ICANN86 Seville | PF – ccNSO: ccTLDs and Registrars Tackling DNS Abuse
Wednesday, June 10, 2026 – 16:30 to 18:00 CEST

CLAUDIA RUIZ

Hello, and welcome to the ccNSO, ccTLDs, and Registrars Mitigation Abuse Session. My name is Claudia Ruiz, and I, along with my colleague, Joke Braeken, are the participation managers for this session. Please note that this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, the ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment Policy. Please observe the following guidelines to participate in this session. They will be noted in the chat for your reference. During the session, questions or comments submitted in chat will be read aloud if put in the proper form as noted in the chat. Interpretation for this session will include English, Spanish, and French. If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute. On-site participants will use a physical microphone to speak. Please state your name for the record and the language you will speak if speaking a language other than English, and please speak at a reasonable pace to allow for accurate interpretation. Thank you. And with that, I will now hand the floor over to Nick Wenban-Smith, moderator for this session. Thank you.

NICK WENBAN-SMITH

Thank you very much, Claudia, and thank you for the housekeeping rules. So feel free to log into the Zoom room, which is available from the schedule, or obviously we'll be keeping an eye out for participation. So my name's Nick Wenban-Smith, and I'm with the .uk registry, and I have the capacity to do this by virtue of chairing the ccNSO's DNS Abuse Standing Committee. Many sessions have been held about DNS abuse. Many sessions. So how do we do something interesting and different and creative? Well, we, in our sessions, have had community suggestions around what do people want to talk about? What is valuable? How can we discuss further DNS abuse across different constituencies? Because what we tend to find is that individual discussions about DNS abuse happen in the swim tracks. So in the different constituency sessions, constituencies talk within themselves about DNS abuse. And one of the suggestions we had was that we should interact more with other parts of the community. So earlier today, we had our sessions with the Registry Stakeholder Group. That's the gTLD registries, on the basis that we're all registries and criminals and threat actors are relatively agnostic about which type of TLD they use. They don't mind if they use a ccTLD or a gTLD. So maybe we should not make policy for each other, but we should have good discussions between each other about what's working, what threats are we experiencing, what trends are we experiencing, what works well, what doesn't work well, to everybody's mutual benefit. And I'm very pleased to open this session, which I've really wanted to have

for a couple of years now, around working with our registrars better. So as registries, we can see abuse moving from one registrar to another registrar to another registrar. Registrars see it the other way around, through the other end of the telescope. They see abuse moving from a ccTLD to a gTLD to another gTLD, et cetera. So we each see different parts of the same picture. So what I'm interested in exploring, and this is why I think I'm so pleased to be able to have this session, is to actually have some of our registrar friends in the friendly ccNSO room to discuss a bit more how we can help each other, what we can learn from each other. And in the nicest possible way, in accordance with all of the ICANN community standards, of course, what are the things that do not work quite so well for each other? So that is also, I think, just as valuable to learn those sorts of experiences.

So I'm very pleased here to have, therefore, two ccTLD managers and two registrars. The registrars we've picked because they are in the Registrar Stakeholder Group and part of the DNS abuse leadership from the gTLD registrars. But we have made sure that they are gTLD registrars with a lot of experience of registration in ccTLDs, so they can see things from both sides of the fence, if that's the right word. So, very, very pleased to welcome Hilde. I think Hilde, everybody knows here, is the CEO of Norid, the .no. We have Christian, who's the registry manager for .se. This does look a little bit like I'm favoriting the Nordic region. Of all the ccTLDs, it's like my children. I don't have favorite ones, okay? But they were the first to volunteer, and so you've got to humor me. So if it appears a little

bit Nordic-heavy, then that's okay, but there will be lots of opportunity for interaction. So especially for people not from the Nordic region, I'd be really interested in your perspectives when we get to the general discussion. From the registrars, I'm very pleased to have Reg from Tucows and Luc from Namespace, and I hope we have a good discussion. So the agenda for today, we've got a full 90 minutes, so we want to make full use of this time and have an engaging and, I hope, valuable community discussion. We're going to spend most of the time talking about perspectives from the ccTLDs about how they work with their local registrars, whether they're ICANN accredited. Obviously, lots of us have registrars who are not ICANN accredited, so that's an interesting point. And then what are the points of pain? How are things working from your guys? Are there any opportunities for better collaboration, or are there any opportunities to reduce pain and friction? And what I'm thinking for primarily is the 99.9% of completely legitimate registrants who operate in our TLDs and how we can make the user experience really, really exceptionally good for those vast majority of legitimate registrants, whilst also making sure that our namespaces are safe and are trusted, have credibility with our governments and regulators, and are hostile environments for criminals and threat actors. That's what we want to achieve here, and I don't think anybody in this room would, well, I hope nobody in this room would disagree with that. So, with that, I will pass the floor on to Christian, on the right, to kick off the lightning perspectives. I'm very open, by the way, for interventions. I will keep an eye on the comments in the Zoom chat as much as I'm

able, as well as managing the session flow and timing. If I've missed something, please feel free, staff, to point that out to me. And anybody in the room who's not on Zoom, this is very inclusive, please wave your hand at me. The cake has been taken away, so you can't throw cake at me. So yes, just attract my attention and I will try very hard to make sure that everybody's voice is heard. Thank you, and over to Christian.

CHRISTIAN EHRMAN

Thank you. Christian Ehrman speaking from the Swedish Internet Foundation. So this, as being a lightning talk in only five minutes, I have two slides, so I had to leave some things out. Now, this says very big, correct registrant information. I think I would like to start making it clear that no matter if we have correct registrant information or incorrect registrant information, there will continue to be abuse. Abuse will continue to happen, but of course, we have to deal with it some way. At the Swedish Internet Foundation, we have a very clear policy saying that we do not act on content on domains. We are an infrastructure provider. But we should make sure to design our systems in a way to give others possibility to act on abuse and criminal activity. So in that sense, we should not act as law enforcement, but we should or may assist law enforcement. And I think we'd like to just compare a bit with real life. So just as an example, if you are a landlord and you have a couple of apartments, there might be illegal activity within this apartment, and this is, of course, not your responsibility, and I don't see as a landlord that you should do something about this illegal activity.

But should the police come to you and say, "Who rents this apartment? Who is in there?" you should probably be able to assist them with that information. So when the police contact us as a registry, we should be able to give them the correct registrant information on whoever has registered that domain, and in that sense, help them with their job as the law enforcement. So this also comes to other people working with abuse, researchers that should have easy access to as much data as possible, also as legally possible. GDPR restricts us a bit. We, for example, also have an open zone file, and we know a lot of abuse researchers use that data in order to find bad things online.

So one of the issues we have in this policy of ours is that people do, of course, want to get around it. There are anonymization services online where people offer that you can register a domain through them, and they will put on their name instead of yours in order to shield your identity. And it's not fantastic for us to put a smile on our face and telling the police this domain is registered to Anonymous Ltd, when it's so clear for us that this is definitely an anonymization service. So we added into our terms and conditions that information must be complete and correct. That was already there, but we added information provided with the intention to shield the identity can be considered as incorrect. And we did that since we have in our terms that we can deactivate domains with incorrect data. So we do see anonymization services as incorrect data, and when we find incorrect data, we will deactivate the domain. Actually, we will notify the registrar to verify the data on

the domain, and if they don't update it within the deadline, we will deactivate the domain. So we use correct registrant data as a way also, when we see abuse happening, we ask for verification of the data. If the data is correct, it's up to law enforcement or others to deal with it. If the registrant data is incorrect, we will then deactivate the domain, but it will be based on that, it will not be based on the abuse. Thank you.

NICK WENBAN-SMITH Thank you, Christian. Are there any questions either from the panel or from the room about the .se? I have a couple of questions, but I'm very happy to allow questions as we go along. So my question to you, Christian, was around your analogy about being the landlord, and you have people who are in your building and they pay their rent on time, but it's not your responsibility for their wrongdoing. And I was wondering, I think in the UK terms, there's a concept of what's called Nelsonian blindness. So Nelson was an admiral, and he was blind in one eye and had a good eye. And when he didn't want to see something, he would put his telescope to his blind eye and therefore refuse to see it. So if you see your registrant, the guy who's occupying your building, taking in stolen goods or operating a fake web shop, do you tell the police? Or do you just put your telescope to your blind eye?

CHRISTIAN EHRMAN Well, I think it's very rare that we tell the police directly, but we use a service from IQ Global called Abuse Manager, where we can share

reports with our registrars. We don't have the obligation for the registrars to act directly, but I would say most registrars do act on abuse, and they are also more nearby the customer, especially if they are a retail registrar. Often they have the hosting service and can maybe do something. And it differs very much if it's a hacked website or if it's someone doing abuse on purpose. And for those doing illegal stuff and abuse on purpose, it's quite often more up to the police to do that. But yeah, normally we do not inform the police directly. We work more together with our registrars in that sense.

NICK WENBAN-SMITH: Excellent, because this is a ccTLD working with registrars session, so that's good. Do you, in your registrar accreditation agreement, require your registrars to act on abuse reports and to act on alleged criminality and to cooperate with the law enforcement authorities?

CHRISTIAN EHRMAN: No, we only require registrars to have information on their website on how to report abuse to them and how they handle these abuse reports. So we don't have direct requirements on how they must act. It is different from registrar to registrar, how they act on these reports, but we see that most registrars handle it very seriously, and we do not want to detail regulate in our registrar agreement how they should handle every case they receive.

NICK WENBAN-SMITH: Excellent. My final question, around the privacy services, I see that you consider identity shields to be considered as incorrect registry data, and I think that's an increasing trend. And is that completely unconnected with your obligations under NIS2 regulations, or is this just a happy coincidence that you're doing it this way?

CHRISTIAN EHRMAN: Well, we have seen a lot of abuse coming from domains registered to anonymization services, and it really comes back to it that it really does not feel great for us to come to the police and say, "This is this anonymous Ltd in this Pacific island," when it's so clear that this domain is registered by someone else. It's also impossible for us to keep on saying that we do not act on content if we would continue to allow these kind of services.

NICK WENBAN-SMITH: Thank you. Very clear. My two registrar friends on the panel, any questions, any observations in terms of the ease of doing business with the Swedish registry on a scale of naught to 10, where are we doing? How is it? Feel free to, because this is like a friendly conversation, right? We want to find solutions and this sort of stuff.

REG LEVY: This is Reg Levy from Tucows. We support a number of ccTLDs and a lot of them have either location requirements or some kind of verification above and beyond what ICANN verification requires of us. So it's not that much different. .se is not the worst. So we know

that in supporting ccTLDs, there are often these types of requirements. So we're prepared for it.

NICK WENBAN-SMITH Thanks. Luc?

LUC SEUFER It's Luc from Namespace. No, I would encourage registries to hire more registrar people, because they know our pain and they try to ease it. So yes, since Christian came on board with IIS, yeah, it became more pragmatic, so thank you.

NICK WENBAN-SMITH Just for everybody's background, Christian used to work in the registrar business and finally came over to the dark side or the good side, I don't know, depending which perspective you take. So Christian does have a lot of experience from the other side of being a registrar, which is why I think registrars like dealing with Christian, because he understands the business and he understands their pain points as well. Thank you. Is anyone else interested in making any observations? Oh. So, David McAuley, who's a fellow member of our DNS Abuse Standing Committee, has got a question for Christian. Christian, how many deactivations do you experience in a year, roughly? And how quickly does a deactivation usually follow a complaint? Thank you for the question, David.

CHRISTIAN EHRMAN I don't have the number right now, how many deactivations we have, but we do have different things that we are searching for, and it could be old, what is it called, bankrupt companies, but it could also be abuse. Most of the deactivations is companies that just didn't reply. Currently, in our data control system, we have 7,000 active cases. And by scrolling through a bit earlier, a very loose guess would I say half of them are already deactivated. So it is quite high numbers. We have a goal of doing at least 20,000 of these verification checks yearly.

NICK WENBAN-SMITH Great. Thank you. Thank you very much. And thank you for the question, David. How many registrars do you have, actually, out of interest?

CHRISTIAN EHRMAN A bit more than 100, so it's on the low side. Yeah.

NICK WENBAN-SMITH And then how many of those would you say are ICANN accredited as, well, just sort of .se specialists, if I call it like that?

CHRISTIAN EHRMAN I don't remember exactly how many are ICANN accredited, but of course, around half is Swedish registrars and half is international.

So I would guess that many of the international are ICANN accredited, but I don't remember.

NICK WENBAN-SMITH: Great. Thank you very much. Super interesting. Great. If I hand over now to Hilde.

HILDE THUNEM: Thank you. I'm Hilde Thunem from the Norwegian registry, so the Just Say .no people. And I will say that in having two Nordic registries, you have gotten two of the registries that are sort of like, we don't judge what is illegal. We don't judge content. And we know that there are registries that do, so I won't say we're an anomaly, because obviously we're the best ones, but we have chosen our path and, joking aside, it's very heavily dependent on the regulatory ecosystem that we are surrounded by. What powers do the police have in Norway? What powers do other authorities have? Where are the gaps? That all informs the solution that a registry chooses. Now, I'm going to talk about a sort of specific service we have, but I need to give a little bit of background first, and that is that we have a local presence requirement. So in order to have a .no domain name, being a domain subscriber or registrant, as it's called internationally, you must be either registered in the Norwegian Register of Business Enterprises or in the National Population Register. So foreign companies can have a .no domain name, but they need to either have a Norwegian subsidiary or to pick a representative that can hold their domain

name for them, and then that is the registrant. So unlike .se, even though we're neighbors, we are different. We do not consider that we have proxies. The registrant is the registrant. And that is partly due to there being a Supreme Court decision in Norway making it very clear that if you let somebody else use your domain name, you are responsible for what happens in that domain name. And that also made it into the new Electronic Communication Act. So it's very clear that as a domain registrant, you are responsible for the use of the domain name. Not the registrar, not the registry, not somebody else, you. And that, of course, informs the whole accountability discussion. At the point of registration, we check that the person or the company exists in the relevant register. And if they don't, they don't get a domain name. So Santa Claus does not get a domain name because he doesn't exist. But what we cannot check is that the person talking to the registrar is actually representing the company. That is something we left to the registrar. So they do the sort of knowing their customer, and they are free to use whatever method works for them, because it's really different from sort of scale on what works for different registrars.

So moving on to sort of not clicking just here, doing this. So we do provide a registration directory service. That is the service formerly known as WHOIS. Ours runs RDAP, but it's basically a service where people can put in a domain name, and they can look up information about the registrant. Who is the one having this domain name? And this is personal data for us. Always. Even for companies, this is personal data for Norid because we ask for a

name of a contact person in the company, and thus we can connect the information to a person. It doesn't necessarily mean that it's personal information for anyone else looking up just the information we show. But for us, we need to treat the data according to GDPR. We still provide a registration directory service that provides quite a lot of data for some registrants. This is after discussions with our data protection agency and because we can separate registrants into what are companies, who of them are sole traders, they get a little bit more protection than ordinary companies, and who are individuals that get much more protection in what we show. And the purpose of this service is to be able to resolve technical problems. So this is basically one of the important purposes for us as a registry, and it's also to allow the public to contact a domain name holder. So if you get a Norwegian domain name, you have to allow people to contact you. You don't have to have the email address clearly identifying who you are, but you need to provide something so they can contact you. Since we have a unique identifier for all of the registrants, either an organization number or a population register number, we can also clearly know which registrant, what are the domain names a single registrant has, even if they're using different registrars. And so we do provide a reverse lookup where you can put in the organization number, and you can get the number of the domain names they have, which registrars they're using, if they have used DNSSEC correctly. So this example up here is basically the National Criminal Investigation Service. I'm guessing there's no problem with having an associated domain check on their domains, but these are the domains they

have. Our main purpose for doing it is to allow the organization to keep track on their own domain portfolio, and also to allow the public to check if they get an offer from a domain, they can also check whatever other domains that business holds. We don't do this for individuals because connecting different domain names when it's an individual can reveal more sensitive information. For example, if I had my name and I had a vote for insert political party, and you knew that that was held by the same individual, you could tell something about my political opinions. So this is why we don't do that for individuals. Of course, by providing the service, we also make it easier for law enforcement or others that have as their business to try to do something about the use of domain names, which is not within our mandate, to see whatever domains a registrant has. If they want that for the individuals, they have to come to us, and then they have to have the right power in law. Law enforcement does, consumer protection agencies does, but not every person on the street can ask for that information. Okay.

NICK WENBAN-SMITH

Great. Thanks very much, Hilde. I am disappointed that Santa Claus in his home country is not able to have his own .no domain name. So, I'm sorry for that. I'm interested, obviously, you have the nexus requirements, so that leads you to much higher know-your-customer checks baked into the registration system. So I'm interested whether that affects, in your opinion, the attractiveness of the .no domain names in terms of it's too complicated, difficult, expensive to register a domain name. I'm also interested in, I know

the Norwegians are very honest, but do you have issues with, say, fake ID being used to get around your systems? And then my third question, actually, sorry, three questions, very rude to do this, but is then the majority of the DNS abuse, as we would understand it in the ICANN ecosystem, is this not through making registrations, but actually attacking legitimate registrants, legitimate websites through compromise because those registrants do not maintain good antivirus protections and content management systems and are bad at updating patches on older websites in particular? And anybody else who's got any other questions, feel free to either put them in Zoom or Signal.

HILDE THUNEM

Okay. Let's see if I can remember all of your questions. But first, my apologies for breaking your childhood dreams of Santa being real, but, you know. So the attractiveness of .no, we think that in a way, we have made a choice in having a local presence requirement that we are gearing towards a smaller market. We are gearing towards the Norwegian market. And what you get by that is when you have a domain name that is a .no domain, it has a different type of identity than .com. And this is a thing that we sometimes talk about when TLDs compete, is that under the hood, we're much alike. Creative setup of DNS is kind of frowned upon because things stop working. So, we can't really claim that .com domains work worse than .no's or better than .no's, they work according to the same IETF standards. But what separates them is the identity they confer on the user, the trust they have in the TLD, and partly the

jurisdiction. If you have a .no domain name, you have an agreement with a Norwegian company, you know that it's going to be Norwegian law that governs the use and the relationship with us. So having made that as a choice and sort of voluntarily, based on the feedback from our local internet community, kept the market small, we still see we are able to compete price-wise with the big ones on the Norwegian market. But that is, of course, important for us. We need to be what our local internet community needs us to be. So that was the first one. Then let's see if I can remember.

NICK WENBAN-SMITH Fake ID.

HILDE THUNEM Fake IDs, yeah. Of course, people steal passports. Norwegian passports are really popular in the black market, I think. People fake their way through a registrar. By doing this, we have sort of ensured that the registrant in our database, the one we have an agreement with, is a real existing entity, but they might not be the entity that registered the domain name, and that is where the registrar is the first line of defense. When we see lots of fake IDs coming through, we have a chat with the registrar in question and ask them to increase their checks on their end, or it will have economic consequences for them. But mostly we see that the registrars are really good at this. .no does not see that much of a level of abuse. There are other and cheaper domains that are easier to abuse if you're a criminal. But as Christian was saying, there will

never be the case that there is no abuse. We are aiming for a smarter class of criminal, but it will never be no criminals at all. There's also Norwegians that register a domain name on their own personal number and then use it to commit crime. Fascinating, and the police had a really easy case in finding out who did the hacking using their own domain name. So, there's always sort of these shades of gray. What we're trying to do is to have a reasonable level that does not impact the legitimate registrants too much.

NICK WENBAN-SMITH Compromised.

HILDE THUNEM And compromised, yes. As one that has local presence requirements, one of the things we see with research, if people have seen some of the comparisons done with the Irish top-level domain and the Dutch top-level domain and the Belgian top-level domain, is that if you have local presence requirement, you usually see more that domain names are compromised than that they are registered maliciously, because it's cheaper to attack somebody else than to try to steal identity. And criminals are really good at getting cheap deals, I guess.

NICK WENBAN-SMITH Great, thank you. Are there any other questions? Let me read the Zoom. Yeah. So there's a question here about if you're using a fake ID and you use an individual fake ID, like a real person, they get

better protection through your data. I think you have exemplary personal data handling, but that also acts as a bit of a shield to criminals who've stolen fake ID, makes it easier for them to evade mitigation action and justice. Is that a problem?

HILDE THUNEM I think at least it makes it harder to look up and find out that you are a domain holder in our domain database, because you need to do a bit more in order to check. You can yourself check if there's something registered on your personal number, but it's, of course, a bit harder to discover. Now, we do one other annoying thing that really annoys the criminals, and that is that we have a quota, a limit on the number of domain names each registrant can hold. And for a private individual, it's only five domain names that you are allowed to register. And so if somebody steals your identity, they can't really do a lot of spamming because five domain names is not too much when you want to spam a lot of people.

NICK WENBAN-SMITH You only allow five domains.

HILDE THUNEM Per person.

NICK WENBAN-SMITH Per person. This is really fascinating. Do you not have any secondary market investors in Norway? They must be pretty angry, right?

HILDE THUNEM Yep. Companies get 100, lots of domain names. But yeah, we basically put that in place as a mechanism to ensure that there is cake left at the table for the latecomers, that somebody does not buy up all the domain names and sit with a large portfolio. And this is, of course, not that good for the secondary market, but we think people could buy the domain name directly from us for the price of a cup of coffee instead of going to the secondary market, and having to deal with somebody saying, "Yeah, I have a special price just for you."

NICK WENBAN-SMITH Well, you've done a very good promotion for the Norwegian registry. I'm interested to hear from the registrars. It sounds perfect, like it's completely frictionless. It's cheaper than the gTLDs, has no crime and no speculation, and is small but perfectly formed and probably one of the easiest registries you have to deal with in the whole world. I'm only doing that to make the conversation a bit more spicy. It's all friendly, so keep it nice. Luc, any observations on, do you distribute Norwegian domain names, or is it too annoying?

LUC SEUFER

Yes, we do. And yeah, if you keep your zone completely closed, you will have no abuse. So you can turn off the internet, no abuse. It's the same principle. But yeah, no, we are working with Norid and we have a hands-on approach, I'd say. And we can be pretty restrictive when we look at our terms of service, but we are a good partner.

NICK WENBAN-SMITH

But commercial registrars, the last time I checked, it says on the description they are commercial registrars. Is it still possible to make money doing business with these incredibly small, restrictive, low-abuse registries? Don't give me any trade secrets, your competitors are in the room. But it sounds challenging and why do you bother where you could just sell lots of .coms and make lots of money?

LUC SEUFER

What do you call it? Universal acceptance. You need to offer domain name registration to everyone in the world. That's how we see it. And yeah, and also international entities, they will want to be present on each market and have their own piece of the namespace, so they will want to be protected even in Norway, even if it's just with, no, it's 100 domain names you said now, so that's enough.

NICK WENBAN-SMITH So there's enough cake on the table for the registrar to make an honest living from the business is important, right? Otherwise, the thing doesn't work. Reg, sounds great.

REG LEVY Yeah. Similar response. Our customers want it, and so it is worth it to us to offer to our customers what they want. Our direct customers are primarily resellers, and so if a reseller is a local Norwegian hosting company, then they're going to want to be able to sell directly to their local clientele, and that's something that we very commonly see and one of the reasons that we support as many TLDs as we do.

NICK WENBAN-SMITH Great. And this sounds wonderful. So I'm really looking forward to increasing ccTLD business and, yeah, this is going to be a shorter, less spicy session than I thought. But this is before the registrars have had the opportunity to tell us about the things that perhaps don't work quite so well from their perspectives. So the clicker. Oh, there's a question in the chat. I'm sorry. So we have a question from Jaijit Bhattacharya. Christian, are there punitive powers that the registrar directly has, or does Norwegian legal system provide for punitive action for those detected with DNS abuse? Also, what are the statistics of false positives? I think this is actually a question for Hilde, if it's the Norwegian one. So, do you provide for punitive

action around DNS abuse and do you have false positives, I think is the question as I read it in the chat.

HILDE THUNEM

I think as we don't judge what is illegal and neither expect actually the registrars in their hat, in their role as the registrar, to judge what is illegal, we are not doing any punitive things toward them. The police will, of course, if it's criminal activity, do something about that. And I think the registrar also often have the role of a hosting service provider or something else. We try not to mix those roles. We have no right to require any certain quality of their hosting service because it's not part of the role as the registrar. But as a hosting service provider, people are more itchy about having illegal content on their servers, and that makes perfect sense. But as a registrar, all you do, in essence, and it's a really important job, but it is, you log on, you put stuff into our database on behalf of the customer. And it's not really a content hosting service.

NICK WENBAN-SMITH

Excellent. I've got a couple of other questions for you, Hilde. And we have got plenty of time, and I do want to be able to answer questions. If there's any other questions in the room, please indicate with your hand or add it in the Zoom question. So I've got a question here from Vojislav Rodic. Is it possible, I think this is for Norway, for legal persons as domain subscribers to hide their true identity from public view? And if possible, is it an additional free

service, free of charge, or do they have to pay for that privilege of having their identity hidden?

HILDE THUNEM: No, it's not possible. We will show the name of the company, we will show the organization number. This is after discussion with the data protection agency that this is information that we can provide. If you have a domain and you look it up and it's held by a legal person, they cannot pay us to hide that information or get that hiding for free either.

NICK WENBAN-SMITH: Christian.

CHRISTIAN EHRMAN: Yeah, I just wanted to add that it's the exact same for .se. It's not possible either to hide the identity if you are a company in the WHOIS.

NICK WENBAN-SMITH: Thank you. I've got a further question from Pablo Rodriguez. Do high prices serve as a deterrent? I think everybody on the panel should have an opinion on this question. It's a spicy question. Thank you. But Hilde can go first.

HILDE THUNEM

I think that, yes, a way of deterring a lot of certain types of DNS abuse would be to have your price really, really high, because that would make it really expensive. The business case of spam is having a lot of addresses and a lot of domains you can burn through. The domain generative algorithm, you need a lot of domain names. So if it's really expensive, it becomes a bad business case. Unfortunately, it also becomes a really bad business case for legitimate users, so we don't do that. And domain names are, in a way, really incredibly cheap if you compare with other services, at least from the registry perspective.

NICK WENBAN-SMITH

Who's next? Luc?

LUC SEUFER

Oh, yeah. Sorry. I wasn't paying attention. No, high prices don't always deter abuse. I don't know if we have someone from .cu in the room. We are reselling them. I don't know if we can mention price, but above 1,000 euros per year, because it's also a high price from the registry. And we had one case where it was for a BEC attack, so a business email compromise, like a president fraud, and they absolutely wanted this domain name to impersonate one company. They paid for it. They did not care. They had the resources to do that, because they knew that at the end of the telescope you use, there is money to be made.

NICK WENBAN-SMITH Wow, thank you. And Christian and Reg?

CHRISTIAN EHRMAN So I think often there's a bit of connection. We used to have some extreme campaigns, like in 2017, and it was clear that we had more abuse, more ADR cases, and so on. But that's when you come down to really cheap pricing. I think if a domain is $10 or $15, I don't think that makes much difference, but if you sell domains at $1, that usually increases abuse.

REG LEVY Yeah. We have found that there is a relationship between price and abuse to an extent, which is to say, if you're giving domains away for free, that probably attracts abuse. But if you are selling domains because there's such money to be made in abuse, it's so lucrative that they'll just absorb the cost. So they will go to the lowest price available, but as Luc demonstrated, if that low cost is still high, they will simply absorb the cost.

NICK WENBAN-SMITH Yeah. We're here friends, but I don't think any of us are sorry as to what happened with the .tk domain name and the business of giving away thousands and thousands of domain names for free. There's a final question here just about this ID stuff. How do you know when someone supplies the ID? It's obviously a remote transaction. How do you know that they are still alive? Because you don't check the date of birth or anything like that, right? I guess.

HILDE THUNEM

I can answer the part that we can check, which is we check in the population register if they're alive and they are living in Norway, and if so, they get a domain name. Then every year after that, we will check in the register and see if they've died. And if they have, we will close off their ID from being able to get any new domain names, because we don't believe in zombies. But we will not do anything else. We will leave that to the registrar, because often the registrant will not know who we are and to get a letter a long time after the event as well. Our experience is that that sorts itself out with the registrar handling it and either transferring the domains to somebody else, a family member or something, or just not renewing, and it will sort itself out. For companies, we check every day if they have died. And if they have, we will put them on a list for the registrar in question, is, "Here are the companies that have been deleted from the business register. If you want to do something before we start a process, here's the list." And then after a while, we start sending out warnings that, "You no longer exist. The domain name has to be moved to somebody who does, or we will delete it."

NICK WENBAN-SMITH

Sad times. No walking dead in Norway, in the domain name registry anyway. There's another question here, but Christian, feel free to reply as well.

CHRISTIAN EHRMAN

Yeah, just a quick follow-up from .se. Since we started to do the same as Norway recently, we only do it on Swedish private registrants. We found that we did have a decent amount of domains that belonged to people that didn't exist anymore. So we use this procedure where we notify the registrar. But since this is highly sensitive cases and it could take a long time for the registrar to handle, we have decided we only start five of these per week, and we see that it will take us about a couple of years to go through all those that we found already. But yeah, that is highly sensitive.

NICK WENBAN-SMITH

So we have one hand up and one question. So let's deal with the hand first. Thank you, Maciej. And for Hilde, after this question, there's another question about the Norwegian Supreme Court ruling, so get your lawyers ready.

MACIEJ PIASECKI

Maciej Piasecki, ICANN Fellow with EURALO. So thank you for your help in fighting crime, including DNS abuse, because that's obviously in the interest of end users and some courts as well. But I cannot ignore the fact that you all come from countries where the law enforcement is held to high scrutiny and high standards. And are you sure this exact approach should be applied in countries with higher levels of corruption where police might be pressured to spy on political opposition or thwart legitimate businesses? For

context, two years ago, a Polish court acknowledged I'm a victim of unnecessary police repressions when I was working as a journalist, and my editorial office was a victim of numerous cases of government overreach. So this is not a complete edge case. Or maybe our chair would let somebody from the room to share their opinion.

NICK WENBAN-SMITH

I think it's a great question, and it's a very important subject. So yeah, I think we are looking at a specialist area of the globe where I think it's understood that the societies have quite high trust in the public institutions, and there's lower levels, not completely zero, but there's lower levels of corruption. I'll leave Hilde to respond.

HILDE THUNEM

I think that's an excellent point, and this is sort of the beauty but also the frustration of the ccTLD world, is that at the heart of it, we are local, and we're fitting into a local internet community. And we're surrounded by, as I was saying, a legal regulatory ecosystem. So in Norway, the official databases are held by the Norwegian government. We can use them, thus we can do this. And the police and justice and court system holds reasonably well, so we can lean into that. In another country, that might be quite different, and the needs will be different, and the DNS will not be able to sort of fix the underlying issues of corruption. So, this is not a sort of everybody do this. There are countries that having a national population register, where the government has your name and a number, is

culturally a no-go. That will not happen because of the culture saying that we cannot do this. We cannot register people like that. That leads to bad things, and that's completely understandable.

NICK WENBAN-SMITH: Brilliant. So there is a question for Hilde in the chat about the technical specifics of the Norwegian Supreme Court ruling. What I'm suggesting we do, we move on to the next talk, and Hilde, perhaps you can type in a response in the chat. I don't want to either get it wrong or take up more time. Please move on to the next session. So, please now, Reg, I think.

REG LEVY: Thank you. So, as I said earlier, we deal with a number of ccTLDs, and everybody kind of does something differently. But from my perspective, a request that I would make is help us help you. There are, as Hilde mentioned, some countries that have a national register. If you give us access to that, then we can check it. If you don't give us access to that, then it is very difficult to do the types of checks that some countries require of us. There's one ccTLD that requires this, gives us full access. It's wonderful. We can just perform an API lookup. Does this match what you have in your records? And if it does, great, moving forward. And another country that requires it, and registrars very specifically are not allowed to ping that database. So it makes it very difficult. We also have some registries that we work with that they perform the verification. We're also fine with that. If you're fine with us giving you the data

that we have and you perform the verification so that you're pinging that database instead of us, totally fine with that. There's a number of ways that this can be done, and we appreciate all of the help that you can grant to us. I was going to congratulate Hilde on Norway having absolutely no identity theft, because very clearly, in France, there were a number of instances where the entirety of that national database has been stolen. And so that makes it very easy for people to pretend to be someone that they're not. Back in 2024, the ccNSO presented a result of surveys regarding the type of verification that was performed within the ccNSO world. And at that point, 25% of ccNSOs self-reported indicated that there was some form of pre- or at-registration verification. From our own experience, looking only at gTLDs, we have 72% of verification at or before registration. So there's a lot of discussion in the industry, right, or excuse me, at ICANN right now about whether or not data verification is a bar to DNS abuse itself, and it's not something that we have necessarily seen. We published a report recently that showed that 80% of all, no, other way around, sorry, 98% of all abusive domains were already verified. So we know that this is happening, and that registrant verification of the type that necessarily correlates directly to a national register is not necessarily what is decreasing DNS abuse. I think those were my points. And now I'm going to grant this back. Oh, wait, no, sorry. It is my turn for questions.

NICK WENBAN-SMITH

So, this is interesting, the statistics, the 25 and the 72, because from my, maybe I'm selectively looking at the data, but my understanding from, say, Netcraft reports or the NetBeacon monthly reports, more or less, ccTLDs have one-tenth of the level of reported abusive registrations that gTLDs have. But what this data seems to indicate is that gTLDs are doing more data verification, but it seems to be completely disconnected to the abuse correlation. Is that the point you're trying to make?

REG LEVY

That's my understanding of what the data shows, both from NetBeacon and our own experience, that there is virtually no correlation between data verification and DNS abuse. There are certain TLDs that have a very high requirement for data verification, excuse me, registrant verification, similar to what Hilde presented for Norway, but have an astronomical amount of DNS abuse in them. And so, again, as we're looking at the data, we don't see that correlation.

NICK WENBAN-SMITH

Very interesting. So do you think we're looking at the wrong problem, and it's not so much the malicious registrations, although it is a specific problem in certain contexts, but it's more compromised websites, domain names point to compromised websites, and that is the origin of a lot of abuse which is visible and reported on?

REG LEVY

I think there are both. There are compromised domains, and there are malicious domains. And I think those are two separate categories, right? So my domain gets compromised when someone logs into my account. But my name may be used right now on a domain, and I would have no idea because I have a stack of invitations from various companies to give me a year free of a background check for myself because my data has been lost by so many people. So there's not a correlation between DNS abuse and registrant verification, especially since there are such databases available of personal information.

NICK WENBAN-SMITH

Great. I mean, Tucows is a listed company, is that right? So you have shareholders, and shareholders are, we're a membership organization, and so we don't have shareholders. We have other problems, but we don't have quarterly reporting targets, at least not yet. In terms of doing business, I heard everybody say, "Well, our customers want to have ccTLD registrations, so we provide ccTLD registrations." But surely to optimize your commercial returns to your demanding shareholders, who presumably set increasing revenue and profit and share buyback and dividends and all of these sorts of targets, you go for where you can make the most money. And do you think that ccTLDs, through these sorts of things, having more restrictions, doing more checks, having less abuse, are less attractive fields to plow commercially? That's not a

very good analogy, but surely, it's just commercial logic. You go to where the money is and where money can be made, and where money can be made fastest and most easily and all of that stuff. And are ccTLDs putting themselves at a disadvantage through these sorts of good behavior policies because we're not motivated by the same sort of commercial profit incentive?

REG LEVY

If you're asking me if I love making money from DNS abuse, the answer is no, because typically they don't use real money to buy it. So it is a financial incentive for my company to reduce DNS abuse however we can. Because we don't see the data correlation in terms of registrant verification, it's not something that we are looking to increase for TLDs that don't require it. That said, people often ask me how much this domain is worth, right? Is reglevy.com worth something? Is someone going to buy it? And I'm like, "Well, every domain is worth exactly the same amount in a relevant TLD, and every domain is worth what you can convince somebody else it's worth." So if we have a customer who is in Germany, they have a much higher value on owning a .de domain than they have on owning a .com domain. So we provide both options. They want the .de. Someone who's living in Florida, in the United States, probably it's going to be the opposite. So the profit, what's the word that I'm looking for? The desire of the customer is where the profit is. And so if the customer wants a .de domain, we want to be able to provide them with a .de domain. And if that means that we have to jump through a certain number of hoops, I'm not trying to pick on

.de, apologies, I should've chosen one of you guys. If it means that we have to jump through a number of hoops, then that's what we'll do because that's what our customers are asking of us.

NICK WENBAN-SMITH: And I understand that from my use of buying domain names and going to registrar pages, you can specifically target through geolocation. So in the United Kingdom, if I'm looking for a domain name, you tend to get the ccTLD higher up the list in terms of the shop window. In Germany, Peter, obviously you're smiling about the free promotion of .de domain names, is probably going to be presented with .de domain names at least through your user portals and things. So that all makes sense.

REG LEVY: Well, and there's also, especially after the most recent round, there's a number of geoTLDs. So there's .nrw, .bayern. There's other domain names that might be of interest to a customer in Germany specifically. There's .london in the UK. If someone comes to the website and wants a .shop, or wants because they have a shop, then we want to be able to present that to them as an option for them. So again, the profit incentives for us are what the customer wants.

NICK WENBAN-SMITH: So final question from me to you, Reg. Is there any TLD that because of the amount of abuse that was coming through, you

would just not supply it? Specifically a ccTLD. If there was a ccTLD heavily abused, would you just say, "This is too much trouble. It's so abused by criminals. They're not using genuine credit card information. We're not getting paid. The overheads are huge in terms of dealing with the aftermath of the abuse. We do not want to do business with that type of registry or that type of reseller," or whatever?

REG LEVY So at the very end, you said that type of reseller. So yes, we will breach resellers from our platform if they are abusive. But what you started out asking was a ccTLD, and typically that's not what we look at. I'm not the marketing department. The marketing department is who makes the decision of whether or not we carry a TLD. And if a TLD is a lot of work, whether it's because of data verification or the amount of abuse it attracts, then we will just price it accordingly.

NICK WENBAN-SMITH Got it. I'm just curious, actually, do you carry every single ccTLD in the world? My favorite example for this is .aq, which is the ccTLD for Antarctica, which I believe has three registrations and no registrars. But apart from places like .aq, do you basically carry them all?

REG LEVY I know that we do not carry them all. I do not know off the top of my head which ones we do not carry, and I would say that some of

them, we may be restricted from doing business as a United States company, with entities in certain areas, so that might be one reason we may not carry them. Or they have extremely high requirements from a registrar, typically along the lines of data verification, and we have a very low call for it. Yeah, market percentage. Thank you. If we don't have a lot of domains under management and the requirements on a registrar increase, then we may drop a TLD, whether it's cc or not.

NICK WENBAN-SMITH Thank you. So I think the next presentation now is Luc, so I need to retrieve the clicker. Luc, last, but certainly not least.

REG LEVY I think we have a problem.

NICK WENBAN-SMITH Oh, have we got, I'm so old, I have to put my glasses on to read anything here. Oh, got hands in the actual chat. So got Andrew, and then Roelof, and then Christian. Great. And Christian, you didn't need to raise your hand, you could've just said. Okay. Andrew first. There you are, Andrew.

ANDREW CAMPLING Yeah. Hi, Andrew Campling for the record. Really interesting discussion, so thanks to all of you, including, I guess, Luc, who clearly hasn't done his bit yet. Just to push back politely, hopefully,

on the picture being painted, really just to ask a question on this. In the SSAC Lightning Talks just before the break, one of them summarized some of the most recent research on DNS abuse, and amongst other things, and I'm obviously cherry-picking the relevant things for this, suggested that bulk registration through API was attractive for phishing registrations, as was a low price, as was acceptance of cryptocurrency. And all of those would correlate with high prevalence of phishing registrations. Whereas even most basic verification, so email verification, which is laughably useless, even that had a correlation with reducing the likelihood. So that was painting a very different picture to some of the discussion just now in terms of what is or isn't a deterrent. And I've heard similar research longer ago from the DNS Research Federation, I think even from ICANN's OCTO, suggesting similar correlation. So that's quite different from what I'm hearing now.

NICK WENBAN-SMITH

No, I think cherry-picking data is my favorite form of statistical analysis, so thank you. And yeah, I've heard the same sorts of things. That's why I'm asking the sort of question, do we see that sort of pattern of correlation? Roelof, Christian, and then Byron.

ROELOF MEIJER

Yeah, thanks, Nick. Roelof Meijer from .nl for the record. Maybe first a kind of a disclaimer, I think as CCs, our job is easier fighting abuse than for, let's say, a global gTLD. We have a single jurisdiction to deal with. We can have nexus requirements for both our registrants

and our registrars. That said, coming back to this slide, I think it's a bit of a quick and easy conclusion. I wouldn't be surprised if there is a correlation between data verification and abuse after you take certain measures. If you just verify data and you don't do anything else, it's obvious that there is no influence. But if you take action and you take action quickly, I think the combination can be very effective, and I think statistics would prove that. To make a point, especially on the difference in this slide, our largest abuse is with global Gs, not with global registrars accredited by ICANN, and not with European or Dutch, which are our largest. And that's because they respond very quickly to our, let's say, suggestion, almost instruction, to do something within a limited time about abuse. So in that case, it has nothing to do with verification of the data. It's about taking action. And in the Netherlands, at least, with our registrars, in many cases, the slowest to pick up that action are global ICANN-accredited registrars, the larger ones.

NICK WENBAN-SMITH

Very interesting. And actually, Hilde, I think, made a similar comment about if they have a registrar who seems to be picking up levels of abuse, they, this is the most threatening I think I've ever heard Hilde sound, where she says, "We will call them up and have a chat." And it's like, well, that sounded pretty threatening to me. Yeah, I think that's a very interesting topic for a different discussion on mitigation and proactivity of mitigation. The speed of mitigation in itself changes behavior because there's no point exploiting that namespace and creating new registrations when you know that

your opportunity to exploit, to commit crime is a very small window. Choose something easier where the door is wide open, right? So Christian, and then we do need to have time for Luc, but, Byron, I saw your hand.

CHRISTIAN EHRMAN Can we go one slide back? Because I had one question for you, Reg, on this one.

REG LEVY Yep.

CHRISTIAN EHRMAN Because I'm looking at it, I'm like, we as .se are failing on basically all what you require. We are not clear on the level that is required. We do not do verification on our end. And for the access to relevant databases, yeah, well, we do give you a link to Swedish, Danish, Norwegian, stuff like that. But since we are open for registration from all over the world, it's not possible for us to provide access to any relevant database. And I want to give just a short example. Very recently, we had a meeting with our regulator. We invited two registrars, one retail registrar and one brand registrar. And they did a presentation on how they worked with registrant verification. And as you can probably imagine, it was very, very different in how they performed their registrant verification, but they were both very good at it. So this is one of the reasons why we don't want to be too detailed. We don't want our regulator to start being too

detailed. So that's one of my background and I kind of want to hear your thoughts on that.

REG LEVY

We love you anyway. So these are my requests. That doesn't mean that if you don't do it, we're not going to carry, as you know, .se. It makes it easier. There are third-party companies that will do this kind of registrant identity verification, and every moment that goes by, they get easier to fool. With LLM video technology the way it is, even having a video conversation with someone is not necessarily a way to prove that you are a real human or are who you say you are. So we outsource a lot of the verification because we don't have professionals who are versed in every single form of identification in the world. But there are services that we can buy that claim to have at least most of the world. At which point it means, okay, if we can verify you, we can sell you a .se, and if you're from a country where we can't verify you, then I guess we cannot. Just makes it harder.

NICK WENBAN-SMITH

Thanks very much. Byron, are you, there you are. I can see you. Floor is yours.

BYRON HOLLAND

Thanks. Byron Holland, .ca. And two questions, one for Reg, one for Hilde. Reg, in terms of the verification, I wonder if you've parsed that to look at registries that have nexus requirements, some sort

of legal tie to the country, and if you see differences in abuse for ccTLDs that have nexus requirements of any substance? And Norway, I'm curious, in the position that you've taken, and you've taken these positions for as long as I've known you, your registry rather, as you see at least the gTLD space, but I would say the broader abuse space, start to evolve significantly, certainly in the last couple of years. The position that you continue to take, one could argue, seems to be out of step with the way the abuse conversation is going. So even just things like associated domain check and those types of things that are issues that are advancing rapidly in the ICANN space and others. Do you expect to be onboarding some of the types of abuse mitigation efforts that we're seeing happen elsewhere in the industry, or do you anticipate staying where you are with the policy environment that you've defended for a long time?

NICK WENBAN-SMITH Great questions, of course. Reg, so obviously CIRA operates in an environment with a Canadian national nexus, so I guess that's a leading question, but it sounds like it's going to be safer than the alternative. Is that right?

BYRON HOLLAND And I just want to say, it really pained me to hear that Tucows was an American company, but I believe it was Canadian. I thought it was Canadian, but ChatGPT that.

NICK WENBAN-SMITH For the wrong answer. Reg.

REG LEVY We're traded on the New York Stock Exchange, so we have to comply with U.S. sanction policies, so that's very specifically why I called us a U.S. company. We are also a Canadian company, and most of the time that is what I call us. But in that specific example, there are far fewer restrictions because of sanctions on a Canadian company than there are on an American company. We're also a German company. So with regard to abuse in ccTLDs with nexus requirements, you said abuse, you did not say DNS abuse, and we don't see nexus requirement ccTLDs not being abused. So it just gets abused by local people, I guess, is what I would say, or people who are pretending to be local. So if someone is targeting, I was going to pick on .de or .ca, but I'll pick on Christian this time. If someone's targeting Swedish customers and .se is a popular ccTLD, then that's what they're going to buy, because that's what they want to represent themselves as. And as I said, it doesn't seem to matter that there are both registrant verification requirements and nexus requirements. There are not nexus requirements for you, but if there were, because that's who they're targeting. So I can't figure out where he's sitting, so I can't look at him, but I, there you are. But I don't actually think that we are seeing a decrease in abuse, even for nexus requirement ccTLDs.

NICK WENBAN-SMITH Thank you. Hilde.

HILDE THUNEM Yeah. I think that for us, it will depend on what is happening in the local ecosystem. As long as law enforcement are able to act efficiently and consumer authorities are able to act efficiently, they are the people that the parliament in Norway has given the right to sort of act on illegal behavior, not us. And so as long as that works fairly well, we will stay within the Norwegian model. It is not something where we see that law enforcement is pushing toward a different behavior. They don't really want us to run around pretending to be superheroes on the internet. So we think we have both a consistent and very clear way of dealing with it, and now with the new Electronic Communication Act, it becomes even more clear in the legal system who is responsible for the use of a domain name. And so currently, we see no change, but you never know. Several years ago, we didn't know there would be a worldwide plague either. So, you don't know what's going to come, but we have no plans and no signals from our government that they want things to be different. We're very much so following the legal system.

NICK WENBAN-SMITH Great. Thank you. I'm going to hand over now to our last speaker. Luc, I'm sorry that we've been a bit time-crunched, but take as long as you want, and that's great.

LUC SEUFER Okay. Thank you. Okay. So yeah, before you ask, yes, I made both slides myself, no AI involved, and so I was saving water. So I'm Luc from EuroDNS/Namespace, as you can see. So, I wish we had more oblivious registries on the panel to spice up the conversation, but Nick decided to invite the savvy ones. So yeah, blame him if my intervention is bland. So as we discussed, regulators around the world, they are pushing for greater data verification of registrant details. So I'm not here to debate whether verification measures are actually preventing abuse. My personal opinion is that a risk-based approach, as the European Commission, in its wisdom, adopted, is more effective, but that's a topic for another day. What I'd like to touch upon is how those verification procedures are being carried out. Because we are seeing registries being tempted to run full verification measures or procedures themselves, and they are reaching out to the registrant directly without involving us, the registrars, or involving us when it's too late and the domain is already suspended or even deleted. And so that's exactly what we should be avoiding. So you have to realize the mixed message we are sending. As a registrar, we are spending a considerable amount of time and resources to educate our clients, the cyber hygiene, if you will, not to click on the links sent by unknown third parties when it comes to their domain names or other aspects asking for

credentials. And now all of a sudden, we have been telling them not to click on that link, and we say, "Click on that link or your domain name will be suspended." And if you reach out directly to the registrant, the registrant, they don't know you as the registry. And it's going to be a different registry for each extension that we have a domain name with. And yeah, I think at one point, your registry had a contest to have the most obscure names. So when the registrant is receiving something from Nominet, they have no idea who you are. They know EuroDNS because they know they registered their name or their domain name with us, and they trust us. So basically what we are doing, or what you would be doing when you do that, is you're creating a vulnerability that will lead to more DNS abuse. Because if we are now telling the registrant, our clients, to click on unknown email or unknown sender's email, they will get their domain name compromised at some point. And as we said before, compromised domain name is a great part of DNS abuse. So yeah, like the Canadian poet has said, isn't it ironic, don't you think? So yeah, you can thank me for the earworm later. But first, my ask is simple. So if registries need to conduct this verification measure, please go through your registrar. We have the relationship, the trust. We've built the channel to the registrant to do it safely. And like Reg said, if you have access to tools that can help us do that, please provide the tool to us. Thank you.

NICK WENBAN-SMITH Great. Thank you, Luc. So just to get the conversation going, we have a Mentimeter poll now. We have eight minutes left. So if we

move on to the Mentimeter. Oh. There we go. Staff have rescued me. Thank you, staff. Oh.

REG LEVY Oh, cool.

NICK WENBAN-SMITH Do we need a code to get to the, there. Oh, all right. Okay. Phew.

LUC SEUFER When we are all voting, maybe I can tell the audience. Yes, we are carrying .aq, for Antarctica, and we had one registration. It was really complex because they have a scientific center there, and they had to evidence that they were actually living there, because that's what the registry requires. And yeah, it's hard.

NICK WENBAN-SMITH I did not know that. That is a good abstract piece of data, which is my favorite type of domain geek data. So what's your affiliation? And then review the following statements.

REG LEVY To Luc's point earlier, we spent decades convincing people not to click on random links, and now we've moved to QR codes.

NICK WENBAN-SMITH

But a trusted QR code. So just coming back to Luc's presentation about things that ccTLD registries do, which delight registrars, and things that ccTLDs do that disappoint or confuse customers or introduce points of pressure and pain. I think what I'm hearing is that unsolicited emails from the ccTLD registry to a registrant who's not heard of the registry, not expecting the email, is unwelcome, basically. And you can see here from the following statements, quite a lot of registries actually do conduct their own verification. And so, sometimes I guess that's inevitable. I suppose for registries which do conduct verification, why don't they, because presumably you have a registrar and a contract with the registrar, you could require your registrars to do this and to not have the situation where registrants who are rightly suspicious of unsolicited emails don't click on the link and then have their domain suspended. That's not a good user experience for the ccTLD's credibility and reputation either. So why don't more registries contractually require their registrars to do this kind of stuff? Or is it a question that there's low trust that the registrars will do what they're contractually required to do, and it therefore becomes a compliance challenge? Do registries not trust you guys? Luc can go first, and then Hilde.

LUC SEUFER

I hope it was a rhetorical question. No, but yeah. Nominet, you are one of the good examples because normally you leave us the choice. I realize that not every registrar wants to do it. We have smaller registrars that may want to have the registry operate it

when, like Christian said, when it's a very local registrar and it only carries the local ccTLD, then maybe they are very small, they don't want to take care of that, fine. But for the other one or for every registrar, leave us the choice, and you've accredited us, so there's a level of trust here. And if we are breaching the agreement by not authorizing the verification, then de-accredit us. Yeah.

HILDE THUNEM

Thank you. I think for us at least, it's sort of a shared task. We will check in the register that the registrant that we are also, in a way, entering into agreement with, actually exists in the register. But all of the verification of contact details and other things is left to the registrar. And we do have a requirement in our contract that the registrant is the one responsible for giving correct data, but that the registrar is assisting the registrant and is acting when they find out that the data is wrong. And that is our preferred way of doing it. And it's only when we see lots of identity theft slipping through, where we will talk to the registrar, and we will also, if we have to, start canceling the domain names of a registrant that did not actually enter into agreement to have that domain. But it would not be our preferred method. If we have to do that, we will send the bill for our hours to the registrar. So it's not their preferred method either. But I think I would like to just say, I heartily agree with you from our perspective in that a lot of this is best carried out by the registrar, and that for the registry, instead doing audits or checks is a better way than emailing the registrant directly. And especially in the case of, I saw the slide and I have the scars, so I saw your slide and I

thought, NIS2 Article 28. It's about verifying and it's about a certain Danish initiative of emailing and phoning the customer every year. That fortunately did not go through, but it would directly present the problem, not only of confusing the customer, but it would give a lower resilience of the DNS because you would have very important domain names being canceled because somebody did not pick up the phone or click the link.

NICK WENBAN-SMITH

Yes. And I think that did happen with google.dk. So, thanks very much for that. I think that what I take from that is ccTLDs, think carefully about how you operate with your registrars. Don't forget the registrars have hundreds if not thousands of TLDs that they work with, so don't make things too difficult for your own customer base and confuse things. So I'm just moving on the slides. There's a couple of informational slides to close the session. Can you move them on for me, Claudia? There's a survey coming up, the third survey, coming up later on this year. There's a draft questionnaire out. Please take time to look at that. It has been distributed through the usual ccNSO website and mailing list channels. And that is going to come out later, as you can see there, between 17th of August and 20th of September. So heads up to look out for that. And then, just to remind you that the ccTLDs, including myself and Eberhard from .na, Diego from .co, Bruce from .au, and Mira from .id, we are all part of this DNS Abuse Mitigation on Associated Domain Checks. Back to Roelof's point around speed of mitigation, and especially with the big gTLD registrars, there are some specific

policy initiatives there to make gTLD registrars more standardly responsive, promptly to deal with domain name abuse and reports and associated domains under the same thing. I just want to finish off then by saying a massive thank you to all my panelists, to all the people for attending and asking interesting questions. I know I'm between you and the community drinks, so now's the time to let you go and enjoy those. Thank you very much for everybody, and I'd like to, just a big round of applause please for my panelists and their openness and their willingness to come and answer everything.

ALEJANDRA REYNOSO

Hi, everyone. This is Alejandra Reynoso. I want to give a very quick few last words on today. As we know, we've been celebrating Bart's retirement, but if you were able to attend yesterday's cocktail, you heard that there was also an announcement of another dear person of our community retiring even before Bart, and that is Nick. So Nick, I would like to thank you so much for all your contributions in the ccNSO. You've been part of the Council, on the Council Triage Committee, on the DASC, DNS Abuse Standing Committee, on the Policy Development Process 3 regarding retirement of ccTLDs, regarding review mechanisms as well, on the Policy Advice Implementation Group of the ccNSO, on the Policy Gap Analysis, and now Vice Chair of the GNSO PDP on DNS Abuse Mitigation of the GNSO, and we really appreciate you, and I didn't want this

opportunity to pass by now that we are all together in this room. So a big hand to Nick, please.

[END OF TRANSCRIPTION]