
ICANN76 | CF – GNSO: BC Membership Meeting
Monday, March 13, 2023 – 13:15 to 14:30 CUN

BRENDA BREWER:

Thank you. Hello and welcome to the BC membership session. My name is Brenda Brewer and I am the remote participation manager for this session. Please note that this session is being recorded and is governed by the ICANN expected standards of behavior. During this session questions or comments submitted in chat will only be read aloud if put in the proper form as noted in the chat.

I will read questions and comments aloud during the time set by the chair of this session. If you would like to ask a question or make a comment verbally, please raise your hand. When called upon kindly unmute your microphone and take the floor. Please state your name for the record and speak clearly at a reasonable pace. Mute your microphone when you are done speaking.

This session includes automated real-time transcription. Please note this transcription is not official or authoritative. To view the real-time transcription, click on the closed caption button in the Zoom toolbar. To ensure transparency of participation in ICANN's multi-stakeholder model we ask that you sign into Zoom sessions using your full name. For example, a first name and last name or surname. You may be removed from the session if you do not sign in using your full name. And with that, I will hand the floor over to BC chair Mason Cole.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

MASON COLE: Thank you Brenda. Good afternoon, everyone. Mason Cole here, chair of the BC. It's good to have you all in the room. It's good to see everybody and we've got a few remote participants on the line as well which is good to see. So welcome to the BC call on 13 March while we're here in Cancun. We have an hour for our meeting today and a fairly busy agenda to get through so you see the agenda on the screen in front of you. Are there any changes or requests with regard to the agenda before we begin? Steve?

STEVE DELBIANCO: Thanks Mason. Steve Delbianco. I wanted to note that the executive committee discussed whether we would have time to discuss a little bit about the statements of interest or the SOI discussions that are happening this week and that will be in all other business if we get to it.

MASON COLE: Very good. Thank you, Steve. We have some guests with us today. Ching Chiao and Ed Gibbs from WHOIS XML API. Gentlemen thank you for joining. I think there's some interesting information that they have to share in the area of DNS abuse which is a long-standing issue of interest for the BC and I understand you all have some research that you're going to show us and then maybe we'll have some time for some questions afterward. And then if there's anything else you'd like to follow up on just feel free to do so. But let me turn the floor over to you. Go ahead.

ED GIBBS:

How's that? Hopefully you can hear me. Okay now. We're going to talk about unmasking global DNS for good, evidence of badness techniques, kind of exposing what is already out there on the surface web and how it relates to some of the tasks that you have and the subjects that you may want to approach in that.

Next slide. So just real quick, I'm the field CTO for WHOIS XML. 30 years' experience in this industry and also published version one and two of ideally a handbook of computer crime investigation. Also a volunteer for the National Child Protection Task Force. So you can imagine we see a lot of things, particularly when it comes to DNS and we're closely aligned with law enforcement and government agencies around the world. So we have a lot of exposure to what is out there on that surface web.

Next slide, please. There's a lot of room to, of course, misbehave on the internet. We're not going to stop it. Whenever there's humans involved, there's going to be good, there's going to be bad. And how do we deal with that? Do we allow ourselves to be exposed to that? And what we have done is find techniques to deal with this, what we call badness right on the internet and expose it. And kind of really if you've heard the term, it's a technical term, dig, undig, and re-dig, means to really expose the records, the DNS records that are there, who's behind them, where they're being registered and what's potentially the intent of those. Is it necessary to monitor? We're going to be talking a little bit about that and then wrap it up and bring it all together towards the end.

Next slide, please. So with the National Child Protection Task Force, as I mentioned, there's a lot of exposure. And one of them is of course, as

you can imagine, the child sexual abuse material called CSAM, which we highlight here is this is a small snapshot of the day in the life of what exists in DNS. And so being able to find these things very fast and make them aware to law enforcement or whoever needs to be informed of those, these different platforms that are out there, how do they want to deal with them? Do you issue takedowns? There's a lot of concern that what's behind these, the material essentially being. Wasn't sure if that was a fire alarm. We got to run.

Apparently, those DNS records are interesting. But it's real, they exist and it's not going to change anytime soon. So being able to isolate these and draw attention to them, to the proper people is critical. Next slide. So just recently has anybody heard of the NetWire Cross-platform RAT? You may or may not have. This is a site that was recently seized by the FBI and taken down through something interesting. They used DNS to do the server, redirect to indicate that the website was taken down. And a search that we were able to conduct found that actually there was 1,537, keep in mind there's probably more today because every day that number goes up, the domains that were associated with the takedowns.

So having this type of hyper indexing capability is critical in being able to associate records in these datasets to be able to produce something that's actionable. Because a lot of times when you're dealing with big, the term big data. It could be chaotic and you're not sure exactly what you're looking for. And you end up not knowing where you are and produce nothing. So...

UNKNOWN SPEAKER: Is that the same as reverse lookup.

ED GIBBS: Exactly, yeah, reverse lookup. And so reverse lookup, being able to normalize the data though, is also important. By normalizing, I mean these records come in in various formats. There's information a lot of times that you have to use some machine language to be able to translate it into something useful. So once you index it, and you can do these reverse lookups and look up the associated records, a lot of times I'll give some examples of where reverse looks up are really effective in being able to find the information you're looking for.

Next slide. So cyber-squatting domains, domains that essentially may or may not contain strings that look like keywords that you might be familiar with. I'm sure we've all probably get the emails once in a while that our Amazon account is locked or something. And you look at the link and go, that's definitely not Amazon. But they want you to think it is. And then it related to something that potentially looks associative. So when we look at the things that we ran analysis of, we could see within a given snapshot, that there are effectively a lot of domains that get created every day that the bad actors are pursuing and creating. So this DNS abuse is very prevalent. And we'll just not going to go anywhere, like I said.

Next slide, please. Fake fashion is a big. A lot of money involved, where the research strings that we typically use, the brand names that are out there, you can see for yourselves, Gucci Louis Vuitton, the big ones 2500 domains between January and March were created. Now, these brand names have a lot of money behind them. And they have brand

protection within these organizations that can issue the takedowns very fast.

But the problem that we see is not only within the root and domain names that they use, they're pushing them further to the left in the sub domain fields to where they exist in AWS or Azure or in a cloud platform, and nobody's going to block a cloud platform. So they create these sub domains using these techniques. And that's becoming more and more common. And when DNS is involved, it's very hard to issue a takedown on the sub domain because you don't know who's exactly behind it, other than the platform that it's running on.

Next slide. This is a very bad attempt to show exactly the research that was conducted, but hopefully, it's not too technical or anything. But you can kind of see here what we call clusters of badness. By clusters, I mean these bulk registrations within domain names that may or may not be more than anything frivolous, somebody doing clickbait or just doing it for the fun of it.

There can be many reasons or it could be everything, of course, to a malware campaign or anything of a really an abusive nature. And when we look at these, the total number of group members is a high number. And the most we've ever seen was 13,358 registered domains at one time. And so it kind of represented the pattern there of this gobu campaign that was being launched.

Of course, we couldn't tell who exactly was behind it, because we don't have the reseller IDs or anything like that, when you look at these records. But you can get into the country that was behind it, the data created, your typical fields that are associated with the WHOIS records

behind these domain names. But you can see that we deal with this on a constant basis. And now we have the tools and the necessary visibility to work with the registrar and registrants to let them know. And of course, they can decide to take action on how they is it infringing on a brand name or anything? And what's the impact, the business impact?

Next slide, please. So this is another example where domain name strings of interest, you can see that on a given day, we found 465 domains of those 465, 137 of those related to in this case, a Louis Vuitton search. And going into popular brand names like Gucci, and being able to easily identify those and bring that to attention.

And again, reverse WHOIS is very, very important, because a lot of these when you look for these, they could be using techniques to squat or obfuscate the name in some way that for example, with Gucci, or Louis Vuitton, maybe they can replace the O with a zero, and your exact search is not going to work, and so it breaks. And there's algorithms that are in the public domain, that do distance measuring, bit swapping and different things to be able to find those type of variations that exist. And that's a lot of the tools that exist out there today, have that capability.

Next slide. Again, another example, we can see that in this case Tokyo Louis Vuitton, obviously, Louis Vuitton did not register those, but the websites are almost identical, even down to the code behind them. So very, very difficult to distinguish what's real and what's not. And so this becomes a major problem for a lot of people, we can see that in this particular case, there were three bulk registrations, I call bulk anything

more than one, of course, where the Tokyo Louis Vuitton name was used on different CLDs.

Next slide. But if we dig deeper, and sometimes in these records, of course, we'll take Prada.com, we can see the creation date, obviously, Prada has been around a long time. The actual domain name itself was registered around what was it? 1997. But all these newer domain names that exist in DNS have a new creation date. And the registering company, I doubt Louis Vuitton is going to use Malaysia to register their brand name. So those are easily identifiable. So combining those signals to indicate that this is a false domain names behind these product attempts would fail.

Next slide, please. So in case of Prada USA online store, these are really difficult a lot of times, because web categories that they're automated, they're using machine language, a lot of times to be able to scan the website, trying to figure out exactly what it is. And using these keywords, build the categories associated with what the results that came back. In this case, they look identical to what Prada.com actually used to what was set up as a staged attempt to commit fraud.

So next slide, please. Yes, that's it. So again, some more hosted on shared DNS infrastructure, what really this means these people aren't very well funded. So they're going to go as cheap as they possibly can a lot of times. And on shared infrastructure, what that means is these are virtual servers that are running, particularly more than one domain name.

And in the case of Prada, Prada is not going to run a web major website, along with 300 other different domain names on it. And so that that

would be a signal in and of itself that this is fake. So it's an interesting study where we see a lot of times, repeatedly using analysis of the brand names that we presented, that shared infrastructure was used. And it's a common signal that there's something bad going on behind it.

Next slide. There you go. And so what are the breadcrumbs? We mentioned being able to redo reverse who is, again, on every field within a record, a DNS, WHOIS record and being able to cross index at to figure out exactly what other type of information, perhaps an individual registered. In this case, we can see that in that one example, where Jeff Randall registered 214 other domain names. Well, what are those domain names? What is our campaign? We can then build that M/O strategy. Well, they're doing PayPal, they're doing Amazon, they're doing maybe brand names or targeting airlines, whatever the case may be. But we're able to start building that profile of exactly what that person's doing.

Now, in this case, this only works when the record the WHOIS record actually is exposed with real information. If there's a privacy shield behind it, which means that there's a company that registered on behalf of them, and they don't actually give out their information. So you don't have that luxury of being able to do a reverse WHOIS to be able to dig deeper. So 20% of the time, it works 100% of the time. So it becomes more -- we see that privacy shields are used more and more. But a legitimate business, such as you take Wells Fargo, Microsoft, Facebook, or any of those, they're going to use their legitimate domains behind the WHOIS records. For the registered contacts and things, you'll see like `hostmaster@wellsfargo.com`.

That's a clear signal that that is a valid WHOIS record. But a lot of times corporations will use privacy shields, it makes it really difficult to tell it exactly who is behind it, particularly when they start using these bad actors start emulating that brand name. So it makes it very, very hard. Next slide, please. In this situation, we can go back and look at the history of a domain name.

Now, what's interesting is we were able to go back to roughly 2011. And so this was pre GDPR. And in those situations where we can look at the actual original registrants of who those people were that registered these domain names. And we get requests all the time from people that say please take my name off of it, but it's pre GDPR. So we don't typically discard those. And so this is just a great example of being able to look at the history.

Next slide, please. And I'll go ahead and wrap it up and bring it all together right here. Next slide. Now, this is a lot to take in, you're more than welcome to take a picture of that or screenshot. But getting a grasp of DNS and involves finding the badness, exposing it, and continuous monitoring, essentially.

Next slide. And of course, being able to detect not everything that's visible, but also invisible behind that. Next slide. And this is the last slide, of course, the new PayPal app is here. I use PayPal, because that's probably the most prevalent case of badness out there. It's easy to emulate. And there's a lot of scammers that use that and abuse DNS for that purpose. But if you wanted to try reverse WHOIS yourself, you're more than welcome to sign up for our website. It's free to use. And you can explore if you have any questions, let me know.

MASON COLE: Thank you very much, Ed. Appreciate the presentation. Before we get to questions for you, I'll just open with one question, which is, based on your observation, what do you see in terms of trend lines for DNS abuse? Do you find them increasing, decreasing, or definitely staying the same? Getting more sophisticated?

ED GIBBS: Definitely increasing and getting a lot more sophisticated. Like I said, being able to really not rely on root domain names anymore, but sub domain names, and hide records within sub domain records, everything from MX, text records, info records, which are all different types of DNS records that have various purposes. But not at the root level anymore. So if you if you did a search at the root level for DNS, record types and things, you're not going to find it. So you have to do what's called flattening and being able to look at the entire DNS records themselves and expose everything that you can't see initially and find out the badness there.

MASON COLE: Is your new involvement in ICANN, Mark, I see your hand on, standby one. Is your involvement in ICANN predicated, at least partly on the idea that you're here to help eradicate DNS abuse?

ED GIBBS: We'd love to.

MASON COLE: That's good to hear. Because that's a pet issue for the BC. We've been active on that issue now for several years. So that's good. Mark, go ahead, please.

MARK DATYSGELD: Thank you. This is Mark Datysgeld, GNSO counselor for the BC. You mentioned a term specifically, bulk registrations. And we are just coming out of conversation with the contractor parties about exactly that. So to give some background, the GNSO council sent letters to the contracted parties asking whether they feel bulk registration is a path for abuse in the DNS. And their general answer seems to be no, that's a thing from back when Configure was active.

So when I see you mentioning that we like some clarification because now we're set to enter them to the statements. So could you give us some idea of your feeling from this research of what bulk registrations mean at this point, and if there are strong patterns or weak patterns associated with that particular practice?

ED GIBBS: Bulk registrations are useful. And they serve a purpose. But they can be abused significantly as we've seen in our research, the majority of times it's used for abuse with no good intention other than, like I said, it could be anything from clickbait or just a whole a park domain, all the way to a C2 campaign. And it's just made it easy.

Essentially, when we do our analysis, one research we did was how long does it take for a domain name to go from the point it goes active to the point that it becomes live? Or there's a DNS record change. And what we found is a year ago, two years ago, maybe it was taking 10 days, 15 days to where they would start trying to use some of those bulk registrations to where it goes down to three days.

And today, in some of those cases, they're waiting longer because they know that a lot of the security intelligence software out there will look at the creation date and go, "Well, I'm not going to let you go to that. This is fake." It was just created. So they'll hold on to a domain name for six months, a year. And then your creation date signal starts to fail. And so you have to base it on other criterias. So, it's a tricky subject.

Because bulk registration, like I said, it's really useful. It can be abused and it is being abused. And some of the registrants, I got to be careful how I word this, when they know what exactly is going on because they have those records first and foremost. They're able to do the distance algorithm learning, look for keywords and things, and then they can block a lot of it even before it happens. But there's other reasons and motivations behind why they don't. And so, I'm not sure exactly where the bulk registration is going. If it's going to be a continued process, can it be enhanced, can be used creatively and positively instead of the way it's being used today?

MARK DATYSGELD:

Excellent.

MASON COLE: Thank you. Go ahead. Thanks for the question, Mark. Crystal, go ahead.

CRYSTAL ONDO: Thanks, Crystal Ondo Google. I just want to say thank you. I was a little late. Sorry, I was sitting in IPC, totally lost. I thought I was in the BC meeting and then awkwardly had to remove myself from that meeting. So, apologies for missing it. I think data like this is wonderful. I think specifically to Mark's point, when you're talking about bulk registrations, you said more than one, and then you kind of paused and did a little smile. I think the contracted parties are like but what does the bulk registration mean. Is it more than one? Is it more than 10? Is it more than 100? And I think that's a really important distinction.

So, the more data that the BC finds and the more work it does to get narrower on a definition, is it one customer and one registration flow. So, Google domains doesn't allow you to register 2000 domains with two clicks of a button. So, we would consider that action bulk registration as opposed to adding one or two or three to your cart.

And then also the other thing to consider when you're talking about bulk registration as the BC prepares to also input for the GNSO discussion is Google domains is the backend for cloud domains. Bulk registration via a cloud domain product is a much different process than our retail registrar. AWS is the same way. So, when you're talking about bulk registration for cloud computing, it's a possible abuse vector, yes, but it's also a very useful tool for folks that are using it.

So, you have to balance out those two aspects. And I think when you're asking contracted parties for data, the more clarity on what is being

asked would be more helpful because right now us defining it, because I sit in the registrar and registry stakeholder groups, is almost impossible without more data or more guidance around what exactly is being asked. So I think this is great work, definitely worth thinking about and helping the discussion for the VC.

MASON COLE: Thank you, Crystal. Any other questions for Ed or Ching? Oh, I'm sorry, Marie.

MARIE PATTULLO: It's Marie. Thank you very much. We see a lot of the same trend. Could you go back to the slide with the list of the domain names, the bulk one?

ED GIBBS: Oh, sure.

MARIE PATTULLO: Because...

ED GIBBS: The screenshots I gave?

MARIE PATTULLO: Yeah. Where it was various numbers from the same domain name. I think it was...

ED GIBBS: I keep going.

MARIE PATTULLO: There. That black. So we see that scenario a lot in abusing our brands. And when I think about bulk registrations, because I agree, there's lots of legitimate reasons to have a bulk registration, and we wouldn't want to have a policy or commitment that prevents the legitimate uses. It's when it's linked to abuse. So imagine that string where it's Facebook Security Center, one down to say, a 1000 names. And when you get to the point where you've done a takedown notice on the number one domain name, and you have the proof that it was used for phishing or fraud. That's when I think it shifts like the obligation related to bulk registrations should shift.

Because if you know that that customer has already been proven to have had DNS abuse, and you see the same trend, same pattern in the list that's where I think that there's a room for having a policy that could address DNS abuse at scale, because the problem with the current discussions are it's basically a whack a mole situation, you have to wait till it goes live, have the proof, take it down, you've got the three days or however long it depending upon the action of the person who gets a receipt, it might take hours, days, weeks, maybe doesn't go down at all. And it's an endless cycle.

But if there's a way to get to the bulk registration policy in a way that that protects the legitimate uses of bulk registrations, because there's absolutely, Crystal's correct about that. But also pick when there's

already in addition of abuse, you already have proof and you see a pattern like this as an example. That's where I think there's room for improvements in what we're thinking about as DNS abuse and what can be done. So I just wanted to share that for the BC because this is a very real example.

ED GIBBS:

The problem I had with answering what constitutes a bulk registration? Is it two, three, 10, 20? That's a good question. What if you miss something? It's a gray area. It's not an answer that can be concrete and say well, we're going to make it 10. But what if somebody does five and launches a major campaign with it? And you missed it? Because you ran it through a bulk registration engine, you're looking for bulk registrations and your thresholds 10. You missed it. It's gone. So from a security perspective, you lost those signals. So it's very hard, hard to quantify exactly what that number should be.

MASON COLE:

Thanks for the question, Margie. I think we're going to cut the questions right there because we're behind on time. But Ed and Ching would you mind making this presentation available to the BC? Would that be doable? That'd be great. Feel free to send it over to me and I'll share it. Thank you both very much for the presentation and answering questions. Let's move on to item three. Steve, the floor is yours.

STEVE DELBIANCO: Thanks Mason. Steve DelBianco, your policy coordinator in the BC. We'll quickly go through the policy calendar in this open meeting. We have one public comment open right now. It's not due till the 18th of April. So there's plenty of time, but it has to do with potential amendments to ICANN's bylaws associated with how did they do the review for how good of a job IANA is doing. And IANA is now part of ICANN. How good of a job do they do in fulfilling for their customers? And the primary customer of interest would be those of you that have TLDs, top level domains. You would want to know for sure that they're doing that job well. There's also the numbers allocation function.

So we have supported minor amendments in the past. We commented on the very first review three years ago, but now it's the time to see whether we want to look at these amendments and decide whether they're appropriate for us. Google, Amazon, for instance, are running multiple TLDs. And I would ask Crystal, Rajiv, if you take a look at this and see whether it serves the customers of the BC who decide to pursue, say, a .brand or decide to light up a lot of their own TLDs. So it's not due for quite a while. If you can take a look at that. Is there anybody else? Because Crystal is nodding, yes. Is there anyone else who would want to assist with that?

CRYSTAL ONDO: I'm going to volunteer Jordyn, but he's not here. But he's probably the best one to comment on this.

STEVE DELBIANCO: Jordyn Buchanan?

CRYSTAL ONDO: Yeah.

STEVE DELBIANCO: Please do. I'll write to him again like I did on the last one. And thank you and Rajiv for commenting on the previous. Anyone else? Plenty of time on this. Thank you. The other is the NIST2, which we put in every time. And it doesn't have a public comment for ICANN, but it's a publicly visible and important initiative for the BC. We've been very active at trying to nudge and monitor the European Union, the European Commission's work on this. And just last December, the final text came out.

We are now in the throes of European member states transposing the NIST2 directive into their own regulation and law. We had suspected a few countries would move early because they already require significant disclosures with respect to their ccTLD community. And I have learned from Caroline. And Caroline, I'll let you tell everybody just verbally what you've found. Go ahead.

CAROLINE: Thanks all. So we found that the Czech Republic had transposed NIST2 into law. It was the Czech cyber agency that did so. Currently, it has a webpage, which is sort of its landing page for everything NIST2 related. They discuss, it is in Czech, but from a browser anyway, you could translate that into English or your language of choice. They discuss sort of what NIST2 is and what they'll be doing. And then on that page, they

do have a PDF published again in Czech of their transposition of the NIST2 law that will take significantly more time to translate to English.

STEVE DELBIANCO: Thanks Caroline. Keep in mind, they're not obligated to put it in English because it's not a European document yet. It's just a draft and it's only in Czech because that's all they're obliged to. Marie.

MARIE PATTULLO: First Caroline, thank you for finding this your start. Can I just check when you say transposed into law, you're saying it's actually Czech law?

CAROLINE: No...

STEVE DELBIANCO: Let's say it's a proposal.

CAROLINE: It was just proposed, drafted by the Czech cyber agency.

MARIE PATTULLO: Had me a wee bit worried there, but thank you. Thanks.

STEVE DELBIANCO: Necessarily the domains element of NIST2. NIST2 is a very long document and that's why it's very difficult to run a translate and figure

out where in there they're talking about domains. We're looking for an English language version. Please help out those of you with contacts in Europe. Thank you. So that's just a heads up and Caroline, thank you for monitoring the session, doing some digging and circulating that. Channel 2 is council, GNSO council. We have already covered the previous council meeting. So let me just move up to the council meeting that's happening this week while you're in Cancun. And here I put five or six items from the agenda, hoping that Mark and Marie will lead us through.

MARK DATYSGELD:

We've had an interesting meeting so far. We had our first open microphone yesterday, as far as I know, at least in recent history, and it was dominated by the SOI question, which is not even in the council agenda yet. So apparently there's a lot of interest in that question coming from multiple actors. So that's one thing to take into consideration. The council is always looking, also has received now most of the -- not most, has received back all the letters from DNS abuse from the parties that we requested answers for.

And this is interesting because it will allow us to bring this back to the table. And as far as I'm concerned or what I have been noted, the small team on DNS abuse will probably be reactivated. We'll get another shot at doing some work because now we will go through the letters. We'll try to set a position from that and start establishing what exactly will be the next steps from the council. As far as we are concerned.

STEVE DELBIANCO: The agenda for Wednesday, walk us through what on the agenda you want your colleagues to comment on or follow.

MARK DATYSGELD: The agenda is a little. So where is it? We're seeing it in the [inaudible - 00:39:20] policy. Marie would be better at this. I've been doing DNS abuse all week. My head is, I can think of others.

MARIE PATTULLO: Oh, bless you. The points that Steve's put up there, the first one, continuous improvements. It's all about procedure. If you want to know, tell us, but it's really procedural. Expired domains exactly. So what they are. The projects that might impact on SubPro. Now, as SubPro is with the board, they are going through all the recommendations. They've at the moment come up with two ways that it could be taken forward. And our dear friends in the BRG have now come up with a third way that it could be taken forward. But in the meantime, the idea is that we try to be ready when the IRT starts with the most contentious things that have actually been developed. The two main ones that were concerned to us, one is applicant support and one is closed generics.

Now the closed generics conversation started by the GAC. As we don't actually have a policy. Are they allowed? Are they not allowed? We went into this saying, it's going to be none of the above. You're not going to have no closed generics, Anna. And you're not going to have, let's have all the closed generics. It's got to be somewhere in the middle. So what's happening with this so-called facilitated dialogue is

they're trying to come to umbrella scope that everyone can actually sign up to. So we don't get torpedoed by the GAC at the last instance, at which point it will come back to council and we'll develop the policy around that. The other one, I'm not the expert, it's Lawrence, but very briefly, applicant support.

Last time around, this was left until the last minute when suddenly you went, "There might be some people who need help. Let's do something." And what we're trying to do this time is be a little bit more sensible about that. Paraphrasing something I heard from our experts on the group, Lawrence, this won't surprise you, unfortunately, but there seems to be an understanding that the people that will need support if they want to apply for a new gTLD will be not-for-profits. The end. And our colleague here suggested that maybe small businesses might actually be more appropriate.

And we're going to take that forward in some conversations this week, because being realistic, it is the likes of you guys, the smaller businesses, not looking at small business Margie, but other small businesses who are, but might still be called out Twitter, Margie. So I think we've got some education to do with that. Anyway, that's the bits that are under, if you like, council control, sort of. Then there's going to be a lot of discussion in SubPro, which will normally be trying to stop the liaison to SubPro ODA talking too much. And then we're going to go into discussing a thing that has a new name every time I look at an agenda. And with all due respect, Steve, I think you are the best person here to discuss that for the group.

STEVE DELBIANCO:

I'll do it quickly. This is what used to be known as SSAD, but SSAD Light, and now it's called the -- it was the WHOIS Disclosure System, but now it's been renamed. It's been renamed as, I'll put it in yellow down here, the Registration Data Request Service, because it is only requests. It is not a disclosure.

So we had a meeting on this Saturday morning and it was with staff who's been tasked by the board to develop it before the end of this year. And they keep asking us to specify what reports we'd like to see as if that is what's going to dictate what data they capture and make available. We have insisted all along that they should capture all the data that's entered by the person doing the request. They should capture the transmission of that data to the registrar and they should capture data that the registrars give us on whether they responded.

Now that includes, for instance, the images that you provided, the screenshots that you provided as a requester, which were publicly available screens showing evidence of why you needed to get, you had a legitimate reason to get a disclosure or a name. So I got no answers at all. The IT staff looked at me and said, "We are going to evolve the data model as we go." And they said, the most important thing here is to try to get, solve the board's intent of discovering whether there's adequate usage to justify a new system.

And I did a drill down on what the word usage would mean, because they are focusing it as if it's the quantity of requests that come in. And it isn't, I tried to suggest, and it's in the writing of the small team report, that it's also the quality of the requests, which include who it came from, what was the reason, what was the urgency of it, what was the

nature of the attack that somebody was trying to respond to, who was the domain name, and also importantly, who was the registrar and did they respond at all?

So staff is not really getting it. We're going to meet every four weeks with the small team, and I'll just continue to be a burr under the saddle to try to get something useful out of this. We have a lot of time to work on it because it won't be ready till December, but between now and December, we'll have to figure out if we want to use the system to make a point. We don't think we'll use it to get a lot of information, but if we use it to make a point that registrars are ignoring or denying disclosure when we provide all the necessary information. Anything else for council? Crystal?

CRYSTAL ONDO:

I'll just plus one, Steve. I thought what you said in that meeting was perfectly on point and having gone through with ICANN IT staff when they designed NSP, they really failed to take into account what information, how the use was going to be handled, what reporting would be handled, and it was much harder once they built it to request changes.

I think getting in front of them and having it not just come from registrars who will be using it, but also those who will be sending requests, and obviously the community wants data out of it before they build it, keep hammering on them, please, for this because otherwise it's going to get off the ground and it won't be what anyone -- I mean, we all agree this isn't what we all wanted to begin with, but then it won't

even meet that very low bar. You have full support from, I think, a lot of people to keep hammering on their IT group.

STEVE DELBIANCO:

That's good because I really angered the staff, I'm pretty sure, but I'll keep it up because it's a theme. It's a theme with the DNS abuse discussions is that the folks who show up here at these meetings are rarely the bad actors we're worried about. Bad actor registrars don't even belong to the registrar stakeholder group. Only about 24 registrars belong to the Registrar Stakeholder Group, and there are thousands.

Isolating a bad actor would be what I wouldn't want to use this data on. I would want to show that this data indicates that legitimate requests came in and were ignored. If we can't get that data out of it, why would we use it at all? We've covered a little bit on closed generics. That's a currently active policy. Zach, why don't you tell us where you and Arinola are on transfer policy?

ZACH MUSCOVITCH:

Sure. For those of you who want to take a short break from domain name abuse, we can talk about transfer policy briefly, but Arinola and I have been representing the BC in the transfer policy for about a year now. A couple of interesting discussions occurred recently, the discussion of the thing called a TIAC. You learn a new acronym once in a while, but for those of you representing businesses, this is an interesting thing you may not have heard of.

There's a provision in the transfer policy that creates a hotline for businesses that have lost their domain name overnight in the last few hours. There's been a discussion of that. There's been a discussion of the transfer policy, which is the registrar-initiated dispute between a gaining registrar and the losing registrar when one of the parties says there was an unauthorized transfer. But in terms of procedure, we've been asked by the working group to prepare some early feedback. And so the deadline for that is right after ICANN. I think it's April 4th or so. We're going to prepare that and I'll ask you for your feedback once I prepare a draft after ICANN. Thank you.

STEVE DELBIANCO:

Thank you, Zach. Appreciate that. Let me turn to Lawrence on the GNSO guidance process for a quick update. He just came out of a meeting.

LAWRENCE ROBERTS:

So about an hour ago, we had a GGP meeting that basically have been reviewing a document put together by leadership, my CBA and staff. Took the opportunity of this meeting again to reiterate that from the commercial stakeholder group, when it comes to the process of outreach and awareness, we expect that because the document specifically states that outreach and awareness will be targeted at the not-for-profit civil society group.

So, took this opportunity again to reiterate that we expect awareness to be broad based, not just focus on a specific group and where the applications come in, ICANN, through whatever process, can then

decide to use its own methodology to select. There was a lot of pushback by the chair, saying that even to the point that it appears I didn't understand the process that we're talking about because they don't expect commercial entities to be interested in securing applicant support from ICANN.

I feel this particular position represents to a large extent the mindset of leadership. I particularly asked if there is anything in the ICANN rule that kind of supports this thinking, and we were told that there is none. But yet, that language was not removed, and there was very, very strong pushback from the chair of the committee.

So I think we as the CSG might need to be more vocal about this particular aspect because even for commercial entities, his thinking is like, would you expect a Twitter or call to come for applicant support? But I've said irrevocably that even in my region, for a commercial entity requiring some form of TLD in the next round, we might definitely want to require some kind of support, and I'm hoping that we are able to push back and make some progress in that regard.

STEVE DELBIANCO:

Thank you, Lawrence. One more item up. We already heard from Mark with respect to DNS abuse and the work he did on the small team. I'm going to turn to Mason to talk about response on the contract negotiation.

MASON COLE:

Thanks, Steve. The BC, the IPC, and the ALAC sent in late January a letter to ICANN org specifically to Sally Costerton and Tripti about the approaching changes to the RA and the RAA and outlining to them what the precedent was in the 2013 changes in terms of procedure, that there was community consultation prior, there were several updates along the way, there was even a wiki created to keep the community updated, and we asked whether or not the ICANN org intended to follow that precedent or not, and if so, what the timeline was, what the community could expect in terms of the opportunity to contribute.

Our letter was not answered, so today in the executive Q&A session, I asked the executives on the panel what we should expect, and the bad news is, org seems pretty set on providing one comment period about the changes to the contract and that's it.

STEVE DELBIANCO:

At the end?

MASON COLE:

Yeah, once the negotiations are completed. There are negotiations ongoing right now. They're expected to conclude before ICANN 77 in June in Washington DC. And we'll be handed a set of contract amendments that we'll comment on, and that'll be the limit of our input. Now, that's not to say that we're ready to give up on trying to influence the process, but that's the situation that we have right now. So I wish I had better news, but that's what we've got.

STEVE DELBIANCO: Thank you, Mason. The contract parties did respond to letters that were sent to them, but in the meeting today on outreach on DNS abuse, our letter wasn't written to them, so they didn't respond to it at all. Let me turn now to Tim, our liaison for the commercial stakeholders group. Tim.

TIM SMITH: Thanks Steve. Not too much to report. Here we are in the middle of our ICANN meeting, and I know we've been working on board seat 14 and finding suitable candidate or candidates between NCSG and CSG. We still haven't arrived at anything yet, but are working on it. And it does seem to be moving forward bit by bit. So hopefully we'll have something to report, well, hopefully during this week, but if not in the weeks to come.

But I think it also, one of the other things we talked about before the meeting was having more regular interaction with NCSG. And I think that's probably a worthwhile thing to do. And so something we'll continue to pursue and continue to understand each other's priorities, I think. So that's very much in progress as well. Other than that, we have two meetings for CSG tomorrow. Of course is the CSG and the ICANN board meeting. So everybody's invited to attend that. And we already got through the DNS abuse outreach a little while ago. And so the CSG membership meeting is also tomorrow. And that's really it for me. Thank you.

STEVE DELBIANCO: Thank you, Tim. Mason, I'll turn it back over to you for the rest of the agenda.

MASON COLE: Thank you, Steve. Lawrence, I'm sorry. Well, actually, Lawrence wants to know how much time we have left. Brenda, do we have any latitude to go over at all or not really? So let's keep it tight. I'm sorry, Lawrence. You always seem to get shortchange. But I know we want to cover a couple things under ALB too. So go ahead.

LAWRENCE ROBERTS: So I've sent members our recent newsletter for ICANN67. Big thanks to everyone that helped to contribute an article towards this edition. Please kindly take time to review the content. And I'm sure you'll find it quite engaging. Aside from the newsletter that we have, and thanks to our new members, WHOIS XML, for joining us today. We also have another new member at the back. We are welcoming everyone whose first time it is to the BC meeting. For members, we're going to be sending out some information with regards to a forthcoming election for one council seat. This is going to be Marie's seat. And we also appoint new people into NomCom, the NomCom small and large seats.

I used to wonder why we start this process so early. They're not going to be taking their seats until ICANN78, the AGM. But we have a four-month timeline with which we have to provide the candidates' seats to ICANN. So we definitely have to start and complete this process by May in the list. So there's a timeline that we're working with. We're going to share it on the BC private list. And I want to use the opportunity to thank

Marie for such a wonderful representation. We'll have lots for her to continue, if not for ICANN not allowing a particular term, I mean bringing about a term limit. So thank you for -- she still remains our councilor until after the AGM, ICANN78.

Another thing I want to bring to the notice of members is that the next ICANN meeting in DC, we're planning towards having an outreach event for North America. We have three slots available to bring members into the DC meeting. Such members will have to be members from North America. One of the slots have already been allocated to Caroline. Thank you for that. We now have two slots left for members or would-be members who can also help with the outreach event from within America and Canada. Those two areas are covered.

So please, we would want to fully utilize our slots. These slots are going to expire with FY23. So that means we can only use them for the next BC meeting. So we really would look forward to having members help us with two persons. They could be old BC members that we want to re-engage their interest, or they could be maybe willing BC or potential BC members that we can walk through the process of joining the BC. I'll give the floor back to Mason. Thank you.

MASON COLE:

Lawrence, that was a land speed record. That was great. Thank you. Excellent. Let's move to all other business. I know that Steve has something to raise. Is there any other business that before we go to Steve that anyone would like to raise for the BC? Back to you, Steve.

STEVE DELBIANCO:

Thank you, Mason. And this is a topic that has been, I think, brewing for a while. It was a proposal to amend the statements of interest that are displayed at ICANN. I can share, for instance, what my screen looks like on my statement of interest, give you an idea of what we're talking about. How do I get rid of that piece of -- So statement of interest looks like this. And virtually anyone who wants to be in a working group has to fill one out.

So you see you declare who you work for, identify my employer, my role there, the type of the work we do. And there, for instance, as a trade association similar to Marie and Barbara, I'd indicate in there that I represent NetChoice and that we have no financial interest in the members themselves, registries or registrars, but I have members.

And I went ahead and disclosed NetChoice members could include companies that run registries, Amazon, Google, VeriSign. And in terms of who else I might care about, I let that I'm a trade association of online businesses. And all of my members are listed right there at netchoice.org. Same is true of Marie and Barbara.

But for other representatives who might be, let's say a lawyer or a consultant who's representing the interests of their clients, a slightly different path arises. This is the good-looking Mason Cole. And under his, he uses the wholly appropriate designation of the word private with respect to the entities that he represents. And as working with a law firm and those of your attorneys could indicate what motivates your desire not to disclose the names of the clients that you and your firm represent.

But what is cooking right now is that the SOI discussion here at ICANN is about whether to change it, to change it so that more has to be provided. If you were to say, I don't want to disclose the names of all of my firm's clients, might have to disclose the reasons, might have to disclose, say to the chair of the working group exactly who your clients are so that the working group chair might be able to say there's over-representation or over-weighting by one company or industry by virtue of a representative who covers many. So I don't really know what itch this was intended to scratch.

We do have a representative on the working group, Imran Hossain, but Imran's not been present or communicative about what's been happening there. We will attend a meeting Wednesday to hear staff talk about what they're considering in terms of the amendments. But I thought we could discuss it now to understand whether the BC has a consensus position or more importantly, what are the concerns you have? I'll take notes and convey them to the meeting that I attend on Wednesday. Anyone, I'll open the queue. Crystal, go ahead.

CRYSTAL:

Thanks, Mason. And thanks, Steve, for raising it. I brought it to Steve and Mason's attention a few days ago because this is getting a lot of play. I know it was brought up in the GNSO as well. It was brought up in front of the GAC. I can't tell if there is a miscommunication between what's happening and the positions that people are taking, or if there's just a misunderstanding of what is actually going to result in this form that you're showing. So for Mason, yes, I agree. This is 100% right that this should be private. This is not a working group. But if Mason joined

the transfer PDP, which is a lot of fun for all of us, and he was representing specifically one person on that PDP, then that should have to be disclosed.

And I think that's where the rest of the community is a little concerned with the exception to that. Are we making a bigger exception that's already available. If you can stay private and that counts, then what more exception is needed? That's, I think, where the confusion is because the language as drafted that we see that is being supported by the IPC, the rumor mill is also the BC supports it. And I think that's one of the things that I was confused about because I hadn't seen a lot of chatter on the BC list about this. So I just want to make sure that we are aligned with the IPC or we're not, or at least the members here have an understanding of what is being asked. So thank you for raising it because I also wasn't clear to me what the BC's position was on this.

STEVE DELBIANCO: I was going to indicate the BC doesn't have a position.

CRYSTAL: But everyone thinks we...

STEVE DELBIANCO: Everyone did not ask what to represent. And from my standpoint, staff's not indicated that everyone has ever said what he thinks the BC position is. So we're here to discuss it. I don't expect we'll finish it. We only have a dozen people here. We're out of time, but let's hear your concerns. Anyone else?

MARIE PATTULLO: And again, I've been hearing the rumor mill too. So I don't know what the proposal actually says, but if the -- I mean, I can't -- it's hard to me to, I'm sorry. But if it requires an attorney to disclose its client, I think that's a problem because of the ethical obligations that apply to attorneys. There's a state bar opinion specifically on that that even disclosing the identity of your customer, it creates a legal ethics dilemma.

And I don't know if that's factored in there or not, but I would think that's not a good idea to have attorneys be in a position where they have to violate the ethical rules in order to participate. And we certainly don't want to make it more difficult for attorneys to participate in the ICANN processes. So that's something that I think we should flag.

MASON COLE: Thank you, Marie. Not Barbara, sorry, Marie.

MARIE PATTULLO: One of the questions we've been asking, is this an actual problem or is it, let's fight another bogeyman that doesn't exist? Because the discussion seems to be going the idea that you're in the room as Google. Mark is in the room as lawyer Mark, who happens to be working for Google and so on down the line and maybe you do have 86 members of Google who wrap up and take over every PDB, I don't know. But what I would like to try to figure out, Steve, is if you go to this meeting, is this actually a problem or is it, as I say, they're tilting at Wilmans? Because

I'm concerned on a wider level that Mark and I, as have a little personal battle that we're fighting at the moment.

With all due respect to you, [inaudible - 01:04:07], you are not the BC. And this is what we keep shouting from the rooftops that we have the lights, Mark. We've got Vivek, we've got people from all over the world. We're not just big corporate white America, if I can put it that way. And my concern is it's actually part of that. It seems to be bubbling more. I don't know, Mark, what you think, but that's just a little thing that I'm worried about.

MASON COLE: Is this the creature of counsel? Is this process of SOI revision something coming out of counsel? Does anyone know?

UNKNOWN SPEAKER: That's the problem. It rose from counsel. It rose from the CCOICI, if I get it right. But now I don't think it's our problem anymore because we're not supposed to discuss substance. So in theory, I don't think it's our problem. And I don't know how it would rise to the counsel level. That's where I lost the plot. So I don't even think it should be raised in that sphere, but I don't know what's the idea there.

MASON COLE: Brenda's going to kill me if we don't wrap this meeting up, but I wanted to raise one other issue, and that is on the issue of the exemption, where if I understand it right, and Crystal, you can slap me around if I've got it wrong, but my understanding is if you request an exemption, you may

be asked to disclose your representation, information to the leader of the working group or to ICANN staff. I have a problem with that personally because I don't think ICANN or anyone at ICANN should be in the business of adjudicating who can and can't participate in ICANN. So, and particularly, and speaking frankly, often ICANN is kind of a sieve of information leakage, and that presents a lot of difficulty.

You can't necessarily trust the process going forward if you're asked to disclose a client relationship and trust that that information is going to be held private or won't be held against you. So, I'm afraid we have to cut the discussion here. My suggestion is that we continue this discussion online to make sure that we are or aren't aligned with anyone in the IPC. We can step outside the room and continue it for those of you who are interested in talking about it, but for now, I think that's it, unless there's anything else that's really pressing to raise. BC is adjourned. Thanks, everyone.

[END OF TRANSCRIPTION]