ICANN78 | AGM – GNSO BC Membership Session
Tuesday, October 24, 2023 – 2:00 to 4:00 HAM

STEVE CHAN: Hello and welcome to the BC membership session. Please note that this session is being recorded and is governed by the ICANN expected standards of behavior.

During the session, questions or comments submitted in chat will only be read aloud if put in the proper form as noted in the chat.. Questions and comments will read aloud during the set time set by the chair or moderator of this session. If you would like to ask your question or make your 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.

To view the real-time transcription, click on the Closed Caption button in the Zoom toolbar to ensure transparency of participation in ICANN's multistakeholder model, we ask that you sign into the Zoom session 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.

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 very much, Steve. Welcome everyone, to the BC meeting here in Hamburg, and it's good to see so many faces here in the meeting. We have this huge echoey chamber here.

[STEVE CHAN]: [inaudible] echoey, echoey.

MASON COLE: Yeah. Actually, for a change, we have two hours for our BC meeting today. So we've got some latitude on our agenda to handle more subject matter than we usually do. So we have until, I believe, 4:00 today. So we've got some time to have a good discussion.

You see the agenda on the screen ahead of you. Are there any additions or updates to the agenda as you see it? I understand there could be a couple of AOB issues if we have time.

[STEVE CHAN]: [inaudible]

MASON COLE: Okay. All right, first, since we haven't been together for some time and we have a pretty good sized crowd in here, and we also have some new members, can we quickly go around the table and just introduce ourselves, have a little roll call? Let's start with Marie, please.

MARI PATTULLO: Hello. I am Marie Pattullo. I am with AIM, the European brands association based in Brussels.

NIVALDO CLETO: I'm Nivaldo Cleto. I represent [inaudible] PKI in Sao Paulo, Brazil, and am a member of CGI, the Brazilian internet steering committee.

PAULO MILLIET ROQUE: I’m Paulo Milliet Roque. I am the president of the Brazilian software association, ABES, that represents 2000 companies in Brazil.

RAJIV PRASAD: Rajiv Prasad, Google LLC.

VIVEK GOYAL: Vivi Guil, founder of LdotR, and I also represent the BC on the NomCom on the small business seat. Thank you.

DAVID SNEAD: I'm David Snead with WebPros.

ZAK MUSCOVITCH: I'm Zak Muscovitch, general counsel with the Internet Commerce Association.

MARGIE MILAM: I'm Margie Milam with Meta Platforms Inc. And I'm based in California.

MASON COLE: Mason Cole with the law firm of Perkins Coie in the US. And I'm chair of the BC.

STEVE DELBIANCO: Steve DelBianco with NetChoice Trade Association for the tech industry based in the US. And I'm the vice-chair for policy coordination here in the BC.

TIM SMITH: Hi. Tim Smith with the Canadian International Pharmacy Association. And I represent the Business Constituency as a liaison to the CSG Commercial Stakeholders Group).

ABBY BOWMAN: Hi, I'm Abby Bowman. I'm with AT&T, part of the BC. And I'm based in Washington, D. C.

MARK DAYSGELD: Mark Datysgeld with Governance Primer. We consult for small and medium-sized organizations on Internet governance matters. I'm also currently serving the GNSO Council as one of the reps of the BC.

MARK WILSON: Hi, everyone. I'm Mark Wilson from AXA SA, member of the BC in my first in-person meeting.

SVEN ECHTERNACH: I'm Sven Echternach of EWBCD in Frankfurt, Germany, and we're a member in the BC as of two weeks.

EMILY TAYLOR: Emily Taylor, DNS Research Federation. I'm a guest today,

[STEVE DELBIANCO]: Guest today, member tomorrow.

EMILY TAYLOR: How they start.

NATHAN ALAN: Nathan Alan, DNS Research Federation as well. Also guest speaker

FAISAL SHAH: Faisal Shah with Tracer, based in the US.

CHING CHIAO: Ching Chiao, WHOIS API. I'm a senior advisor to a company based in Los Angeles, and I'm based in Boston.

CHRIS CHAPLOW: Hello. Chris Chaplow from Andalucia.com, actually a BC member since 2009, although this is first meeting for a while.

MICHELLE CHAPLOW: Hello, everyone. Michelle Chaplow from Andlucia.com, based in Spain.

MASON COLE: All right, thanks, everybody. Chris, it's good to have you back. Long time no see.

All right, ladies and gentlemen, we have a couple of other things to cover today. One is there were some recent officer elections. You'll see some familiar faces in current offices, but we've had some rotation in and out of other offices. Our friend Marie is departing the council after a few years of excellent service. Let's have a hand for Marie. Thank you. Marie will be our new liaison to the CSG, replacing Tim Smith. And Tim Smith is now assuming the role of vice-chair for finance and operations after serving as CSG liaison. And Lawrence Olawale Roberts is leaving that post to take Marie's seat on the GNSO Council. So we had some musical chairs, and we're very fortunate to have everybody staying on XCOM, even if some are in different roles. So thank you all again for all your service.

Okay, I think we're ready. We did have on the agenda a brief discussion with Chris Buckridge, who is the new member of the Board in Board Seat 14, representing the CSG and the NCSG. It doesn't look like Chris has been able to make it to the call or the meeting today, so we're going to move on with the agenda.

So let's go to item number three, and that is a presentation from Margie Milam about adversarial threat reports that Meta has just recently published. And this is of interest to the BC due to our ongoing interest in the issue of DNS abuse. So, Margie, over to you.

MARGIE MILAM: Hello, everyone. I'm Margie Milam with Meta platforms. I wanted to talk you through our Meta Q2 adversarial threat report that we published earlier in the year.

Next slide, please. I'll be talking about our overall approach to mitigating DNS abuse and introduce you to a specific type of abuse known as coordinated inauthentic behavior. It's kind of a mouthful, but it's something that we're reporting on in our adversarial threat reports.

We publish these reports on adversarial threats to share our insights into takedowns and also to lead to further investigations and removals of persistent influence operations around the internet. We think that, at Meta, sharing this information can also lead to increased focus and perhaps sanctions on some of the bad actors and increase their costs for performing these kinds of malicious attacks. And also I think it's useful for the cybersecurity community and researchers that can lead to understanding what these threats are all about, and hopefully that leads to a scaled defenses across the internet.

So what I'll be talking about is a few examples that we've highlighted. There's lots of information in the report but two threats are specifically one named Spamouflage and another one called Doppelganger. And then once I walk through some of those examples, I'll bring in the domain name application because this has some implications with domain names. And then I'll move into our work to address DNS abuse at scale. And then at the end of the report, we actually included a series of recommendations from Meta about what kinds of policy and other solutions could help tackle this abuse across communities and other stakeholders. And then if there's any time, we can have questions.

So let's move on to the next slide please. So that's the agenda.

Next slide. One of the things I want to emphasize here is that we will be talking about off-platform abuse. So this is abuse off the Meta platforms. We do though have a robust on-platform abuse procedures and we publish transparency reports that relate to those and I can provide you a link for those if you have any interest in the work that we do for on-platform abuse.

If you take a look at our transparency reports, you'll see for example, that we have approximately 40,000 people that are focused on safety and security efforts, which is four times as many as we had working on these efforts in 2016. And we've also invested more than $20 billion in our overall integrity efforts in 2016. So Meta takes this very seriously and we have a lot of information in these reports that you can see.

We took an approach at Meta to make this information available because we do think transparency is key to tackling some of these biggest challenges that we face online. Our reports have lots of information where we can share with industry, and industry can learn and improve the systems and also collectively take actions to protect the public from abuse across the Internet.

Next slide, please. So what is coordinated inauthentic behavior? This is an interesting term that maybe many of you haven't heard before. We see it as a coordinated effort to manipulate public debate for a strategic goal in which fake accounts are central to the operation. We see this on our platform, where people are coordinating with one another, using fake accounts to mislead others about who they are and what they are doing. And when we see that on our platform, we obviously take action to remove these operations, and we typically do it … We're focusing on the behavior rather than the content.

But unfortunately, even when we are able to take them down, we see a persistent nature of it. In other words, they come back, and they try to come back on our platform, even though we've previously removed them. And so while we continuously block malicious domains that engage in this kind of behavior from being shared on our platforms, we see that enforcements on each platform can only go as far as disrupting while the domain names stay alive. So if the domain names are alive, these types of attacks can continue to persist. So that's one of the points that as we think about what's going on here at ICANN and talking about approaches to DNS abuse, we have to really think about what can be done to prevent malicious domains from continuing to persist.

And one of the concerns we've highlighted in our report is that responding to coordinated inauthentic behavior requires a level of collaboration and mitigation that's across platforms, across companies. And it's really something that we just don't see that kind of cooperation in a way that really makes this kind of mitigation effective.

Next slide, please. So now I'll walk you through a couple of examples that we've highlighted in the report. And if you take a look at the report, you'll see at the end there's an appendix that's full of technical information, domain names, and the URLs that our investigators have identified.

Next slide, please. So here's an example of Spamouflage, which we've identified as the largest known cross-platform covert influence operation in the world. In this example, you can see this is fake news that is targeting journalists. And as the report points out, we've taken down thousands of accounts and pages that were part of this largest known cross-platform covert influence operation in the world. It targeted more than 50 apps, including Facebook, Instagram, X or Twitter, YouTube, TikTok, Reddit, Pinterest, Medium, Blogpost, and a dozen other smaller platforms and forums. And for the first time, we were able to tie this activity together and confirm that it was part of one organization in the security community known as Spamouflage, and we linked it to individuals associated with Chinese law enforcement.

The campaign was focused on disseminating pro-PRC propaganda, dissident harassment, and meddling with elections. So you can see this is pretty serious stuff, and it's something that, as Meta, we don't like to see this kind of thing on our platform.

Meta became aware of the influence operation after the network targeted an NGO in late 2022. And while we removed the campaign from Facebook and Instagram, many of the accounts on other platforms stayed alive. And so that's one of the points that I want to emphasize here: that this persistent nature is something that I think, as an industry, we would like to tackle.

As part of this approach, meta removed more than 7700 Facebook accounts and 954 pages linked to the campaign.

Next slide, please. So the next one I want to highlight that's in our report is something that we call Doppelganger. Funny name, but it's the largest and most aggressively persistent campaign that we disrupted in Russia since 2017. The goal of Doppelganger was to weaken the support for the Ukraine war, and we recently noticed that it expanded beyond its initial targeting of certain countries such as France, Germany, and Ukraine, and it expanded to include the United States and Israel.

Next slide, please. The operation posted links to websites that resembled real news outlets and government websites. And these websites included pro-Russian narratives. So if you look at the example … I'm sorry, let's go back one slide. Yeah, that's right here. Okay, if you take a look at this slide, you can see at the top, you've got the fake site in two different versions, and then at the bottom, you'll actually see the legitimate site for a spoofed NATO website that was at NATO.ws. This is an example of where you could see the domain name and how the domain names are used or misused to provide these types of attacks.

Okay, next slide, please. Since we're here at ICANN, we want to talk a little bit about how domain name policy can address some of these concerns. In our report, we reported that four out of five covert influence operations in the report ran websites that posed as independent news organizations. This was accomplished by deploying typo-squatted and cybersquatted domain names that mimicked independent news sites and even NGOs. And so if you look at the report, you'll see that we identified NATO.ws. Another domain name that's linked in the report is WashingtonPost.ltd, which is a classic cybersquatted domain name.

Next slide, please. So now we'll talk a little bit about our approach to addressing domain name abuse at scale. We take a very broad approach in addressing abuse at Meta and off-platform. We deploy a number of approaches to try to bring down the level of abuse that we see. For example, we team up with anti-phishing and brand protection vendors to detect abuse. We then either address or remove the harmful domains and URLs on our platform. As part of this, we typically make a WHOIS request to investigate and identify bad actors that target our users. And then if that's not successful, then we will mitigate the off-platform abuse through takedown requests, DNS abuse requests, as many of you are familiar with, UDRPS. Or if that doesn't work at times, will also take legal action. The other thing we do to try to combat abuse is to establish trusted notifier relationships to enable very swift action when we need to respond to this type and other types of DNS abuse.

Next slide, please. So our report talks a little bit about the challenges that we see in mitigating coordinated inauthentic behavior attacks. Some of this, I think, will be very familiar to the brands in the room and the brand protection companies that are also in the fight for these types of issues. As you can imagine, the unavailability of domain registrant information is a challenge. And then even if it is available, oftentimes there's a privacy proxy associated with it or the information is inaccurate. So we see a hurdle there, and we're constantly dealing with the WHOIS issues as we try to mitigate these types of attacks.

When we take legal action, UDRPs are very expensive and slow. I mean, for those of you who are familiar with the UDRP, it'll take three months to get resolved, and that's simply too long to be able to deal with this type of abuse. Legal action is also an option we've taken, but even that is too slow, too expensive, and just unable to address the scale of abuse that we see.

As we think about DNS abuse and the contract amendments that have been recently approved, obviously, we're very appreciative of the industry and ICANN for having RAA amendment negotiations, but the types of recommendations that will be in the new agreement as it gets approved don't address this kind of abuse. The definition of DNS abuse is narrowly focused to phishing and malware. So this type of coordinated inauthentic behavior likely would not be viewed as DNS abuse for the purposes of the RAA.

So that's one of the reasons why we're looking for more innovative and faster solutions for this. And that's why you hear me and others talk about understanding what the next steps are as it relates to the RAA amendments and DNS abuse because ultimately, there needs to be some solutions that deal with the scale issue that we're seeing here.

Next slide, please. So, just to talk about scale at Meta (and obviously we're a very large company), we have a tremendous number of abuse that we're trying to combat at any given point. For example, at the time this report was written (so this was Q2 numbers), we'd reported and removed over 6000 abusive domain names that targeted the Meta brands. That's a lot of abuse. And there's no way that UDRPs can be filed for 6000 abusive domain names. With regard to phishing attacks, we mitigated over 140,000 phishing sites in 2022, and that was actually a decrease from the prior year where it was 265,000.

So when we talk about DNS abuse and takedown requests, you just simply can't submit 265,000 takedown requests to registrars. I mean, the scale issue is astronomical, and it's one of the reasons why we're sharing this information with the ICANN community so you can get the flavor of what a major platform or major company deals with.

I'm sure Marie's clients at her association probably, or Faisal's, probably see similar things, maybe not at the same scale as Meta, but certainly the volume is something I think a number of brands would echo.

We see a number of challenges in mitigating domain name abuse, as I mentioned. Our WHOIS reveals are only successful about 35% of the time, as reported by Tracer AI, who helps us with submitting these. So even though we're Meta and people know who we are, and the domain names typically have our brands in them, roughly one in three will be successful. So we're dealing with a lot of uncertainty because we don't even know who the registrant is for these domain names. UDRPS are costly, thousands of dollars. As I mentioned, they just can't keep up with the scale. And then again, litigation is something that we have pursued to protect people from abuse. But again, the cost and the timing is something that really can't address this type of abuse at scale.

Next slide, please. And I think I just wanted to drive home the point that our experience is not unique. This is something that companies across the world are dealing with. A lot of them don't have the kind of resources that we have to be able to do this. So the persistent nature of this kind of abuse continues to persist.

If you look at the examples that we've posted in the report, you'll see that NGOs and nonprofits and government agencies were targets of some of the abusive domain names that were misused for the fake news. They are probably less able to file some of the UDRPS and take the kind of action that's needed to ensure that those types of attacks don't persist.

Next slide, please. So as we think about [the CIB], we've come up with some recommendations about how to really mitigate this, because we think this is something that the larger Internet community would agree is something that's useful to try to tackle. We do believe that transparency and cross-society responses are key to tackling these malicious efforts to manipulate the public debate. We recognize that tech platforms and researchers and media and government entities, even registrars and registries, all have a very unique and limited view into the individual elements of these campaigns. But collectively, there's not a lot of information sharing about them.

So we would like to see solutions to be explored at ICANN for better, obviously, domain name policies and contracts to touch on the scale issue. But we also see that solutions outside of ICANN may be needed because there are gaps in coverage for policies or the regulatory frameworks. So, for example, we all know that ICANN's remit is narrow and doesn't cover hosting providers as a [inaudible] if a solution is to be found to this problem, it's a multilayered, one that includes ICANN and activity outside of ICANN.

Next slide please. So, as I mentioned, we've made some recommendations, and we hope that these recommendations can help focus the discussions in the right areas to lead to timely solutions to these society-wide problems.

And if you flip to the next slide you can see the types of things that we think could be approached from the ICANN perspective and things that may need approach outside of the ICANN framework; so, for example, improving contracts with registries and registrars to take proactive steps to address domain abuse at scale. We think that's something that's within the ICANN remit and would be very helpful. And we hope that as we see what the next steps are related to the RAA, that there'll be a renewed focus on what else can be done and in particular how to address abuse at scale.

So, as we were thinking about it at Meta, one of the things we came up with is requiring the suspension of customer accounts for known bad actors. Typically, you'll see, with a registrar account, there may be many domain names registered to that account. And if one of them or two of them (whatever number you may think is relevant) are clearly involved in fraud and abuse, why not suspend the account, the entire account, so that they can't redeploy these other domain names as part of the attack?

There's also work that could be done around verification of domain names that are highly suspicious and indicative of fraud. So just think of domain strings like Facebooklogin.com or Instagram help center verification. We see combinations like that; login, password, security. There's probably a couple dozen terms that I think would be general agreement that could be indicative of fraud, and having those be a trigger for an additional verification or inquiry would be helpful.

The other thing that we think might be helpful is updating the UDRP to disincentivize cybersquatting because we really don't see that the UDRP is serving as a deterrent at this point because the worst that happens is that the domain name gets transferred, and there's no ramifications to the registrant other than losing that particular domain name.

And then outside ICANN there's other things that are identified here in line with the approach in trying to find a solution to this types of problem. So for example, the NIS 2, we think that was a very solid step forward as it relates to WHOIS information. That type of regulation could be found in other jurisdictions in order to close the gap as to where WHOIS will be available.

We also think there should be incentives for cooperating with this investigations into impersonation attacks (I think that incentives are always helpful) and then taking a look at what can be done to disincentivize cybersquatting by shifting the costs from the brand owners to the abusive actors. You can do that through enhancing the remedies or damages that are under applicable law.

So these are just a few ideas that we've identified and they're listed in our report.

Next slide, please. And then as we think deeper about implications of solutions like this, we're always mindful of making sure that we're accounting for legitimate criticism and ensuring that we're taking approaches that are consistent with UN principles on human rights. That's always something that's top of mind for us.

Next slide, please. So with that, I've provided a link to the report in my slide presentation, and if you have any questions, I'm happy to take that. Thank you.

MASON COLE: Thank you. Margie.

Questions for Margie?

Yeah, Faisal?

FAISAL SHAH: Hey, Margie. The phishing tax went from 265,000 to 140,000. That's a pretty dramatic decrease. Do you have any thoughts as to why it's gone down so much?

MARGIE MILAM: We've taken a hard look at those numbers, and we think the collective benefit of that broad approach to abuse that I've mentioned … Bringing that all together, we spent a lot of time trying to figure out how can we close the gap, how can we better address this? So I think that's reflective of that. In that slide where I showed the multifaceted approach, we do talk about trusted notifier relationships as an example. To the extent that we can get trusted notifier relationships with key players that may be involved in that type of attack or their platforms being used, that helps as well.

So it's an interesting question, but I think the increased focus on how we approach fraud and abuse and the increased resources that were deployed … And that's why I cited the number earlier as to … You can see how much money Meta puts into protecting the platform from fraud and abuse. And all of that put together, I think, produces results. Thank you.

MASON COLE: Thanks, Faisal.

Michelle?

MICHELLE CHAPLOW: Ironically, Margie, just as we've been here, I looked at our Facebook account, [andalucia].com, and we've got a phishing message from Meta. So after this meeting, I'll show you it. And they've actually copied our logo and said, “Your account has been deleted as violating our copyright policy for security reasons. Please click on this link.” Well, obviously I'm not going to click on it, but many people in the public space and the Internet wouldn't know not to click on that.

UNIDENTIFIED MALE: And what domain is listed as the sender?

MICHELLE CHAPLOW: It's PGE [hoppel] center, then a whole load of numbers. It's a long one. It's a long one with hyphens and all kinds of things in it.

UNIDENTIFIED MALE: So I don't think you meant that it was sent from Facebook.

MICHELLE CHAPLOW: Yeah, it's got that it's been sent from the Meta team. No chance.

MASON COLE: All right, thank you. Michelle.

Other questions or comments for Margie, please?

Oh, yeah, go ahead, Vivek.

VIVEK GOYAL: Thank you, Margie. I think the stat about phishing attacks reducing is a common question. Everywhere you have presented this, people are surprised as to how come it's reducing. But my question is more towards the kind of registrar. So have you seen a trend where, with the registrars who do help you out and shut down these things, the repeated number of attacks are lower using those registrar systems? Or there's no discernible change in the pattern?

The reason I asked you what I want to get to is that, with the good guys from the registrars who do actively help, is that actually keeping their platform clean or it is not making any difference according to your feedback?

MARGIE MILAM: Yes. The more cooperation we have with the registrars, the better. And sometimes the bad guys just move to another platform. I think that's addressing your concern. Sometimes they don't. And in particular, for example (and we highlight this in the report), Freenom was giving away free domain names when they stopped delivering … And that was accounting for a large number of abusive domain names. Unless they find another free source, it can disrupt that actor from continuing to register new domain names. So there was a drop, a noticeable drop, in phishing attacks against the Meta brand and against others. I think several people in the room probably have seen a difference in phishing attacks simply because of what they call the Freenom effect.

MASON COLE: Thank you, Vivek.

Other questions or comments for Margie, please?

Okay, looks like the queue is clear.

Margie, could you maybe post a link in the chat for your presentation or the study?

MARGIE MILAM: Yeah.

MASON COLE: Okay, thank you very much. Okay. All right, I think we are done now with agenda item three, unless there's any other comment. Steve, let's just go straight to the slides next, please, because we're going to go right to agenda item four, which is another presentation, this time from the DNS Research Federation. We have Emily Taylor here. Emily, thank you for joining us. And members may remember that we commissioned a study (we and the IPC commissioned a study) earlier in the summer that the DNS Research Federation completed. And we were looking for … Well, Emily will summarize it better than I possibly can, but we were looking for some information about ccTLD practices that could be applied in gTLDs that would help against DNS abuse.

And so with that is a suitable introduction, I hope, Emily, please take the floor.

EMILY TAYLOR: Thank you very much, Mason, for that introduction. And also thank you to the BC and the IPC for funding this study. We also had the benefit of comments from the community which we took on board during the summer and also peer review from a staff member at CENTR. So you may remember that you saw me earlier in the summer in DC when I was presenting preliminary results to show you where we ended up.

Next slide, please. So I'm just going to talk a bit about who we are, background to the project, sources and methods, and I might hand over to my colleague Nathan Alan. And I'd also like to acknowledge our co-author, Alex Deacon, who will be known to many of you in the room, with thanks. So, sources and methods, results, conclusions, and then we'll hopefully have some time for questions.

Next slide, please. So, the DNS Research Federation is a nonprofit whose mission is to advance the understanding of the domain name system's impact on cybersecurity policy and technical standards. So we have cast our mandate deliberately, widely, and I think listening to Margie's presentation just now, the DNS is a thread that runs through all sorts of behavior, good and bad, on the Internet. And taking that wide approach, we hope, enables us to be flexible and dynamic enough to respond to emerging issues and challenges in the ecosystem and achieve that mission through education and research, improving access to data through the DAP.Live platform and engagement in technical standards.

Next slide, please. So, the background to the study. Now for this audience, I'm not going to go into the detail of NIS 2. I think NIS 2 is something that you have all lived and breathed over the last while, but actually the report itself does do a subclause-by- subclause pace through the relevant provisions in NIS 2 and how they relate to WHOIS and, of course, the longstanding WHOIS discussions within ICANN, which have been going back as long as ICANN has been around, and the impact of the GDPR on the WHOIS, as Margie just mentioned in her presentation.

But Mason, you highlighted this. The premise of the study is to look at the practices of EU ccTLDs and to answer the question, or attempt to answer the question, why are their abuse rates so low? And so we looked at comparative abuse rates across the ecosystem, we looked at market share, and we tried to understand the impact of these good practices that we were seeing, which I'll just say right now are very diverse. The wonderful thing about the ccTLD environment is everyone kind of does their own thing. And so that can be a great source of inspiration and good practice as we're casting around and stumbling for solutions.

So, next slide, please. So maybe I can just hand it over to you, Nathan. I told Nathan I wouldn't do this, but I'm going to do it anyway, so thank you.

NATHAN ALAN: Thanks, Emily. So, as Emily said, we used the DAP.Live data platform to obtain the data and perform the research necessary to understand the levels of abuse around the different TLD types, such as EU ccTLDs, gTLDs, which would be new gTLDs, and the legacy gTLDs as well. So the data that we used to perform the research was a combination of zone file data for the gTLDs and domain tools for understanding ccTLD registration numbers. And that was important for us because it's quite hard to get ccTLD registration figures directly in some cases. So we wanted to have a consistent figure across the board from as few providers as possible.

The abuse data itself was from providers from OpenPhish, APWG, URLhaus, and Spamhaus. And we also took into account in the research the pricing of the TLDs and, in the case for European ccTLDs, the population of those areas.

As Emily said. We also used the CENTR study to understand what different measures were in place in those registries to see if we could draw some conclusions from that. And so how we defined the abuse was through combining phishing, malware and spam data. And we counted the distinct domain names found. And that, I feel, is important because we want to compare apples to apples when we're understanding the amount of abuse for a particular TLD versus its market share in terms of registration numbers. And the data was for the year 2022 from January 1 to the end of December.

Next slide, please.

EMILY TAYLOR: Thank you very much, Nathan. So one of the things about the European ccTLDs … We felt like it's important to sort of lay out some of the background. You were dealing with the continent of Europe. One of the most the largest trading blocs in the world is the EU. You've got advanced economies that adopted the Internet early on, have got robust institutions. A lot of them are G7 members, OECD countries.

So you've got also a lot of registration. So the ccTLD market in Europe is very vibrant. 15% of global market share. And the vast majority are nonprofits. And that ranges between private sector and public sector. So often the genesis of the ccTLD might be within a university or some other public sector institution and some have been spun out as private companies, but for the vast majority, they don't have a profit incentive. All of the ones that we looked at operated thick WHOIS, to the best of our knowledge, and 70% differentiate between legal and natural persons.

My personal opinion on that is that the European ccTLDs have been living in a data protection environment for nearly 30 years. And so the distinctions between legal and natural persons come very naturally to those organizations.

But there's lots of other quality markers (high renewal rates, large domestic market shares) and also there's been quite a lot of analysis on the web content. And the web content in a lot of these European ccTLDs is what we would call developed. So in other words, it's not sort of junk parking pages, these are real sites being used for real organizations and so on.

Thank you. Next slide, please. So here are results and also a note about the data. You heard from Nathan and myself that we were wrangling quite a large number of data sets, all of which do their own thing in various ways. So part of the discipline is to deduplicate the data, to normalize it, to make sure that we are comparing apples with apples.

So in about the week before we came here, we noticed an anomaly in the data which arises from a difference in the way one of our feed providers categorizes a top-level domain. So you'd think that was a basic thing and it's no criticism of anybody involved, it's just a different way of doing things that we didn't really know about.

So what difference does it make? It made us undercount the abuse in TLDs that operate through second levels; so the co.uk, the .br, the .au. Actually, for our study, which is the EU ccTLDs, it didn't really make any difference. If anything, it actually increased the level of quality of those. So I just thought I'd note that and we'll be just slightly revising the report to take that into account. And that will be available in the next few weeks.

Next slide, please. So what did we find? We found that the global abuse rate is about 0.5%. Now, you heard from Nathan on the approach that we took. We really tracked quite closely the contracted parties' or the ICANN definition of DNS abuse, which goes down to the individual domain name and also restricts to botnet, spam, and malware. We're not looking at botnets here, but we did include spam, and I think for some members of the community, that is quite a controversial point. So I would just like to highlight that the definition covers spam, where it is a carrier of our other nasty stuff. But of course, the abuse lists that we're using don't really say what type of spam is included and whether it's actually within the definition or not. One of the things that we're hoping to do is to provide views that you can sort of just filter down and eliminate that. But it does seem like, on average, quite a low figure.

But if I could just point you to an excellent blog that Alex Deakin wrote in the spring of this year, he actually shows through data derived from the DAP what happens to the numbers when you go down to the individual domain name.

So we're not saying at all that we have a position or that we know the truth on how you define these terms and how you measure them. As Nathan said, what we wanted to do was compare apples with apples, have a consistent data point that went through all of the TLDs.

So the headline figure is that the EU ccTLDs are far below the average figure, below being good under. Other ccTLDs also perform just under the average, but they're much closer to it. Legacy TLDs are a bit below the average and new gTLDs quite far below being bad.

Next slide, please. So the EU ccTLD abuse rates are the lowest of any TLD block within the global market. That is an uncontroversial finding. It matches the European Commission study that was published in 2022. But it is quite striking how far below the EU ccTLDs are.

Next slide, please. So, if we look at it in terms of market share, we've got 14 or 15% of market share belonging to the EU ccTLDs. And then if you look at the next slide, we're looking at the abuse rate.

So, next slide please. So that's 2% of the abuse is contributed to, if you like, by the EU ccTLDs. And while the abuse rates for other ccTLDs and legacy gTLDs are more or less in line with their market share, which is actually what you would expect coming to the data without any assumptions, you do see that the new gTLDs provide a greater contribution to the global rates of abuse compared to their market share.

Next slide please. Looking at the EU ccTLDs, out in front is dot-DK for Denmark, followed by the Czech Republic and Belgium. And all of them are falling below the global average, which is around the 0.5% rate.

Okay, next slide please. So what about the anti-abuse measures? It is quite striking that as a group you've got quite a homogeneous performance. You can see that there's variation, but it's quite homogeneous. So is there something to do with the way that these ccTLDs are handling data that can explain it, or at least partially?

And one of the things that we sort of set out in the report is the perceived connection between high-quality data and better security is a thread that runs through the ICANN environment almost since the beginning. You've got statements from the ican.org, from the SSAC and so on, and also you see it mapped out in the NIS 2 and reflected there, but it didn't start in NIS 2. This is a thread that has run through our conversations in the ICANN community for a long time. So it's an assumption that people make, but of course we can't know whether one single thing is like, oh, that's the answer. What we wanted to do is to, with the aid of the center study, look at what people were doing.

So, next slide please. So the message of this (I'm not going to go through every data point), is that the ccTLDs generally do a combination of things. They don't do one intervention on data quality. They do a lot. The most common approach across the ones that we had data for was that they make ad hoc checks, usually in response to some sort of report or some sort of suspicion or their own inquiries.

The use of electronic IDs, which is also called out in NIS 2 as an example of best practices, is still quite limited. We identified three specific ccTLDs that use it and we believe there are another two that do. And the CENTR report is very good in sort of unpacking the eID debate. But our conclusion is it's still very early in its lifecycle. There's still not even a pan-European approach to eIDs, let alone a global approach. But you see it's in the minority that are using eIDs. A lot of them take ad hoc measures, some do stuff at registration and some others do other stuff. There's a little bit of checking with external databases. Maybe sometimes they take a copy of a passport, all sorts of things. No one thing comes through as the answer other than the ad hoc checks.

Next slide, please. So there's some debate about if you load the market with obligations to check data, what are you going to do to their market performance, and also what are you going to do to their cost base? So we thought that, given that the vast majority of the EU ccTLDs operate on a nonprofit basis, we could look at the cost price, which most of them publish, and also look at their market penetration and just see what we find. And this is really fascinating to me because it really confounded a lot of my expectations. What we see is that if you're charging a cost price of over €12, you're probably going to have an adverse impact on your market share. But if you go under that, even if you charge nothing, which some of them do, the market shares are all over the map. Right?

So I think that this might be a hopeful thing for the domain name industry to contemplate. I think that there's also a lot of nuance in when people decide to time their checks and who the burden falls on. So checks at the point of registration will typically fall on the registrar, who are typically operating on quite tight margins. For anything that's done during the lifecycle of the domain name, thereafter, the burden with a thick WHOIS registry would fall typically on the registry itself.

Next slide, please. So what do we conclude from this?

Next slide. There are low rates of abuse across the entire sector in the EU ccTLD community. Many take proactive measures to improve data quality. And we felt that probably the clincher in this is that there's a multiple approaches. Most of them do more than one thing. So it's almost like data quality is a seam that runs through their business that they care about and they will adopt measures at different points. Proactive data checks do not seem to impede strong market penetration, and the EU ccTLDs show us that it is possible to achieve both high quality and low price domains with healthy market penetration.

I think that's it. Next slide. Yes, very happy to take questions or comments.

MASON COLE: Thank you, Emily. Thank you, Nathan. Good presentation. And yes, we have seen some of this data before, but it's very useful when you're in the ICANN setting to talk about what can be done about DNS abuse.

Questions and comments for Emily?

Steve?

STEVE DELBIANCO: Thanks, Emily. Were you and your colleagues at the Day Zero event that eco sponsored here? It was Friday. So it was entirely focused on NIS 2, with an audience that had several ccTLD operators in it, but also registrars who specialize in serving European, including European ccTLDs. So they made a remark about how frequently they rely on the redacted personal data in WHOIS registrant data to go after DNS abuse. And we heard some surprising anecdotal, not statistical, answers. Blacknight suggested they never use PII, but rather they use the IP address. So they don't even suggest that they look at names. Another suggested that errors in the accuracy was a telltale for them that this is probably a bad actor, so they actually don't want more accurate data. That was quite a surprising revelation. And we heard another suggest that they use IP addresses more than they use domain names and registrant data.

So my question for you would be whether your research allowed you to determine the measures they're taking that are having an impact. You displayed a matrix showing the things that they do, but that stops short of suggesting what is it that Germany does so effectively that allows them to be at the top of that list? Do you have any more insights about what they look at when they go after abuse? Thank you.

EMILY TAYLOR: Thank you. That's a great question, and thanks for framing it in that way. So I can answer the anecdotes with anecdotes, but then move on to the core of your question.

I'd also like to just highlight another blog by Alex where he highlighted that distribution of malware is at the moment overwhelmingly taking place on IP address space, like 75% or something. So that resonates.

On the more granular detail, I was actually having a very similar conversation in the margins the other day about what next,; where are the gaps in our knowledge? We relied upon a study by CENTR, which just sort of basically, I imagine from a survey, was just going, “Do you do this? Da, da, da.” But actually, first of all, the data set is not complete, and that would be a very useful contribution to our knowledge, to the community's knowledge. And the second of all, exactly as you highlighted, I think an awful lot would be revealed in sort of more conversational, interview-based type of research. We would love to sort of just delve more into this because (and this is a sort of personal anecdote based on very, very out-of-date personal experience working in the dot-UK registry) stuff would come to you and it would be like, really bad and really nasty, but actually it's not really within your role to look at the content or to determine whether something's illegal or nasty. But you're still like it's nasty. And we would often look at the registration data and it would often be inaccurate, and that would give us a contractual nexus to take action.

But whether that just sort of comes down to one individual who happens to hit it, or whether that's something that we can extrapolate from, I think there's an awful lot more to discover in terms of what really makes the difference. But I think we've started the process and I think there's an awful lot more to do. Thank you.

MASON COLE: Thanks, Steve, for the question.

Other questions for Emily or Nathan, please?

Okay, I see nothing in the queue, Emily—I'm sorry, Chris.

CHRIS CHAPLOW: No, just a quick one. Could I ask what was the greatest surprises, perhaps, of the investigation you've carried out, what you thought might be and what you were surprised by, good or bad?

EMILY TAYLOR: Yeah, thank you very much for that. So for me, a big surprise was the market penetration analysis against cost. I didn't really expect it to be all over the map. But on the data side, I think I was expecting a clearer correlation between “more measures equals better performance,” and it doesn't seem to be. But as I say, we haven't really got to a profound understanding of what each registry is doing.

For example, take eID implementation. I think there's a lot of hopes and also sort of queries about how that will work in practice, know your customer in that way. But what we see is that for the three registries we had in the data set, although all of them have great performance compared to the average, they're not like ranking one, two, three.

And so those were some of the surprises. But data always brings you its own story and its own surprises.

NATHAN ALAN: Could I just kind of follow up with that as well? So as part of what we've been doing here this week is we have a stand, and we've been speaking to a lot of registries, and the predominant theme is that … And we've been seeing a lot of ccTLD registries coming to us. Obviously, there is the upcoming know-your-customer aspect to all of this. But as I said, we've been approached by a lot of ccTLD registries who want to know their domains as well as their customer and understand what's happening with the domains that are under management and how they want their registrars to be more in control of understanding their domain portfolio and what's happening within that space.

So it's just been quite interesting that we've had a lot of interest from ccTLD registries relating to that.

Thank you, Nathan. Thank you, Chris, for the question. Margie?

MARGIE MILAM: Thank you for the great report and presentation. I was struck when I read the report about the fact that all ccTLDs in Europe are thick. To me, that almost seems like a best practice, and it just seems like it's a stark contrast to what we heard in the day zero event that was put out regarding NIS 2, where many gTLD registries were saying, we don't need the data, we don't need the data. But if you take a look at your statistics, especially the new gTLDs, actually abuse rates were higher than what you would expect for the market penetration, if I'm not mistaken, versus the ccTLDs on the flip side, where they were lower than the average based on market penetration.

So I was just curious what your thoughts were on the thick WHOIS issue, because I found that striking and I also worry that if the NIS 2 is interpreted in a way that prevents thick WHOIS, which I've heard from some contracted parties that they want to read it that way, that it would actually hurt the abuse rates because if ccTLDs were no longer able to be thick, would that disrupt their operations and make it less likely that they would have accurate information?

EMILY TAYLOR: Yeah, I mean, we're all going to see what the impact of NIS 2 is on implementation, and there's always the sort of surprise feature of what the actual impact is towards what the legislative goals might be or what the expectations might be.

While it's striking that all of them operate thick WHOIS, it's also the case that most of the new gTLDs do as well. And it's really the, I think, dot-net, dot-com, and dot-jobs that are the thin WHOIS market.

Another aspect that might also be useful is, although I'm not sure whether this is the case in the EU, that some of the EU ccTLDs may well have a direct contract with the registrant. I think most of them do have the classic registry-registrar model at this stage. But the genesis of the way that the EU ccTLDs have evolved is the registry taking quite a proactive stance and sort of really being a coordinating figure among the different communities and stakeholders that all have an interest in the TLD functioning properly.

So what really came through to me is that this EU ccTLDs seem to care about data quality, and that comes back to that theme of, like, data quality equals better security. And it does actually seem that that comes through in the results as well in terms of abuse mitigation. So I hope that helps.

MASON COLE: Okay, Paulo?

PAULO ROQUE: Thank you very much for the excellent report about European abuse. Do you have any information about global sites, especially Brazil?

EMILY TAYLOR: Yes, we do. In fact, we've mapped the abuse rates across all of the TLDs that we can find. Sadly, if I was sitting here in the summer … You know, I mentioned that sort of data anomaly. That led to a downgrading in some of the performance of the TLDs that operate through second levels or have some registrations in that way. But we have data for Brazil and other TLDs in Latin America. And as you saw from the overall stats, the ccTLDs perform well wherever they are in the world.

And I think one of the things that we plan to do in the next few weeks is to make the live data much more available and enable people to filter down into areas of interest and, obviously, geographical regions would be a good one to do. So, really happy to pick that up with you afterwards. Thank you.

MASON COLE: Thank you, Paulo. Other questions for Emily? Oh, Margie?

MARGIE MILAM: Another question I have, Emily, is related to privacy and proxy services. Do you have any information on how ccTLDs approach that issue?

EMILY TAYLOR: So privacy and proxy services in my experience have been more of a feature in the gTLD environment historically. And, of course, since the redaction of WHOIS, it's hard to tell what impact there is, but it's made the sort of the publication element of registrant data less of a sort of urgent thing.

What I can highlight (and it's in the report) is that the dot-nl registry, SIDN, recently announced that it would be banning privacy and proxy services. And the justification behind it is, like, we need to know who the registrant is.

That's the only example I'm actually aware of. But again, it would be a very interesting aspect to look to, sort of have a bit of a deeper dig into.

MASON COLE: Okay, any final questions for Emily and Nathan?

Okay, Emily and Nathan, thank you both for the presentation. Very helpful. Appreciate you being here.

All right, Steve, if we could have the agenda slide back and we're going to move to the next item on the agenda, which is the policy calendar review. Steve, the floor is yours.

STEVE DELBIANCO: Thanks, Mason. Steve DelBianco, your vice-chair for policy coordination. And I'm now going to display the same policy calendar that I sent to everyone yesterday. This is an open meeting, so we may well have attendees that are unfamiliar with the BC's practices. But every two weeks, we meet as the BC virtually. And of course, we meet whenever we're at the physical ICANN meetings. We guide our policy discussion through what we call our policy calendar. It begins with the discussion of things we have filed recently with an opportunity to remind us of our work and to thank those who contributed.

But we then segue pretty quickly to the open opportunities for public comment that the BC wants to engage in, and that includes both within ICANN and outside of ICANN. So at this point, we look at two opportunities that are currently scheduled, one being a comment period that closes at the end of November on a new draft of the Terms of Reference for the very first holistic review, called the pilot holistic review, that ICANN will encounter. This arose out of an ATRT recommendation, and that has changed in shape and scope over the past couple of years. This is another and probably the final opportunity for us to influence the scope of what this would cover.

Anyone who has followed the BC's work over the last few years (and quite frankly, this morning's interaction with the Board) knows that the BC is pointing to this holistic review as perhaps the only opportunity to try to change the structure not only of GNSO, but maybe the structure of the ICANN Board in a way that favors the opportunity for us to have more representation at the Board level. This holistic review is an opportunity to do that, and we've made comments on that before, only to be ignored. For instance, the current Terms of Reference say it is outside the scope of the holistic review to look at the structure of GNSO, the Org, or the Board. However, if someone believes that it's relevant to the holistic review, they can submit those comments.

So once again, we'll tilt at windmills, and we'll come back in with a strong comment suggesting that if the ICANN Board were to include additional Board members from GNSO, it would be one more from the contract parties and one more from the non- contracted parties. I'm not suggesting that only to solve our dilemma in the non-contracted party house, but to make the Board representative of the perspective of GNSO, since GNSO was responsible for nearly all of ICANN's revenue and in excess of 98% of its activity. So the GNSO currently has two Board seats, and we'll continue to press for more.

We have several other things that we've had in our previous comments that have been ignored, but we'll submit them again, and then the opportunity for us is to be one of the members of the review team who pulls together for the pilot holistic review.

So at this point, I'll thank Barbara. Margie, you were very helpful as well on the comments we submitted last time in November, about a year ago. But I need volunteers from the BC that would be willing to help me come up with the BC's follow-up comment.

Vivek, would you be interested in helping? That's outstanding. Thank you, Vivek.

Who else in the BC would be willing to assist with that?

Tim. Fantastic. Anyone else?

And Marie. Great. We can stand on the shoulders of the work that Barbara and Margie did last time, so our comment can be quick and easy.

For our interest, this morning, when I brought this topic up with the Board, it didn't get shot down immediately, and I had two or three

Board members say to me afterwards they thought it was an interesting idea. But I do know that the Board Governance Committee board member that was speaking to this topic is not a fan of expanding the board. To which the BC would answer, "Well, fine. Then just take two seats away from the NomCom and give them to GNSO. And the Board won't be any larger than the 15 it is today." Well, that's not going to be popular either.

All right, thank you for that. We have one other—go ahead, Mark, please.

MARK DATYSGELD: Thank you, Steve. Just to reinforce something that we have been discussing this week to any member who wasn't present in those sessions, it has come to light very clearly in the past few months, something that you in particular has said for a long time; that the non-contracted party house is fundamentally set to fail. It is built to be in constant conflict over positions in such a way that we are permanently locked into those situations. And if this year has shown us anything, it's that this is completely detrimental to the policy-making process and derails the actual work that we should be doing in ways that are completely insignificant.

So it is not only important that we pound on this, but we should take this experience TO demonstrate, right? Like, since we went through all of this this year, over Board Seat 14 and vice chair and whatever, let's use it as an example. We already went through it anyway. The community knows. So let's keep advancing this until the Board acknowledges that this discussion needs to be open because it's very convenient for them not to open it. Thank you.

STEVE DELBIANCO: Thank you, Mark. And as you know, if we can't do it as part of the holistic review, there isn't any other place to do this. The bylaws- mandated reviews of each AC and SO don't even speak to the idea of the broader Board fitness for purpose, process and structure. They only look at each stakeholder group, each AC and SO separately.

All right. The second and final element that's open right now is our ongoing effort to assist and persuade member states in the European Union to transpose the requirements of NIS 2 into their national law and regulations in a way that increases our opportunity to get access to the registrant data that we need and vendors need to chase down DNS abuse and problems that plague the customers of business constituency members and damage the reputations as well of registrants.

So I earlier remarked upon the Day Zero event on this too. I sent an email that included pretty extensive notes from what happened that day. And so I don't need to get into the details of that here, but I will suggest something I mentioned this morning in the CSG board interaction. I said that ICANN's draft letter to the GAC group that's covering the NIS 2 implementation framed it this way. It suggested that they were grateful that NIS 2 included mention of the multistakeholder model. They were grateful for that. And the second thing they said is that we're going to attach in the appendix all of ICANN's current policies with respect to the collection, transfer and disclosure of information. And that's about it.

So I would characterize ICANN's response as one that says this isn't our issue. We have policies in place, and the policies allow registrars and registries that are covered by NIS 2 to comply, and we need do no more. It's as if ICANN wants to step back. So it might be incumbent on the BC to try to bring ICANN back into the process. After all, registries and registrars and resellers won't all have to do their own verification checks. I don't think anybody believes that's a good idea, and I don't even think the EC thinks that's a great idea, but they're basically punting and say, "You guys work it out." And that's an opportunity for ICANN, particularly the contracted party house, to step forward and try to come up with ways that will work better, relying on best practices that we heard earlier from Emily but also confronting the fact that within about a year, they will have to comply with NIS 2.

Are there any other comments on NIS 2, since it's being followed so closely by Marie and other members of the BC?

MARIE PATTULLO: Just to tell you where we are with the procedure, if that's useful, as you know, NIS 2 is a law. You may hear certain people complaining that they don't like it and "Can we please change it?" It's a law. That's what we do in Europe. We make laws.

What's currently happening is the 27 member states that make up the EU need to take that European directive and turn it into law within their own states. And there are two ways that you can look at this happening; one, in the capitals themselves; so the national governments. But two, as far as it concerns Article 28, please remember this entire directive is a lot bigger. It goes to cybersecurity itself. It's all about resiliency of the system. But purely on the Article 28 part, the WHOIS part, there is what's called a cooperation group. That is exactly what it says on the tin. It is a way for the 27 member states to try to agree on some kind of guidelines that hopefully will give us some kind of harmonization.

Now, this is under the chairmanship of Finn Petersen, who is here. He's the Danish FAC rep. Very, very experienced. And their next meeting is going to be in Lisbon in November. We from the BC side and also, I can tell you, in the EU side, are speaking with or trying to speak with the national governments, because this is where the touch points are. You can write as many times you'd like to the European Commission. They're not in charge of this. The governments are in charge of this.

And what I will make a shout out for, please, is, if you have, let's say, concerns in Spain, you need a Spaniard in Spain to talk to the Spanish government. With all due respect, lots of letters coming from Brussels, let alone the other side of the Atlantic, aren't going to have as much effect.

Very happy to talk about the procedure in war, but I think that's enough.

STEVE DELBIANCO: Thank you, Marie. Appreciate your constant vigilance there.

The next section of what we do in the policy calendar is called Channel Two, and it's about the council itself; the council being the policy management body of the GNSO. And we are represented by two councilors, Marie Pattullo and Mark Datysgeld. And at this meeting (that is to say, late tomorrow), Lawrence Olawale Roberts, sitting over here on the right, has been elected by you in the BC to succeed Marie on

Council, who is termed out. But Marie is staying on the Executive Committee, assisting with CSG liaison.

So at this point, we typically reexamine what happened at the previous council meeting, which was September 21. Then we talk about the upcoming council meeting. The BC has already had a meeting two weeks ago where we recapped what happened in September.

So I'll go immediately to what is on the books to happen tomorrow at the council meeting. It'll occur at 13:00 hours here in Hamburg and I invite all BC members present to sit in on the council meeting. You can interact with your counselors either by walking up to them at the table and asking a question. You can go to the microphone or interact with the executive committee who's trying to back up our two counselors.

The agenda highlights are listed here and I was going to turn to Marie, Mark and Lawrence to talk to us about what to expect tomorrow and see what you wanted to advise us about.

MARK DATYSGELD: So on that first subject, some of you might remember that this was supposed to be voted on in the previous meeting of the council and was removed from the agenda with a day to go. So what happened at the time, which has not been discussed and technically clarified, is that the CPH said that it would not be able to vote positively or endorse the proposal as it was at the time. And now we are circling it back to try to have another stab at this. I'm unclear exactly on how much this has progressed.

Marie, do you have a grasp on how much this has progressed? Because it doesn't seem like it has. Has it?

MARIE PATTULLO: A grasp about the SOI?

MARK DATYSGELD: Yes.

MARIE PATTULLO: Okay, there are two. There is one that is a mummy SOI. What that means is that when you are involved in ICANN, you tell people who you are. Mummy SOI is going to have a baby, and if you are involved in a working group, a specific group, you've got a specific SOI for that. There has been quite a lot of debate back-and-forth and also quite some confusion. It has always been the case that you do not have to disclose your client. Always. This is not new. If you choose not to disclose your client, that is made known in that "Are you here on behalf of somebody else? Yes." So everybody knows.

And I don't know … I'm thinking Steve can channel Marika because I know Marika did some amazing research on this and got all the numbers. This exception, if you want to call it that (the "No, I'm not telling who my client is") has been used in some minuscule amount of times over the course of the history. It's a tiny, tiny figure, but there is a fear that it might happen in the future.

Anyway, there was no agreement in the working group, which has got this wonderful name acronym, as you see. So, so far as I understand it, what's going to happen tomorrow is we're voting on all of the other recommendations because everyone agreed with those and this one is basically the status quo.

I'm looking at Steve. Would you say that's a rough give or take?

Yeah, with more words.

Massive shout out to Manju, though, who really stirred this amazingly. And she's put up with so much work here.

What I would say is that issue was not going away. And I'm looking at Lawrence because Lawrence, as of Thursday, you will be taking my place on this committee, won't you? Lawrence, nod at me. Thank you.

LAWRENCE ROBERTS: Sure I will. Thank you.

STEVE DELBIANCO: Marie and Mark, discussion of the next couple topics; five, six, and seven?

MARK DATYSGELD: Yeah, sure. So, there are some topics that we would like to bring up; in particular, I think the holistic review that we were just discussing. As you know, there has been a process to … I'll draw straight from the council page. So here is some of the feedback about what has come from the draft terms of reference. The scope of the holistic review is unclear. There is a lack of independent examination in the holistic review. There is a lack of identified dependencies. The community might not have the ability to support the pilot holistic review work.

So as it stands right now, there is certainly a lot of doubt over what is going to take place under that under the current terms. So there will be a discussion on what is supposed to be done. But this is still in the discussion phase. We will not be taking any particular decision, as far as I understand.

So if anybody has any input on how we should be handling that, now would be the perfect time to do it. Otherwise, we will follow with the BC's historic position on this and the positions that we have held on this matter.

Would you like to complement this, Marie?

STEVE DELBIANCO: Thank you, Mark and Marie.

Then, any other questions for our councilors? Again, you can ask questions during the council meeting tomorrow or do anything else on list.

Next up would be some other activities that are managed—Marie, go ahead.

MARIE PATTULLO: Sorry, on that last point, Steve, I wanted to specify there is an open mic at the end of this … first session? Yeah. Because there are two bits tomorrow. One's administration when the new chairs are put in place. But right at the end of the session tomorrow, there is time for an open mic. Please come and please talk to the council. Don't talk to me. I won't be there. I'm leaving. But Lawrence and Mike would love to hear from you in great detail. Thank you.

STEVE DELBIANCO: Thanks, Marie. But if a BC member had a concern that is relevant to the BC interests and mission, it would be even better to discuss it with your councilors and your colleagues rather than surprising us all by going to the mic, since we can reinforce and have much more opportunity to make the points. And this is a golden opportunity to do so.

There are some other activities the council is managing, and we'll just cover them very briefly. One of the first is the working group on transfer policy. We have Zak Muscovitch over here and Arinola who represent us on that group. I would turn to you to see whether you have any updates or any questions for your colleagues on that.

ZAK MUSCOVITCH: Hello, everyone. So Arinola and I have been the BC's representative in the Transfer Policy Working Group for close to a thousand days. And this is the first time I think we've seen each other in person across the room. So that Transfer Policy Working Group meets, I guess, once a week for an hour and a half. And there's been not just 1000 days but 110 sessions of that working group. And the last few months have been focused on mainly technical matters that aren't of direct interest to the BC. So that's when Arinola and I tune out a little bit. But there are some new issues, or at least old issues, that are re-arising that are coming up shortly.

One of the ones is what I've previously reported to the BC about, which is a reconsideration of a possible registrant-initiated transfer dispute resolution policy. The way it works now is if there's a transfer dispute, it's registrar to registrar who must handle the dispute. But due to ALAC's input and our own input, there's been some more discussion of considering it at the GNSO level; the ability to or the creation of a policy or an amendment to the current policy that would enable a registrant who's had their domain name stolen from them, being able to handle the dispute themselves directly with the gaining registrar, rather than rely on their losing registrar to represent them.

The second thing that's going to be coming up shortly is we're circling back to transfer locks, and there's going to be a discussion commencing about the registrant lock; the change of registrant lock, rather. So this is a lock that is put in place when there are certain details or wholesale changes made to a registration.

And so that's something that Arinola and I will continue to report to you on as the matter progresses.

Arinola, a few words from you.

ARINOLA AKINYEMI: All right. Thank you, Zak. You've captured virtually everything and then you've reported as it should be. I think you've done great. Thank you.

STEVE DELBIANCO: Thanks, Zak and Aaron. Appreciate that very much.

ZAK MUSCOVITCH: Can't thank Arinola for working with me throughout this whole period. It is so nice to have somebody else along for the ride with you and so I appreciate that very much.

ARINOLA AKINYEMI: You're welcome, Zak.

STEVE DELBIANCO: All right, thank you. The second item up is under the GNSO guidance process. Lawrence Olawale Roberts has represented the BC on that working group. I'm going to quickly display Lawrence's email, which describes some, I think, progress on this. Initially, the working group was heading down the path of suggesting that when ICANN promotes the assistance it can provide to applicants in the next round, the working group was heading down a path where they would expressly not promote the program to business organizations, trade associations and private sector entities around the world in developing regions. And with his single-minded determination, Lawrence seems to have been successful at changing that. So, Lawrence, over to you. And I have it on the screen.

LAWRENCE ROBERTS: Thank you, Steve. So again, thanks to the BC comments that went into this process by Vivek. And is it Daniel or David?

Yeah, thank you. And incidentally, both of them are sitting together. The comments we made coupled with what the entries that came in from the GAC and Com Laude helped to sway members' thinking to the fact that we should definitely not restrict private entities, private sector players, from being outreached to when this process begins to discourse.

We had some suggestion to the change of the recommendation and while the focus was also to try as much as possible to get ICANN Org to still focus on certain groups, but give them the leverage to also reach out to business.

So right now the comment reads, “Target potential applicants from the not-for-profit sector, social enterprises, and on community organizations from underserved and developing regions and countries. This should not exclude any entities from outreach efforts, such as private sector entities, from developing underrepresented regions, recognizing the goal is to get as many qualifying applicants as possible.”

While this does not say that by the time private sector entities will put in applications when applicant support opens (and it's supposed to open about a good number of months before the program itself starts), while this is not some form of guarantee that private sector entries might receive consideration, it's at least a good effort at ensuring that entities get to understand that there is this level of support, whether it is the pro bono services or the discounted fees that can be assessed through the program.

So we'll keep working on this to ensure that business does not get disenfranchised in any way. Thank you.

STEVE DELBIANCO: Thank you, Lawrence. Appreciate that.

The third one up is the Registrant Data Request System, or RDRS. It's a voluntary system that is supposed to assist the decentralized entry of—Vivek?

VIVEK GOYAL: Sorry, just on the last one, on what Lawrence was saying, I wanted to suggest that when the time is right, the BC should also do some outreach to make the application support popular in the regions in which he are active, because we really should get businesses to apply for this and make use of the application support program. Thank you.

[MARK DATYSGELD]: To briefly follow up on Vivek, if I may, exactly. And I have been discussing with Kathy Kleiman, one of the founders of the NCUC. They were initially very against us. The whole fight was around this. But I think the position has come around to the fact that SMEs are institutions that need to be recognized in that way.

And one of the things that she was asking me is that we provide use cases for it. That's one of the points of skepticism that she has had. So if we work together to bring up some use cases, I think that would be useful to continue to strengthen our position. So, for example, if one of our members, the Brazilian Software Association, wants to do a TLD for Brazilian software, that should be all good and dandy, and they should have access to that process and be within the limitations of what their currency and region is. So if over the course of the next few months, we can keep generating some examples of how we would use that, I think it will continue to increase our position. But again, thank you. Lawrence. That was a thankless battle that you carried out for us, and you won so many, many congratulations.

STEVE DELBIANCO: Great, thank you.

That was the GNSO guidance process.

Another one is the Registrant Data Request System. I represent the BC on a small team of council that is now monitoring that system, which will be launched in two weeks. I've discussed it with you many times, and I spent a couple of hours trying my best to ensure that requests that go in for non-participating registrars are retained in ICANN's databases (not disclosed, but retained), at least long enough that we can do analysis later on on registrars that ought to be participating since their domains are being subjective requests.

Going to continue to press on that. But at this point, it isn't clear that we'll be able to gain sustained participation from the requester community. I do think that in discussing with other members of the BC that we might well start by submitting requests. But if we don't see some satisfactory responses, we are unlikely to sustain that. And I'm doing my best to suggest that it might be worth sustaining if we can use it to generate the data that will become the driver for new policy. So, for example, if we retain what it is we're submitting, and it shows that a substantial portion of domains about which we need information are domains that are covered by non-participating registrars, we may be able to drive ICANN to policy that would require all registrars to participate in the RDRS. That would be a simple example. But if we don't use the system to submit requests, the data will be used against us. The data will be used to say, "Look, there's no demand, obviously, for WHOIS anymore. We have boiled the frog, and there is no need to reinstitute or rebuild or fix WHOIS because there's no demand for it." And that is a trap. It's a trap that we saw very early on. I identified it at every meeting, was assured the data wouldn't be used for that purpose, and yet that's precisely what is going to emerge from this process.

Okay, next item up was the subsequent rounds. And Ching, you represented us on that ably, and I really appreciate that work. We're in implementation right now, and one of the issues that's hot is the registry voluntary commitments. There'll be a session on that at 11:00 tomorrow, sponsored by the Non-Commercial Users Constituency, the NCUC. They invited me as an individual to participate by drafting stress tests about what would happen about ICANN enforcement of registry voluntary commitments if they involved content; content that is explicitly not to be covered by ICANN. It's outside of the mission under the bylaws we adopted after the Iana transition. So I have those stress tests. I'm going to circulate them tonight to the BC. So I'm not there representing a BC position. I'm Steve doing his stress test thing.

And my stress tests draw the conclusion that it would be a disaster for ICANN to lead governments to believe in the next round that they can raise objections, the applicant can agree to make changes to address the objections, the GAC then removes their objection, the applicant wins, the domain is delegated, the TLD is delegated, and six months later the GAC says, "Wait a minute, you're not following the voluntary commitments you made," and they turn to ICANN to enforce it, and

ICANN says, “No, we can't do that because it involves content.” That may be true, but it should have been identified upfront, prior to the opening of the round and prior to the governments relying upon ICANN enforcement to remove objections. Nothing could be worse than to play bait and switch with governments who hold the fate of ICANN in their hands at the General Assembly of the UN in 2025.

So it's all wrapped together, and we're going to continue to press on that.

Tim, I wanted to turn to you next in Channel Three, which is our commercial Stakeholders group, and I'll scroll the screen as you instruct.

TIM SMITH: Thanks, Steve. As you will see, or maybe as you won't see, depending on whether you're watching or not, we started off ICANN 78, actually, with a day zero event, with CSG and NCSG coming together to discuss what we agree on, what we disagree on, and to try to move our agendas forward. So I put in my report some of the attendees there, and you'll see it's all in first name, on a first-name basis. And that's, I guess, as collegial as the meeting really was.

And so I’m very happy to have spent that day discussing issues. It really, I felt, brought us back together and sort of mapped out a future for NCPH with the intention of having regular meetings at the ICANN meetings, but also trying to get back to a regular intercessional, which we'll be investigating over the next while.

So just a few of the bullets of the things that took place. There was an agreement to put together a small team or a micro team to review the process for GNSO vice-chair selection. And there were a couple of drafts that have been done over the years. And I guess the micro team will take a look at those and polish them up and come back with recommendations.

"The micro-committee to establish expectations for new Board Seat 14." As you know, we just seated Chris Buckridge in Board Seat 14. The feeling in the room was that we need to set out good expectations for him, for him to be able to succeed in his role and also going forward to have, while he's in a three year term (and anybody else would be in a three year term) also annual reviews. And because the NCPH will be coming together on an annual basis, that should be fairly achievable.

Also in future selections, it was agreed that the idea of joint interviewing would be a positive step. This time around, NCSG and CSG identified different candidates interviewed independently, and it would be good to come up with … well, I called it a script. I don't know that it's really a script, but certainly a set of questions that both NCSG and CSG could be hearing the answers to. So that's another thing that's going to be worked on.

We also had a discussion as it related to things that we have in common. We've already talked a lot about the holistic review, and it was agreed that we would continue to monitor that. And other issues we agree on we would continue to try to work together and periodically discuss.

And on the final note that I've made here, which is about the updating the NCPH Wiki, it was interesting in the meeting that not everybody had full recall of past discussions and past decisions. And while there was a NCPH Wiki, it appeared that there were two people who actually knew that it existed and where it was. So we increased web traffic to that considerably just over the course of the day.

So that was that. I thought it was a pretty productive meeting.

Other meetings that are taking place here, which have already taken place, was the CSG membership meeting that took place yesterday. I think most of you were in the room. It was a pretty well attended room, I thought. And we had a report or had a discussion with the Public Safety Working Group, which was worthwhile. Margie also gave us her presentation, which you saw again today. So that was good to be sharing that with the broader CSG. So that was pretty positive.

We also had a bit of a legislative update, but there wasn't too much on NIS 2 to really be adding at that time at the meeting. But that was good.

And this morning we met with the Board. The CSG met with the board. Again, I think there were a lot of people who were there. I know we're sort of short on time. We won't go into it, but we were able to present the issues of concern for us, and we were able to address what we thought were important issues at a high level in the next three to five years for ICANN.

Incidentally, just as an aside, there was today sort of an open session on planning for FY 26 to 30, and there'll be a webinar, I guess, in mid-November. But it was an opportunity to go into a room and sort of do a SWOT analysis and do some recommendations of casting forward, which will help Org actually plan out the next few years. So it was a good session.

STEVE DELBIANCO: Thank you, Tim. And then Marie will be succeeding Tim in this role after the end of the week, right?

TIM SMITH: Yes.

STEVE DELBIANCO: Okay, great.

TIM SMITH: Well, transition. Mid-transition.

STEVE DELBIANCO: Very good. And Tim is staying on the executive committee as well.

TIM SMITH: So, just the last point that I'll make here is the CPH and CSG ExComm lunch for the past few meetings. We've had a meeting with CPH and CSG and weren't able to coordinate the time, but did have a lunch with their leadership yesterday. And that was actually nice to break bread with the CPH. And the hope is that we will have a more formal meeting without beer, I guess, before the next ICANN meeting.

And in trying, while we haven't said it and we haven't discussed it, one of the discussion points was that maybe we should wait till after all of the voting takes place on the RA and the RAA amendments. So that would probably put it into the beginning of January.

And that's that for me.

STEVE DELBIANCO: Thank you, Tim.

And Mason, back to you. Policy calendar is done.

MASON COLE: All right, thank you all. We're a bit behind on time, and Lawrence always gets the shaft in any BC meeting when it's time for the finance and administrative update. Tim will be moving into Lawrence's role, so Tim will start getting the shaft here before too long. But we do have a couple of AOB items to mention. So, Lawrence, I'm sorry, can you proceed through your agenda item as quickly as you can? Final time.

LAWRENCE ROBERTS: Yeah, for the final time, until at least physically. So we have the traditional BC newsletter for ICANN 78 now on the BC's website. Please, you can visit the site. I will be sharing the links with members on the private list, but once you go to ICANNBC.org, you will definitely find links to the newsletter, and it makes for an interesting read.

Aside from that, we have concluded with the BC elections for offices. Our current chair, Mason Cole, is returned as the BC Chair for the coming year, FY 24. We have Steve DelBianco also returned as the vice-chair for policy coordination. We have Tim Smith coming in in the role I currently occupy as the vice-chair for finance and operations, while we have Marie taking up the CSG representative seat for the coming financial year.

We also have our delegates for NomCom seated, and definitely the change of guards is taking place after this particular AGM.

In the last couple of days, we have had to welcome two new members into the BC membership. We now have CleanDNS as a member of the BC. I'm sure we might have run into them in the halls during this particular meeting.

And we also have EWBCD with Steven as the primary representative also seated here. Incidentally, this is our first member in this particular part of the world, and we've been having some discussions on how to help grow our membership in Germany and also accounting for the EU. So to this course, there is a planned outreach for Rwanda, which is ICANN 80. Our BC member, Tola Sogbesan, and Olajide are coordinating this, and we will definitely be sharing more details with members as this progresses or pans out.

We still have a few invoices open for FY 24 and we want to encourage members to quickly work at closing that out in earnest.

We will be sharing details concerning the timelines for BC committee elections in November. Members are encouraged to not only watch out for this, but to also actively participate. This is a means by which we are able to get members to also keep actively being engaged within the BC. More information in these regards will be shared with members, Mason.

Ff there's any question for me, I'll take that. Otherwise I'll yield the floor back to Mason. Thank you.

MASON COLE: Wow, Lawrence, that was a land speed record. Excellent job. All right, thank you very much for that update.

Questions for Lawrence, please?

CHRIS CHAPLOW: Not a question, but I just think a round of applause for the new members and the elected officers. Thank you.

MASON COLE: Thank you, Chris.

LAWRENCE ROBERTS: Sorry, Mason. Just want to also say a big thank you to all the committees that have been actively engaged, especially in my short time as vice-chair. Kudos to the Credentials Committee. (they've done a very wonderful job led by Zak), and also to our Communications Committee, which is headed by Vivek, the Finance, and all of the committees. Just to say thank you because we shook the bridge together.

MASON COLE: Thank you, Lawrence. It's very important, yes. Thank you for the good work for the BC.

All right, we have eight minutes left. I think we have an AOB item with Ching. Would you like to take the floor for your issue?

CHING CHIAO: Thank you, Mason. So this AOB item that I'd just like to bring to your attention is about the CCWG auction policy. I would like to maybe to have our councilors in the council meeting tomorrow or in the next few weeks to keep closer eye on this because I think, for example, yesterday during the GAC GNSO, this item was on the agenda for exchange, but it seems to be pushed back because of the time constraint.

Right now, the key issue I'd like to share is that it seems that, [in] the community that's been working [on] the draft plan and the implementation part, it seems that there's a gap in it. So to put it simply, is that the Board seems to try to kind of tweak around the current ICANN, the IRP, processes. So for the applicant, if the applicant is being rejected, such applicant cannot use the IRP to file any type of independent kind of review.

The drafting team, which I serve as a co-chair, is fine with this, but we asked the Board to amend the bylaw just to make sure that in the future it has a certain type of insulation in case of any legal activities against this grant program. It actually offers the Board a better type of protection. But it seems that right now the Board is trying to use contractual language just to move away from the fix of the bylaw. So we think that's kind of an issue. So I'd like to bring that up. Thank you.

MASON COLE: Thank you, Chang.

Any other follow up for Chang on that issue?

One more AOB issue for Steve. Go ahead, please.

STEVE DELBIANCO: Thanks, Mason. How many of you remember or attended the 2014 NETmundial in Sao Paulo, Brazil?

Mark, Nivaldo, Paulo. Were you both there?

[PAULO ROQUE]: Mark, speak to me, please.

STEVE DELBIANCO: No. Were you there?

[PAULO ROQUE]: Nivaldo was not only was there, but was chairing a bunch of stuff.

STEVE DELBIANCO: Yeah, I bring it up because, ten years later, CGI Brazil, the multistakeholder group in Brazil, is part of a planning group that is likely to do another NETmundial, NETmundial+10. It would occur next April, tightly fit into the calendar as we lead up to the WSIS+20 in the United Nations General Assembly. The NETmundial from 2014 was a two-day, very action-oriented conference managed tightly by the Brazilian government and CGI. And it resulted in a set of pronouncements or resolutions that came out of it. And they were very friendly to the multistakeholder model. And the notion here is that they may do it again.

So this morning, Nivaldo and Mark arranged for Mason and I to meet with the CGI chair and staff to talk about how to bring business into a central role of another NETmundial, should it occur. They are seeking what they call support from the BC, among other business groups. And I believe that Mark and Nivaldo had as their mission for the BC to step forward and say, “Yes, we'd like to participate. We want to help to shape the agenda and to attend,” because this is an event that’s very different than the IGF. It's very different than ICANN. It's an opportunity over two days to come out with some pronouncements that have a balanced view towards protecting users and registrants, a balanced view with regard to the role of business, civil society, technical and governments in multi stakeholder management.

So we attended. I think we made some good progress, and we can report back to the BC after we learn more from CGI on what they want to do next.

MARK DATYSGELD: Yeah, real quick, the development on that is very quick. April is dawning upon us, as you may know, but this is an interesting time to reflect on some of the things that have been going on outside of ICANN. So, GDC and the UNGA is approaching. WSIS+20. There's just a lot of things going on that are very UN-led, and this will be an opportunity to be in a space that's not UN-led, that is actually driven by the community. So we'll be in touch. We'll keep you up to date, and hopefully we'll make a strong presence of the BC in the event. Thank you.

MASON COLE: Thank you, Steve. Thank you, Mark.

Any other business for the BC? We have a couple of minutes left.

Okay, in that case, I will donate those two minutes back to you. Thanks, everyone, for attending. Thank you, Steve Chan, for the support. And the BC has adjourned.

[END OF TRANSCRIPTION]