind of making my point for me. Because were you compliant in the previous situation?

JORG SCHWEIGER: You actually really can't—

UNIDENTIFIED MALE: This is a hang yourself question, I think.

JORG SCHWEIGER: No, not at all. We couldn't simply say because we never ever got a statement from our data protection authority that we are or that we are not compliant. But, if there had been complaints, official complaints, to the data protection authority, [responsible] for us, we never get fined or we've never gotten a complaint. So, obviously, we are but we never get something like a certification for that or something that is signed saying, "You are compliant." So, we simply just didn't know.

And to make it even more complicated – and that is one of the driving forces as well because we opted to minimize as much as we can, for

DENIC, a federal data protection authority is responsible and that is the one in the federal state of Hesse. The situation could be completely different, for example, if we take a look at our colleagues in Hamburg or in Bavaria.

So, what we expected is that even though we may be compliant with collecting everything and publishing everything, that will change. So, our data protection authority, over time, would change their opinion. And as we never had a written saying, "You are compliant," we felt we had to do something about it.

ROELOF MEIJER: Something, I think that's clear. But, what is puzzling me – and it's an honest question, so there's nothing behind me. And maybe it's a cultural thing. It's also possible. But, you went from a situation in which we, as a registry, looking at your WHOIS, thought, "They can't be complaint," to a situation where now where we feel we are. We think, "Whoa! They really go very far. They give themselves a hard time." And a lot of other people, they're giving a lot of other people also a hard time. For instance, if you want to opinion, it's not possible.

I'm just wondering why you went from a zero to a one. Maybe that's the explanation. Because you could have followed – and I know you guys thought this through, so there must be a reason, but you could have followed a more agile approach. So, you do something where you think, "Okay. This is an improvement and we're looking at our peers in the rest of Europe. This is about fair." Because that's a very defendable position at the moment. You won't get fined immediately because you came

from a situation where you yourself already said there's very little difference with the GDPR. Nobody ever told you to do something else. You've kind of voluntarily improved matters. If now somebody feels that you're not compliant, I think they will first tell you and ask you to change something, but you went the whole way. And that kind of puzzles me because it must give you difficulties with all kinds of [parties].

PETER VERGOTE: I have to cut it short here in order to allow Brent, but I think you touched upon a point, Roelof. I'm also convinced that it's probably more related with cultural and philosophical approach. You can either say, "I'm not going to take the risk that I encountered negative case law in the future, so I'm going to do it very strict to prevent, that I get a negative legal precedent." Or, you could take another approach and say, "I'm going to do it as I see fit to stay within the boundaries of GDPR compliance, and in the worst case, if I would get a negative precedent, I will then adapt my procedures and my systems to it." I think that's the difference between the two approaches.

UNIDENTIFIED MALE: And [off mic] try and balance the interest of the different segments.

PETER VERGOTE: Anyhow, Brent, sorry to keep you waiting. Here is the clicker. I'm going to briefly introduce, because in New Zealand, we have a very interesting privacy related court case that was brought up and it has to do with a

company that actually tried to gain unauthorized access to the dot-NZ domain space, but [inaudible] more details, Brent.

BRENT CAREY: Okay. Thanks, Peter. And I know I'm standing between drinks and we have a very tight schedule to get to the bus, so I'll try and talk very quickly because of course I have my PowerPoint here. As Peter said, this is quite a novel case, because it centers on unauthorized access to the dot-NZ domain name space by a US-based company.

So, I'd quickly like to just touch on who we are, talk a little bit about what the action is and why we took it in the United States, which is a lot of flying time between New Zealand and the US. Also, I'd like to talk about where we're at and a little bit of things for you to consider as ccTLDs.

So, just quickly, who we are. The Internet New Zealand Group comprises of two entities. We have Internet New Zealand a charitable organization which effectively runs the dot-NZ registry. It's also the steward of dot-NZ policy. It provides technical research and also grants. Domain name commission limited is also a charitable organization and remains a separate independent subsidiary that authorizes sellers to sell dot-NZ domain names, monitors the dot-NZ market, and enforced dot-NZ policy and contractual compliance.

We also have a Memorandum of Understanding with the New Zealand government which allows us to be the steward of the dot-NZ domain name space.

The commission also has an operating agreement with Internet New Zealand which allows the commission to bring legal proceedings and that's why we've taken this case.

So, what is this decision about? Domain Tools is a digital intelligence-gathering company from the United States. It is a Delaware-based company. But it is also a subsidiary of a registered company based in Luxembourg of which Domain Tool is the sole member.

Domain Tools has been scraping registration data from New Zealand's Domain Name Commission for many years. We felt that the mass collection of data breaches our terms of use and exposes details of domain name holders who choose to have their details kept private. This is because Domain Tools makes available historical records which now can be withheld. With effort, found it important that we be able to enforce our terms of use and also our new individual registrant privacy option.

We took action claiming that Domain Tools had breached contract terms and also violated Washington consumer protection laws. And that is the material facts of the case which we pleaded were, one, Domain Tools submitted high-volume queries to the dot-NZ register. This was despite us having technical controls to try and rate limit this from happening. Two, they created and built a secondary database, containing the details of all dot-NZ domain name holders and have stored that offshore and out of the control of dot-NZ domain name regulator. This database did not just contain current records, but also contained a number of historical records.

Three, that this database, that Domain Tools was profiting from this database and selling this to third parties.

These actions were happening against a backdrop of us bringing in a privacy option for people from the 28th of March this year.

So, what happened on the 12th of September? We're very pleased to report that Judge [Laznik] found in favor of the Domain Name Commission and on the merits of our breach of contract claim alone have said that the Commission is likely to be able to show that Domain Tools has violated our terms of use when it downloaded our data to create a private version of the dot-NZ register. The judge did not go on to determine our claims under the computer fraud and abuse set. That no doubt will come when we have our full trial.

What this means is Domain Tools is no longer able to access the register and all licenses have been revoked and they're no longer able to publish any of the New Zealand register data.

Where we are now. Our full trial is not scheduled until September next year. We're also taking steps to ensure that Domain Tools complies with the preliminary injunction. We're also having to defend the preliminary injunction because Domain Tools has filed an appeal in a high court. And we won't know the outcome of that appeal until the middle of next year.

So, what might this mean for other ccTLDs? One of the most notable comments in the preliminary injunction was that the lawsuit may cause an avalanche of litigation as other registries attempt to protect the

privacy of their registrants to which Judge [Laznik] said this may well be very correct.

Therefore, in closing, what our case could highlight is: is Domain Tools collecting, using, or storing your current or historical WHOIS registration records? If so, is this permissible under your own terms of use or do you have similar terms of service provisions to dot-NZ that restrict or prohibit multiple or high-volume queries to download all or part of the register?

And more importantly, has GDPR or local privacy law changes meant that there's a different expectation on ccTLDs in relation to enforcement action to protect registrant's personal information? And perhaps you have your own basis to look at whether or not third parties should cease and desist from mining your own databases.

So, thank you for your attention today.

PETER VERGOTE: Thank you very much, Brent. Questions for Brent? Seeing none, then I think we can bring this session to an end. I'd really like to thank our presenters. Sorry. That was already at a [inaudible]. Thanks very much for my presenters. Give them a round of applause, please.

So, that nearly brings us to the end of day one of ccNSO. And out go the lights. But, before adjourning the meeting, I would like to turn the mic to Alejandra to brief us shortly on the practical details for the [EurID] event for tonight. Alejandra, over to you.

ALEJANDRA REYNOSO: Thank you, Peter. So, please, everyone, leave everything you don't need to bring to the dinner quickly and gather in front of the venue at the doors, the rotating doors. There will be staff of [EurID] checking your confirmation and they will lead you to the bus to take you to the [inaudible] for the new event.

PETER VERGOTE: If you're seen checking your confirmation, there is no written thingy that we got. Everybody confirmed electronically.

ALEJANDRA REYNOSO: No, there's no physical thing they will have there. As far as I know, their iPads and they will check that.

PETER VERGOTE: Okay. We don't need vouchers or things like that.

ALEJANDRA REYNOSO: Not as far as I know.

PETER VERGOTE: Okay, good.

ALEJANDRA REYNOSO: 6:15 departs the first bus, so as early as possible.

PETER VERGOTE: Okay. Well, thank you very much. Meeting adjourned and see you tomorrow at 9:00. Thanks. Good evening.

[END OF TRANSCRIPTION]