PANAMA – Tech Day (3 of 3)
Monday, June 25, 2018 – 17:00 to 18:30 EST
ICANN62 | Panama City, Panama

UNKNOWN SPEAKER: Can we please all settle down and sit down. Can we... Garth... is Garth Miller here? I don't see him. We'll expect him any time now. Where are the panelists? [inaudible], who else was going to be on the panel? Somehow Garth Miller got lost, but we saw him so he will come any time now. What we're doing now is going to be a little round table about the GDPR. As we have said before, this is nothing to be worried about, we're not going o do the politics here, but some registries, if not all, are affected in one way or other and we for example, in [inaudible] we had to make some changes. We loaded a newer version of the [inaudible] tools, which allows us to filter out on the WHOIS display, according to residents of the registered address. We have a different, fairly unique model, in that we have got [inaudible] and foreign clients which have a different pricing, so [inaudible] clients, companies in particular, have to be listed according to [inaudible] law and any correspondents, so that's not a problem. European's we filter out and we only see the only problem that we re having would be [inaudible] who are also Europeans. We have decided that if that were to happen, we'd tell them that they can either be [inaudible] or European's, if they want to be

European's they have to pay the European price, which is a little bit steeper than the [inaudible] price, and they will probably figure this out for themselves, what they want to be this year. Otherwise, we notice when we read the [inaudible] court case, that we have never, over the last 20 years, once looked for the billing for the technical contact address. So, for us, we are going to stop collecting this information, we are most certainly no longer going to display it. The problem is now, how do the technical contacts and the billing [inaudible] at the moment displayed on the WHOIS, and we are not going to do this any longer. OK. We don't need this information, who needs it? We don't. In order to contact the customer or the registrant, you can use the admin contact. The problem is how do we communicate this to the registrars that it doesn't break their systems? At the moment, one option is probably to just let them load the data and we throw it away, or and then eventually start accepting empty data, because we don't want any registrar who uses EPP to having to change their systems too much unless it's in a way that everybody does at a same time, in the same way. So, without further ado, we collected a nice [inaudible] Garth Miller as I said is still wandering around here somewhere, he will come just now. He is in charge of the [inaudible] project. We have Christian [inaudible] from [inaudible], from the dot NL. We have got Alvin [inaudible] from dot DK, so we have got two full European members sitting there. Then Jacques [inaudible] from

dot CA, and Nick [inaudible] who is from Nominet, which means he is a little bit between with the Brexit looming, and then we have got [inaudible] from CZ, which they're all inside the EU and affected. I've asked Diego Espinosa, who many of you know to moderate the topic as from now.

DIEGO ESPINOSA: Well, good afternoon. [inaudible] said, we want to talk about maybe the technical issues, or technical implications of the GPRD and thinking about the information management, why we do capture that information and if we need it or not don't need it? How can we deal within our systems or the ccTLD systems, facing these new revelations from? I will let each of the speakers talk about their own opinion or position about these topics, we have plenty of time, we can talk freely. Let's start with Christian.

CHRISTIAN: OK, thank you Diego. So, the... we... I'm responsible from [inaudible] which is the research team of SIN and we in 2014, we developed a system called [inaudible] which is basically a system that collects the DNS traffic on our name servers and puts it in a large [inaudible] cluster for easy analysis so to speak. One of the things that we ran into initially in the first few months that we were working on the system is that, with the IP addresses, we considered them, in some cases, and they're now

in all cases, personally identifiable information. So, we... this is not really... this is actually a pre GDPR era, but we knew that the GDPR was coming, so we developed what we call a privacy framework, and it basically consists of two major components, so one is privacy board, which is a group of people within our organization that evaluates privacy policies. Policies are basically easy to fill out documents for application developers that, if they are using data from the Entrada system, so the DNS traffic, then they need to briefly describe what they want to use it for, how they're going to retain the data, and that sort of thing. Then the privacy board evaluates those policies and says, OK, you can do this, or you can not do this. This is something that we implemented back in 2014, 2015, so we've been doing this for quite some time now. But, recently with the introduction of the GDPR, the privacy board has also expanded their, basically their role, and it's now basically covering all the privacy related aspects within the company and what we think is unique is that we do have a data protection officer, which is, let's say mandatory by the GDPR regulations, but she operates in a team of three, so the privacy board has the data protection officer in there, the technical expert, who is actually somebody from my team, and somebody who is really experienced in processes and knows about customer interaction and that sort of thing, and who is also on the management team. So, we basically in our... in our... privacy board we combine three different perspectives

on the same problem, if you will. Like I said, this is something that we now have operational for... we had it operational for a couple of years already, so for us, this was business as usual and that part of the organization wasn't really affected by the GDPR, because we already saw it coming and we were basically prepared.

UNKNOWN SPEAKER: Yes OK. Christian, do you need to make some changes in your system to finish implementing GPRD, now it's alive?

CHRISTIAN: No, we developed the privacy framework and everything else around it with a GDPR in mind, because we knew it was coming.

UNKNOWN SPEAKER: Next one please.

UNKNOWN SPEAKER: I think I like best what you said, it's business as usual for several aspects. For us, it's the same thing. We work under the Danish Domain Act, which means that, I talk about before, about the real name and address. It also has a requirement for us to publish the name, address, and phone number of the registrants publicly, unless there's other regulation forbidding us from

doing so, which in practice means that for a Danish registrant, he can go to his local city and get his name and address protection, which [inaudible] something. So, that means our WHOIS is going to stay open, the GDPR requires you to have a legitimate reason for processing the data. A requirement in the Danish law, of course, is a legitimate reason for processing the data, so that it's not incompatible with each other, and we just keep doing so. We did have a close look at what information we do publish in our WHOIS service, and we are going to take some of that information out. So the name, address, and phone number of the registrant is a requirements, we are not required to publish the user ID, which is also the login name into our self service portals, so we're not going to publish that anymore. For the admin and technical contact, well billing contact was never published anyway and the other ones, there are different meaning in a Danish system, but the equivalent used to be published, we got to remove those. We've still got to collect them, because we do them in our own system, but not publish them and we'll make a form available, a web form available to contact those people through us, but we don't make their details public anymore. I'm just going to say to Christian, we don't have a DPL, it's not a requirement, we decided that we do not... there's specific reasons when you need a DPL, and when you don't need a DPL, and our current understanding of our interpretation of the regulation is that we do not need a DPL.

UNKNOWN SPEAKER: Thinking about the root cause of these GDPR, all information you request or require or have in your systems is needed to work, needed for something?

UNKNOWN SPEAKER: Yes.

UNKNOWN SPEAKER: OK.

UNKNOWN SPEAKER: Just because we have a model where the registrant and his proxy, which kind of like the admin contact, can do systems directly with us through the self service channels, so we of course need to know who they are and they have to have a log in, so we need to process their data in our systems.

UNKNOWN SPEAKER: [inaudible].

JACQUES: I am Jacques [inaudible] with dot CA, from Canada, so we're kind of an ocean away from Europe. But, so in terms of privacy policy, Canada since 2010 we had the registrant privacy policy,

so individual registrant persons we would hide the information from WHOIS, so not make it available anyways, since 2010, and only business enterprise registration, we make the full information available anyway. So, from that point of view we didn't have to change anything or address anything for GDPR from a WHOIS point of view. Internally, being in Canada, the privacy commissioner established that IP addresses are PII for a long time, so we've been operating at that mode for... since a couple of years so it didn't change a lot of internal process on how we handle data, so from a Canadian point of view, not much that we had to do to support GDPR.

UNKNOWN SPEAKER: Yes. Not thinking only about the WHOIS, as you suppose in the web, but thinking about the [inaudible] the data you capture in your system and keep it, since the GDPR have that scope, even if you... when you capture the data, you are really are in cost to the personal data of the customers personal information. Then it is within the... what is within the... GDPR, [inaudible] are you capturing that additional data that could be inside the GDPR in some way?

UNKNOWN SPEAKER: For the private individual we are collecting the technical admin contact information and we are storing that, we;re just not

making it available in a ways. But we need it to do our own business, we are a registry.

UNKNOWN SPEAKER: Another question, maybe for all of you. Another thing they mentioned in GDPR is, the possibility of the user to request to remove all the information... all the personal information there. I don't know if you already have your systems on that, but let's keep going with the other presentations and let's talk about this later.

NICK: Thank you, hi, it's Nick [inaudible]. I am from Nominet UK. So yeah, the UK is, as we all know, is in the process of leaving the European Union but one of the things which is going to stay the same is that the, obviously GDPR has now been implemented, and the UK government was very early on in saying that we would stick with the European Data Protection Regulations for the foreseeable future. So we had, obviously to implement it. I should explain that I am and have been for about 7 or 8 years, Nominet data protection officer, and I had taken the view that Nominet had always operated quite conservatively in terms of legal compliance, is the first thing, and as a registry that tended to be our guiding philosophy. Secondly, I took the view that actually GDPR was a new set of laws, but a lot of the principles

was exactly the same as previously, my explanation for this is a bit like, you have speed limits on the roads, and the speed limits are not changing, but all of a sudden there is a lot more traffic enforcement cameras to catch you and the penalties for breaking the speed limits are much more serious. So, this makes it a more corporate strategic issue, but with regards to our WHOIS policy, I felt... this was about two years ago, that we were in a very good place because, firstly, we didn't publish any telephone numbers of email addresses for any registrants. Secondly, that the... if you said that you were a private individual, and you were not using your domain name for business purposes, you were able to opt out of having your address displayed already, and it would just be the name of the registrant. Thirdly, this policy was developed by the UK community many years ago and it included representatives from our information commissioner office. So, I had thought that effectively there wouldn't be very much work to be done, and I think I have to come with a bit of humility to say that it actually created a lot more work than we thought. We were very mindful when we implemented WHOIS changes of the impact on our registrars, so we needed to have as minimal impact as possible, and we needed to obviously, make some system changes, we needed to communicate those system changes, we took a view... we had a sort of one month public consultation, we were a large registry, we have 12 million domain names, and there is an

optional field where you can say if you're an individual, or a company, or some other type, a charity, or foreign company. This is an optional field and when we looked at it in detail, the application of this field amongst all of our, we've got 3000 registrars, the application of this field was very inconsistent. Some of them didn't use it, some of them always said that it was a business registration, some of them always said it was a private registration, so you couldn't really rely on this, whether you were publishing personal data or non personal data. We ended up, almost taking quite a pro privacy approach, slightly to my surprise. So now, we do not publish the registrant name or address, unless they have specifically consented to opt in to this process. It is quite similar to the ICANN model. But, it was a sort of a simple process to communicate, it was consistent with all of our large registrars were also doing for their gTLD work. We are monitoring to see, really, whether that has been the right decision, but so far no real issues. We had existing data release processes, we haven't really seen any impact on the amount of queries we get as a result of the data no longer being published. In terms of the data we collect, the introduction of GDPR made me go through a bit more of an analysis as to why was it that we needed to collect the data fields that we collected and actually document some of the processes and justification for this. Fundamentally, it came down to there are some times that we we need to contact the registrant and that's because there's a

dispute resolution process, in terms of rights holders and abusive registrations. We also do suspend domain names for bad data quality, but also for criminal use, and in that case we send a notification direct to the registrant, and we cannot do that unless we have the registrants information, so we need to collect it. The third thing was important to us in terms of collection of registrant data, is that registrars do go out of business from time to time and in those sort of business failures, the registry is there to ensure continuity of service and to transfer the domain registration to a new registrar to have some sort of backup continuity. So, we did go through a lot of thinking and documenting of these sort of processes around our WHOIS, we had quite a big project going through lots of different parts of the company not just the technical parts, but also, for example the HR department, outsource payroll arrangements, all of which deal with quite a lot of personal data, in fact, you know, selfishly it's my personal data, my bank account information and I'm quite concerned to see that it's kept securely in accordance with GDPR.

I suppose the final thing which touches on the technical out departments, is that we recognize, we do a lot of data analysis and whilst most of the data is basically anonymized or very hard to de-anonymize, it is possible and in fact we know it's possible as that's what we tried to do to identify bad actors, and you can

identify specific individuals through data analysis. So, you had to take into account that some of our data analysis and IP aggregation work would be caught by GDPR, and that doesn't mean that you cannot do it, you just need to be careful about how you do it, and you need to think through why it is that you're doing it. If we're doing it to improve our systems technically, to reduce criminality and abuse, and that includes technical abuse such as malware and phishing mitigation threats, then I would be happy in the face of any complaints to argue with our information commissioners that those are legitimate purposes and entirely justifiable. But, part of the checks that we do, is we go through those processes, those under the GDPR there's a requirement to do sort of a data protection impact analysis, so that's where you look at a proposed new operation or a particularly complicated operation and you take a device from technical colleagues around, well are you keeping the data securely, are you using it in accordance with the principles to minimize the processing that you do beyond what is not reasonable for your business needs, and then to sort of document that so that if there is any problems, you can show diligence in having gone through some sort of processes to have a prudent and compliant approach to the way that you approach personal data. I think the final thing which is quite a big project, was that every single person in the company had to have a mandatory data protection training course, it's an

online course. Because it's an online course, we knew who had done the training and then who had passed the test and which departments were the slowest in doing the training and passing the test and that was not the legal department, although we were one of the last. It was the technical department in fact, so you know, ultimately everybody in the company has passed that and we've documented that everybody has had the training. Nobody is infallible, there is a lot of manual processes, it's possible that we will make mistakes, but the regulatory environment around GDPR, is not that you have perfection, is that you put in place the right controls and processes in terms of the culture of compliance, and that's what you can... or that's what I believe that we can now demonstrate if we needed to.

UNKNOWN SPEAKER: Very good. Andre.

ANDRE: OK, so GDPR for us, this was a quite a big deal. Not because of itself, but [inaudible] performs more functions in the country than just domain name registries. So, we started at the end of the last year, and we started with the analysis for whatever, databases, our personal data. We have... I saw 27,000 so we should be aware of it very well, but to be honest we [inaudible] risk assessment again with the special emphasis on personal

data because that was something we really didn't have in mind when we started, or certification, [inaudible] certificate our company, and we found several areas where the personal data are captured and processed. One of them is, of course, the DNS like it was mentioned by Christian and it's quite a complicated area because it's quite tough to understand whether the data can really identify some personal... because not every IP address can really lead to this close of personal data, of course. Also, we run national [inaudible] we do a lot of other functions where personal data are processed, maybe one more important than the DNS industry is the single sign on service for the internet services, so that was probably bigger than domain, but that's, I hope, I believe out of scope of this discussion. So, we started to kind of, we had identified a few areas that needs to be changed in our registry, we consulted this [inaudible] with our personal data authorities in Czech Republic. We don't have any specific implementation of GDPR, so we just had a previous data protection law and GDPR directly. In our registry, we have a policy that you can hide some parts of your data, that the registrant submitted it as, and there were one part that can be hidden which is the name of the registrant and also address, if the address is not verified. So, we believe we have a legitimate reason to display this information, if they are not verified because then we can use the control of external people who are accessing the data and many times people submitted this

information is not valid, can you check it, and then we usually start a process of validation of the data. In the previous version of the registry, if you register domain, you have a possibility to hide some of the information that you submitted, with the beginning of GDPR, when GDPR had become active we changed the defaults. So, when you registered contact that is necessary for registering a domain, all personal information are by default hidden, as I said except the home address of the registrant and the name of the registrant. Again, the address can be hidden just by the verification, and that means that we sent you a mail to that address and you verify some code that you received in that mail. One thing that complicates us, is the role of men, is that [inaudible] is not used in just the Czech Republic but in many other countries and most of them are outside of European Union, so we released a version of the [inaudible] registration system 2.37 which implements those changes but we plan to release, I think in a month, a new version which is 2.38 that will allow to disable all those changes that we implemented, it's for the registries, they are not part of European Union and they don't care of this legislation and I must say they are lucky. The last change we implemented in our registry is tied with the fact that if any company is collecting personal data, you can ask for them and also you should have some way how to transfer them to some other entity, so we created a webform that you ask for the personal data we collect for you and you get it in a machine

readable form so you can also transfer it to some other entity, I don't know what is this good for but it's a part of GDPR as well, so that's our implementation of GDPR.

UNKNOWN SPEAKER: Thank you Andre. [inaudible].

UNKNOWN SPEAKER: Yeah, I think not a lot to add here with our software which is like the [inaudible] software used by quite a few ccTLDs, I think almost 60 now. Each of them have their own policy they developed, so we had to come up with a variety of options for them, a lot of them didn't care. A lot of them were actually concerned. I think the challenge for small ccTLDs, is they don't have a lot of leverage over the registrar's, you know, if you're Nominet or [inaudible] you can sort of dictate the things to registrars, so our approach was really to really not change things on the data collection side, so that nothing broke from the registrar community and focus our energy on the public disclosure side, and basically that was fairly straightforward, we added a bunch of filters based on location of registrar and location of registrant and whether the organizational contact field existed, and on the web side we basically didn't leave it upto registrars to [inaudible] emails, we added a web form, a lot of the small registrars in the small countries don't have the

capacity to, you know, retool just for GDPR and [inaudible], so we sort of built that in. I think that was fairly straightforward, I think the only challenge were sort of looking at now is, you know, on the next stage with [inaudible] and we're just sort of monitoring what happens and what the best approach is there, so we did a [inaudible] version that allowed people that were concerned about it quick compliance, best efforts and monitoring what's going on elsewhere, and the one thing we're looking at now is really how long to retain data and that's a challenge for us, so we've put a lot of tools in there that allow registry to purge data if it's not used for X, Y, or Z time or if it's been... the domain has been deleted content. The challenge there is that it breaks the historical abstracts in the history, so if there is a dispute or something and you need to go back five or six years, or whatever the case may be. That's really where the... what we're sort of interested is, how to actually clean up artifacts in the database and comply with GDPR by not storing data that is no longer relevant, without actually breaking historical abstracts might be useful to mitigate abuse or look for disputes or complaints.

UNKNOWN SPEAKER: In that context, maybe at the prescription date is three years, so anything that we would look at purging anything over three years. We already delete names that are not in active use but are

not taken off the system as far as I understand it. My issue is basically, how to tell the registrars not to send us data that we don't need anymore. I think at the moment we're talking with [inaudible] about not displaying the technical contact anymore and the billing contact that's simple, but we need to basically start having a process where we can accept empty data, so that if a registrar stops sending us the data we accept empty submissions and when the registrar sends us the data, we just dump it. That's what I think we are going to do, because if you don't need the data, why keep it?

UNKNOWN SPEAKER: Yes. I want to talk to you about a little example I have about keeping information, and in this case we're talking about personal data but, for example, in credit card processing, when you capture credit card information you have two options. You can keep the information of the credit card and save it, and use it for another transaction, or you can use that information process the transaction and discard the data. What is the responsibility of the owner of the system, has when keeping that information with the credit card? Could be an issue if that information is hacked in some way, then in some point you can think about the personal information could have that value of the credit card information. It's not financial information, but in this kind of policies in GDPR, you can see how important is that

information for these communities. Then thinking about the information you are keeping, the personal information you are keeping from your customer or registrars, or... in some point you need to think about maybe, how to [inaudible] that information, or maybe is simple or cheaper just to discard information, or remove information you don't need because can carry a high financial consequence, you don't manage the information very well. I don't know if somebody want to add something to this.

UNKNOWN SPEAKER: I was going to say that one of things we have been doing in advance of GDPR, but GDPR made us do it more thoroughly, is to have a proper retention schedule for all the different classes of data. Not just personal data, but all the DNS records and there are some records in terms of financial information which you are required by law, for the tax authorities to keep for a minimum of 6 years, so obviously we keep it for 6 years, and we try to have a relatively simple alignment of most document retention around that, sort of 6, 7 year period. But, for example, for payment information we wouldn't keep that for the exact reasons you spoke about. There's regulations around this stuff, it's a real business risk to keep all of that information and you know, you should not be keeping data for longer than you can justify it for. So, some of the data, we keep for virtually very short periods of time, so I mean, for example, I the DNS sort of record, we do

keep all of our DNS name server records, we analyze them and until about 5 years ago, we had never deleted anything from the start of Nominet in 1996. When I joined the company in 2007, it didn't seem such a big problem, we hadn't got so much data and we hadn't kept it very long, but now, it's so much data, it's expensive to keep, it's a risk... we never look at it, so there's no justification to keep it. So, we started going through a process of deleting old DNS data, old domain name registration data, domain name that was registered in 1998 and deleted in 2000, no one ever registered it again, and we still had all of that information and we never used it for anything. Which is kind of...we had an institutional desire to keep everything and not delete it. That was quite hard culturally to shift, but actually, it's quite a nice feeling when you throw a bunch of stuff away, it's like yeah, it's a good feeling to clear out all of the old data that you never looked at and I should be a bit more disciplined around our practices. I mean a couple of examples, so, when we... sometimes there are complaints that a registration is using identity theft and we require a registrant to provide some sort of evidence that they are who they said they were. That would be in the form of say, a copy of their passport, or some other ID, and we just... people would email it in, then it's on our email system. The email systems are backed up, they're copied and we have a warm site in Geneva, outside of the EU. None of this stuff was particularly thought about, and it was pretty much kept forever.

So, we had to be a bit more rigorous about, we're only going to keep that ID verification for three months maximum, and then it's going to be deleted and the system needed to be changed. For those of us who travel for work, our passport information and visa status, dates of birth, all the other information you need to have for visa applications and travel bookings, are kept by an external travel company. But when a member of staff left we didn't have a process to inform the travel company that that member of staff had left and their details are still on a third party company, right? This is then actually we need to some improved housekeeping to make sure that there are better processes, so actually now when someone leaves, part of the leaving checks is, OK, tell the travel company that they've left, otherwise 5 years time, the travel company has still got all their passport and personal data on their systems and they can;t need it, they've left the company. So, there were quite a lot of fairly small, minor, non-compliance issues around the way we were operating which fell out as a result of the GDPR project and we're still uncovering a small amount of those, but ultimately I think, I think everybody is in agreement,our board and the audit committee who oversee the sort of corporate risk, have been very pleased that this is absolutely the right thing to do, and it has resulted in a better operation as a result.

UNKNOWN SPEAKER: We also apply a data retention policy for the DNS traffic that we use for data analysis. So, we have a data retention policy of 18 months and the motivation there is that we keep one month one year of data to analyze and then we have six months to do the analysis. After 18 months we basically throw it away... we aggregate it, so that it... all the IP addresses are removed and we can only keep it for statistical reasons.

UNKNOWN SPEAKER: The DNS data is not really personal so that's not a major issue. I heard him... I heard Diego say about credit cards, we don't even... we don't keep any credit card data, we don't even process this on our side, we push them straight offline so it is not our problem. I propose basically, to look at what time you need to keep data for text record purposes, and what time you need data to keep for prescription, so that if a client can... wants to sue you that, you have only got three years in [inaudible]. So, we don;t need audit data that is beyond the time we can actually be commercially attacked in any way in a sense of commercial disputes. If the text that takes [inaudible] it's five years, so after five years we can actually destroy the paper documents. They haven't come after us for five years, [inaudible]. Maybe that one can be used, one can look in each country at a figure out for each country when what your local regulation is, and if there is no real need to keep that data and then just kill it.

UNKNOWN SPEAKER: I want to ask you something, all of you. Who of you consider the password sensitive information and encrypt that information in your database? I assume all, right? And, which other information is considered sensitive and is encrypted inside the database? Emails, phone numbers, address? Yes, I want to ask you if you're encrypting, and if you're encrypting backups? Obviously, probably yes but it's a thing we need to think about.

UNKNOWN SPEAKER: I think account login information and ID and password is personal data, so falls under the regulations and therefore you have one of the principles of data protection is to keep it securely, so it's very important that that information is kept securely and therefore to have... it should, if you have ISO 2701, these sorts of things you should have good processes in place for strong passwording, two factor authentication and all these other sorts of things which should mean that, that is secure and that we should be compliant, so it is personal data or you should treat it as if it were personal data, and that involves things like basic security levels. In terms of sensitive personal data, the registry... the domain names, the names and addresses of registrants should not be sensitive personal data. Sensitive personal data is a special type of personal data which attracts a

higher level of protection, and these are things like your religious beliefs, political orientation, sexual orientation, so personal health data, financial information. These are all things that require explicit consent for processing and you need to be much more careful about, but, in terms of sort of DNS traffic analysis, the usual domain name records that you have as a registry... that was largely free of the sort of considerations used at the higher level, considerations that you would have to apply to sensitive personal data. Obviously in terms of the HR department, finance department, payroll, then that does apply, but the payroll department needs to have my financial information to pay me, please, and HR obviously, they have sort of health status, we have some staff members have got disabilities and these need to be taken into account in terms of health and safety. There's a legal obligation to collect these, so, it was a fairly small part of the overall analysis but it was an important part.

UNKNOWN SPEAKER: OK, in terms of GDPR, any of you think this new regulation is raising the bar of how you're handling information?

UNKNOWN SPEAKER: I think it is, but like Nick said, if your ISO 2701 compliant, then you are already say, quite advanced.

UNKNOWN SPEAKER: Any questions from the floor or from the remote audience? Whoever reaches the microphone first is on.

JOHN LEVINE: Hi, I'm John Levine. I have sort of a background question, particularly for Jacques and for [inaudible]. I notice that the dot US ccTLD has done nothing whatsoever about GDPR, they don't provide proxy registrations, they haven't changed the rules at all. I presums your registries are subject to your national law, so like, why do you care?

UNKNOWN SPEAKER: I think people care, particularly, in a lot of the small ccTLDs because a percentage of their revenue, often comes from registrations overseas. So, let's say you're an African or a Pacific island ccTLD, quite small, 5-10,000 domains, but the bulk of your commercial activity actually comes from foreign registrations because your domestic market is so small. You need to make sure that essentially your marketing channel is satisfied. If you're on the Solomon islands, or something, and you have registrars in Europe that are registering names, even if it's a small number, they want to make sure that their treatment of the data that they're sending overseas is GDPR compliant. I

think for small ccTLDs and other ccTLDs that do allow registrations from outside of their national environment, it's very important for them to comply, basically to be shown as a mature grown up registry, to preserve their... essentially their sales channel.

UNKNOWN SPEAKER: For Canada, there are Canadians that live that are resident in Europe, so we need to comply with their requirement as legitimate. So, a Canadian that live in Europe can get a dot CA domain, but they're a resident of Europe and we need to follow their. It's a good practice.

UNKNOWN SPEAKER: OK.

UNKNOWN SPEAKER: As I said [inaudible], one of the registries you referred to small registry in Africa, a largely commercial overseas component. First of all, it's the right thing to do. I don't want people to do this with my data, personally, and on the other hand as a registry, I take a totally different view. But, it's the right thing to do, and it's not that they going to go after the small registries, this is the Facebook's and the Google's of this world that this legislation is being written for, but if I don't need the data, why

should I collect it, why should I display it, and why should I bother? Also, my registrars, the European registrars are as he quite rightly said, talking to us about these things, are we compliant and what are we doing? Because, they don't want to get into trouble of it. It is this concept of data process and data control, nobody knows which is which, but either one is the other or not, but the point is the registrars may be spoken to by the local authorities in Europe and they will speak to us, so I feel that it's always better to be compliant, pre-empt any problems so that we don't have to bother with this.

UNKNOWN SPEAKER: If you have [inaudible] in Europe that makes sense. I'm still scratching my head about how European law has extra territorial effect in Canada, but maybe we can discuss that over beer sometime.

UNKNOWN SPEAKER: That's a thought that I don't have. Some American ideas also apply abroad without anybody really being able to do anything about it, rendition and what not. That's not the point, the point is it's the fact of life and it's relatively simple and cheap to comply with it. We don't need to display the data because we've been asked about it, we need to have it on occasion, the competition commission asks and on occasion the police ask,

it's a legitimate request, but the data that we don't need, we really don't need to take and the data we don't need to display, we don't to display. It's sort of a wake up call, we don't necessarily have to comply but in the end it's cheap, it doesn't cost me much to do it. It takes a few hours of effort, update the version and then we're compliant and we never have to worry about it. If somebody files a complaint and I'm not compliant, I have to start thinking maybe I am affected and maybe I have to defend myself, and maybe I have to pay some money. If I am not, it doesn't bother me,

UNKNOWN SPEAKER: I want to add something, this is a call... it's really a thing we need to think about. For example, in Costa Rica, there's data protection law right now in place, and not so different from the GDPR, except for the fines. But, yes, it's in place and everybody that collects information, personal information from any Costa Rican shall report that data in some kind of authority, and say they can handle information, they will protect information, they can remove the information when they see it is requested. That is really in place some laws that cover in some point, information collected by TLDs, or ccTLDs.

UNKNOWN SPEAKER: Go ahead please.

MARK SIDEN: I am trying to do an 8-way diff. I'm Mark Siden from the SSAC. I am trying to do an 8-way diff on the stuff that all of you do, and I'm not getting very clear occurrences. In one case you've removed the technical contact, which I find I use all the time, because the problems that I am concerned with are technical problems, and often there is a distinct entity as the technical contact, the agency that built the website, or registered the domain or something like that. So, I am actually surprised that you haven't found it useful for resolving technical problems.

UNKNOWN SPEAKER: When you say...

UNKNOWN SPEAKER: Can I answer this? We like to not talk to clients, we like to talk to our registrars, we don't have contractual relationship with our clients so we do not want to have anything to do with this, it's 5000 individuals are much preferred to talk to 70 registrars, it's their problem. The contract is with us, the registrar is with us, and the client has a contract with the registrar, the contract between the client and the registrar has to conform to certain specifications but we don't want to go after 4000 and I'm quite sure Nick [inaudible] doesn't want to go after 10 million

individual clients. The idea is to have as little contact with the end client as possible and use the wholesaler channel. Therefore if there is a technical problem, it's not us, it's not my problem, talk with the registrar, I am not interested.

UNKNOWN SPEAKER: I think you misunderstand my point. I am a third party who sees a problem with a website, I want to report it if it's a technical problem, I would like to report it to the technical contact. So that's where the technical contact is useful for third parties. Not in your case, but for other...

UNKNOWN SPEAKER: Report it to the admin contact or to the registrar, that's what we see. In smaller places the registrar is identical to the webhoster, most of the time anyway. The do the DNS and they do everything, so if there is an issue, they just go to the registrar anyway, and that's what I want. I do not want to have to talk to a client who does not understand anything that the website is not working... website... domain name. We are on the internet...

UNKNOWN SPEAKER: I understand, and the other thing I saw as a difference... I am sorry, somebody else wants to talk about this issue?

UNKNOWN SPEAKER: I think one of your initial question you said that you find is largely the tech contact is useful. We done an analysis about 40 TLDs that are on our shared infrastructure and platform, and close to 90% of the time it's the same as the admin or registrant, or it's a commercial entity or an ISP or somebody, in which they have an organizational field, in which case it's displayed. So, I would question whether, you know, obviously, you're probably talking a very small percentage of times where it's actually something different or useful, and I think one thing if you're looking at the different things that... we've actually differentiated in our WHOIS between European and local, so in our software, I run Christmas Island, but our software used by [inaudible]. If the WHOIS isn't changed at all, if the person did not register through a European registrar or one of their resellers, or the contact is not... we still display the full information. So, we're a hybrid model and I think a lot of the other ones have taken more of a blanket approach. We went with a... essentially a best efforts initial compliance with the GDPR, so we've only filtered based on registrars, resellers, and contact. If so, if you registered through a Canadian registrar and you live in the US, there's no change to the WHOIS at all. There are different ways to accommodate these sort of things.

UNKNOWN SPEAKER: Some of you distinguish between commercial entities and personal information of individuals, that's an interesting difference, also.

UNKNOWN SPEAKER: [inaudible].

UNKNOWN SPEAKER: I was just going to say that while we're going to remove the technical contact and admin contact from the WHOIS information, we will have, exactly for your case a possibility for you to contact the technical contact and then they can get back to you directly or whatever, but yeah we don't need to publish it for you to get in contact with them.

UNKNOWN SPEAKER: OK, next question.

UNKNOWN SPEAKER: Just a remark from [inaudible]. The thing is that, if you look at [inaudible] which has 400 registrars and 18 billion domain names, they have now a small [inaudible] number of legitimate requests from people that really want to the own data of the domain. So, this is absolutely survivable and I want to emphasise what [inaudible] said, you don't need the data and

you have to really throw it away. I read the 101 paper from SSAC, and I thought at every argument that was given there regarding keeping WHOIS alive in the current form, is forced. I think would be an interesting discussion for a technical meeting perhaps, whether this is necessary or not, so don't know how you will comment as a member of SSAC on that.

UNKNOWN SPEAKER: I wasn't really involved in that document.

UNKNOWN SPEAKER: I put it in a question. How did you come to the conclusion that WHOIS is in the current form really necessary, what you wrote in 101?

UNKNOWN SPEAKER: Perhaps some of the authors will respond there.

UNKNOWN SPEAKER: OK.

UNKNOWN SPEAKER: I have one, I think in what I'm seeing from the registrar, it's really the intellectual property community. I think the thing that's really useful for mitigating abuse and criminal activity are DNS

records and domain records which are available under the ICANN agreement now through the centralized WHOIS. For the people who I speak to, and the abuse mitigation and cert community, even for the IP people, you know, the zone file access is their first area of first stop if you will and I'm just curious maybe the other people, whether you provide zone file access publicly or not, or whether that is something you're considering. We have gone the route of basically shutting down or closing large segments of the WHOIS, but zone files we do make available to law enforcement and IT people through the secure domain foundation in Canada, which has various connections. So, rather than having to respond to an individual request for zone files, which is a headache, we basically let the secure domain foundation have access and distribute it to law enforcement or IT people, or whoever they want.

UNKNOWN SPEAKER: I wish some of the other SSAC people were here, because I am so tired of this nonsense that WHOIS is useless. I mean, I know, people at spamhaus are trying to figure out and analyze, like the domain names they see in spam and figure out which ones are hijacked and which ones are malicious and so forth. I mean, they have this [inaudible] but they will do typically upwards of 100,000 domain WHOIS lookups per day, looking at new domains and they actually have the infrastructure to look at the

stuff and correlate it, figure out, and recognize WHOIS is the same as other known domains. I know lots of people who do this to, so merely because you don't personally happen to know the people who do this does not mean that they don't exist. It's fairly insulting to tell us that we're lying because you haven't seen us do it.

WARREN: So, yeah Warren [inaudible]. Speaking as an individual only. So yeah, following up from what John said. This is used very often, there is a huge number of cases where people's hosting boxes get owned, and their domain gets used for something that they weren't intended it to, random farming or similar. Being able to contact that person and say hey, do you know that your domain is now broken / has gone walkabout / is serving malware, is a really useful and important thing. If it's something that you can actually do in, you know, five to ten minutes, that's one thing. Requiring going off, talking to proxy registration people and getting warrants and stuff, it suddenly goes from I'm willing to help fix this, to it's not worth the trouble.

UNKNOWN SPEAKER: I think really we're sort of getting a little bit away from the topic at hand. Personally I am also upset about when I get a spam mail from a UK entity and find that domain was registered the

same day and the next day it's gone again. Big deal. Grow up. Get on with it. There are some things that is not worth really blowing ones blood pressure on. Whether on the gTLD WHOIS, they can have a privacy system or not. On the ccTLD it depends on each ccTLD manager, and basically it really doesn't... the idea is, actually what we can do technically, not what we should do, or what the SSAC should do or whatever.

UNKNOWN SPEAKER: There's the whole endless swamp of tiered access that I will stay away from here, but it really is the case that even in its current cruddy state, the information in WHOIS and the contact information is useful both for what Warren is talking about to contact people to say to fix stuff, but it's also extremely useful to recognize, you know, when you seen... to basically to recognize phish and malware domains in close to real time, because you can correlate the WHOIS data with other WHOIS data that you're already familiar with.

UNKNOWN SPEAKER: It presumes that any ccTLD must provide the same WHOIS data as the gTLD. It is for each ccTLD manager to decide what the hell they want to do, so to make assumption, I don't think you can do that.

UNKNOWN SPEAKER: Sure, but this is ICANN, we're talking about the contracted TLDs, which are, you know... which are... certainly there's a handful of very large ones. The abuse we see, typically, basically the cheaper domain is the more abuse we'll see, and the easier it is for random people to register in it. If your domain is relatively expensive and you require an excess or something like that, then you're not going to see a lot of abuse. But for the common TLDs with the wholesale prices under 10 bucks and your registrars all over the world, I mean, there is an enormous amount of abuse that gets swatted down in real time that you guys just don't see.

UNKNOWN SPEAKER: Thank you very much. I have some conclusions here, or inconclusions... as I see, there's a lot of things to discuss about this, there's a lot of things, we need to check inside each organization. Each of these organizations here handle information different way, and as thinking about how we handled this personal data or personal information, is not just about GDPR, it's about the personal information and the information we manage, and the way we manage. I think it's very important, think about, this is a call, this is the start of things. The thing is not finished here, probably we will see some GDPR like other laws in other countries, and with more

restrictive laws and restrictive policies. Then we need to think about, I don't know, maybe 15 years ago, 20 years ago, have the WHOIS with all information, that wasn't an issue. Or, have your email published in some web page, it was not an issue. Right now it's an issue, then the illusion of the information, I think it's important to take into account what is not sensitive today, would be sensitive in a few days, a few years, then we need the infrastructure that can handle that change and evolve as information is evolving to protect the information, the personal information of our user, our customers, the people of course. Well, that's it. Thank you very much for your participant and yes.

UNKNOWN SPEAKER: That leaves us, thank you very much, two minutes for Warren [inaudible] to wrap up. Just hang on for a second, let him finish for two minutes. You can take the standing mic.

WARREN: This is my wrap up thing, some thoughts from this, can we have the next slide, woo full screen. So, there have been a couple of general themes which I feel have been going through this, more regulation seems to be a fairly common thing happening now in the world, specifically on the NIS directives, feels like a lot of ICANN people have been distracted by GDPR, and so this new thing which is coming along hasn't got quite as much attention

as potentially it would have otherwise. Apparently, that broke. There we go. As with all regulation, you know, the devil will be in the details as to how it actually gets implemented. It also seems like this is going to affect a large number of ICANN people, so thanks Jim for that. Next slide. Another common thing seems to be a lot of registries and registrars seem to be rebuilding their infrastructure with new better or faster, etc, architecture, and also more sort of attention paid to actual software development methodologies. So making things more secure and more reliable which I think is already good thing that's happening. Next. TLD ops, I think this was also a really great session, you know, how many people here actually have a DR or business continuity plan. I think it's one of those things that people need to focus on before they suddenly discover that they should have made it just before the big flood, or before the earthquake or a fire, or whatever. I think in general people are supportive of this, but we need to keep in mind that, you know, you should have a how do you build a playbook, not here's the playbook for doing it as everyone is different. Next. This was also, I think a really fascinating thing, you know how [inaudible] is managing malicious webshops, or preventing malicious webshops, similar things. I think that there's a lot of fascinating stuff about privacy and how different countries have different things that they will be willing to share with their government or require different amount of government interaction for things like registration

etc, you know different countries have different views on what's acceptable on citizens thereof. Next. SSAC emerging security threats, obviously this had the most handsome presenter, thank you. There is a lot of scariness here, I think that people have spent a lot of time securing their DNS infrastructure, but haven't necessarily paid quite as much attention to the underlying infrastructure and potentially that's going to be something that will be interesting to people, and/or scary, and/or both. Next. GDPR, everybody's favorite topic. I think it was really interesting how similar many different, or many people's sort of response to this is, and also how different it was for many people. And also in many cases, people who are not part of the EU, or potentially won't be part of the EU in the future, are still following along with the general sort of, theme or that because it served general best practice in many ways. Last, I think that there's one last. Thanks to everyone and [inaudible] for organizing this, because it's always a huge amount of work, and for staff etc, and see you in 63. Thank you.

[END OF TRANSCRIPTION]