ICANN78 | AGM – GNSO CSG Membership Session
Sunday, October 22, 2023 – 3:00 to 5:00 HAM

DEVAN REED: Hello and welcome to the CSG membership session. Please note that this session is being recorded and is governed by the ICANN expected standards of behavior.

During this session, question 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 be read aloud during the 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 the Closed Caption button in the Zoom toolbar.

To ensure transparency of participation in ICANN's multi stakeholder model, we ask that you sign into Zoom 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, please stop the recording.

And Mason, go ahead.

MASON COLE: Thank you very much, Devan. Good afternoon, everybody. Welcome to the CSG.

MARGIE MILAM: Next slide, please. Yeah, so, as you guys know me, I'm Margie Milan from Meta. I lead the domain advocacy efforts at Meta and also the domain enforcement litigation programs that are designed to protect our users from fraud, abuse, and brand infringement. And I thought it would be useful to share our perspective as it relates to some information that we've published recently.

Next slide, please. So, in particular, we're going to talk about something called coordinated inauthentic behavior. It's called CIB. It's a type of abuse that we've reported on in our Q2 2023 Adversarial Threat report. We publish these reports on adversarial threats to kind of share our insights into takedowns and what we hope will either further additional investigations or removals of persistent influence operations across the Internet. We also think that sometimes highlighting this information can lead to sanctions or even a higher cost imposed on the threat actors. And by exposing these kinds of threats, security researchers can take a look at it and understand the kinds of scaled defenses that may be needed for some of these threats.

So I'll start with some examples that we shared in the report, two particular threats, one being called the Spamouflage network, and the other doppelganger threat. And then I'll talk a little bit about what kind of work we do to deal with the domain abuse at scale. And then finally, I'll look at some recommendations that we listed in our report, and we'll provide you a link. So if you have any questions, please feel free to see me after the presentation.

Next slide, please. So the reason we published this report is because we think transparency is key to tackling some of these big challenges that are faced collectively online. Our reports focus on industry issues and how we can learn from each other and improve our respective systems and, in the end, keep people safe over the Internet.

Next slide, please. So what is coordinated inauthentic behavior? It's a coordinated effort to manipulate public debate for a strategic goal in which fake accounts are central to the operation. We see people coordinating with one another and using fake accounts to mislead others about who they are and what they are doing. And when Meta investigates these and removes these operations, we really focus on the behavior and not the content. We do what we can to take things off our platforms, but it's a continual effort because we see a lot of what we call persistence, where the networks that we've taken down try to reengage in our platform and continue the harm. So we might actually block malicious domains that are engaged in violating this activity that violates our terms and conditions, but we can only go so far because it doesn't just affect Meta. It affects other organizations as well. And when the domain name is involved, if you take down the content, the domain name can still appear somewhere else. And so that's the persistent nature that we're dealing with.

Next slide, please. So now I'll walk you through some a couple of examples. And if you take a look at the report, it actually has an appendix with all the technical information. So all the nerds and the technical folks can really look at the domain names, look at the URLs, and see the kinds of examples of the things we're dealing with at Meta.

Next slide, please. So Spamouflage is the largest known cross- platform covert influence operation in the world. We saw it hitting our network. It was targeting journalists, and we recently took down thousands of pages and accounts that were part of this large covert influence operation. It targeted more than 50 apps, including Facebook, Instagram, X, YouTube, TikTok, Reddit, and Pinterest. It goes on; large and small platforms. For the first time, we were actually able to tie this activity and confirm that it was part of one operation that we called or it's been called Spamouflage, and it was linked to Chinese law enforcement. The campaign focused on disseminating pro-PRC propaganda, dissident harassment, and meddling with elections. So this is pretty serious stuff.

The operation stemmed from a group of geographically dispersed operators across the internet with different types of content directions. We became aware of the influence after the network targeted an NGO in late 2022. And while we removed the campaign from Facebook and Instagram, many of the accounts on platforms like X, Reddit, TikTok remained online.

In the end, we ended up removing about 7700 Facebook accounts and 954 pages linked to the campaign. And if you take a look at this slide, you'll see the kinds of content that was targeting journalists and trying to influence how these journals were being perceived.

Next slide, please. The next one we report on is Doppelganger, which is the largest and most aggressively persistent campaign disrupted in

Russia since 2017. The goal of Doppelganger was to weaken support for the Ukraine. It expanded beyond its initial targeting of France, Germany, and Ukraine to include the US. And Israel.

And so if you take a look at this particular slide, you'll see we have got on the top the fake site, which was a spoofed article by Doppelganger on WashingtonPost.ltd purporting to show what appears to be a non-existent interview with the Ukraine's president.

Now you take a look at the picture below. That is the actual Washington Post site. So they did a very careful job of trying to mimic the legitimate news organization.

Next slide, please. So now we're here at ICANN. So how do domain names play into the CIB attacks? In that particular report, four out of five covert influence operations in that report ran websites posing as independent news outlets, including a Russian based campaign that spoofed mainstream media organizations. And this was accomplished by deploying typo squatted or cyber squatted domain names that mimicked independent news organizations or even NGOs. So, for example, we identified domain names like WashingtonPost.ltd. Or even NATO.ws. Many others are listed in that appendix, the report. So you can look into that and see what kinds of domain names we identified.

Next slide. Sorry, next one. Okay. At Meta, we have a very wide approach to dealing with brand abuse. We have brand and this type of fraud. We have a multifaceted approach to dealing with this. In order to protect our users from fraud and abuse, we team up with anti-phishing and brand protection vendors to detect abuse and then we address them or remove harmful domains on our particular platform. As part of this process, we do WHOIS requests to investigate and identify the bad actors that are targeting our users. And then if that doesn't lead to resolution, we'll actually mitigate the off-platform abuse through takedown requests, UDRPs, or even legal action. And sometimes in order to address some of this abuse, we're able to establish trusted, notifier relationships with various parties so that we can have swift action.

Next slide, please. So, next slide. So I want to talk a little bit about the scale, just so you guys understand what we're talking about when we're dealing with DNS abuse and why the DNS abuse amendments, while helpful, really can't solve this issue. In 2023, we've reported and removed over 6000 abusive domain names that target the Meta brands. That's a lot of domain names. We mitigated in 2022, 140,000 phishing sites, which was a substantial decrease, actually, from the prior year, which was 265,000 phishing sites. And so when we're trying to protect, obviously, our users from this type of fraud of abuse, we see a lot of challenges. And a lot of it relates in the sense to the ICANN policies and the ICANN contracts.

As I'd mentioned in the prior session, our WHOIS reveals are only successful about 35% of the time, as reported by Tracer AI, who we use to submit our requests. And this limits our ability to identify the bad actors and take swift mitigation steps. UDRPs are costly. They're thousands of dollars. And so if you think about thousands of dollars for a UDRP, it's not really a solution when you've got 6000 abusive domain names, it just doesn't work. And UDRPs are slow and can't keep up with the volume of abuse that we see. Litigation is another avenue that we've pursued to protect people from abuse, but that also is costly, slow, and unable to meet the scale of abuse.

Next slide, please.

STEVE DELBIANCO: Marge, I just want to stop before you moved off of that slide. The statistics.

MARGIE MILAM: Can you go back to this slide before, please?

STEVE DELBIANCO: And in particular, on the RDRS that we've been working on, staff has put together these nice posters, and in it they talk about the requester community. The spectrum is consumer protection advocate, a cybersecurity investigator, government officials, intellectual property professionals, and law enforcement authorities. And what I wanted to stop and point out is that that might be an intellectual property lawyer who's doing the work, but it's not about protecting a trademark, right? It's trying to protect 140,000 instances to defraud Facebook and Instagram users into giving information that can be used to defraud them further. Right?

So it isn't consumer protection advocate, it's not law enforcement, and it's really not an IP professional and [trade market]. We were calling it protecting customers, right? And I think you understand that. So more often than not, an IP driven query or RDRS request is all about protecting customers from being defrauded.

And I realize it's not appropriate maybe to change the slides that we do, but I wanted you to understand firsthand what we mean by using RDRS to try to track down fraud of the customers. Thanks.

MARGIE MILAM: Thank you, Steve.

Next slide, please. So as we think about this, our experience is not unique. I think this is the point I want to drive, and perhaps some of the brand holders here in the room can probably echo the scale of abuse that they see. We're just out here trying to shed light on it so that there can be a wholesome discussion on some of the policy recommendations and solutions that could possibly address this.

Next slide. So transparency and cross-society responses are key to tackling these malicious efforts to manipulate public debate. Solutions are needed both at ICANN, but actually outside of ICANN as well, unfortunately, because some of this is outside of ICANN's remit. Tech platforms, researchers, media and government entities, and even domain registrars and regulators all have a unique but limited view into the individual elements of these deceptive campaigns. We encourage solutions to be explored at ICANN for better domain policies and contracts to address this. But there's also solutions that may be needed outside of ICANN to address some of the gaps in policies or regulatory framework. So, for example, hosting providers are outside the remit of ICANN, but they actually play a key role in some of these CIB attacks.

Next slide, please. So if you're interested in some of our recommendations (I won't go through all of them), they are in the threat report that's in the link in the slides. And we really gave some thought to trying to identify what kind of enforcement and policy recommendations could address this at scale. We hope these recommendations can focus discussions at the right venues and to lead to timely solutions to protect the public from this type of coordinated inauthentic behavior fraud and other types of abuse.

Next slide, please. So this addresses some of the things we talked about earlier at ICANN. We do think it's important to improve the contracts with registries and registrars to take proactive steps to address domain registration abuse at scale. Some examples of what this could look like is requiring suspension of customer accounts for known bad actors and imposing additional verification for domain names that include a combination of a famous brand plus a word that is suggestive of fraud like “login,” “password,” “security,” or, “help center.” We see those kind of combinations all the time as we're trying to protect our users from abuse. We also think that updating the UDRP to disincentivize cyber-squatting might be a good idea, because right now, the UDRP is just not any kind of disincentive because it takes so long. And in the end, the only remedy is to transfer the domain name from the bad actor over to the brand holder.

Outside of ICANN, it may require adopting laws that require accurate, complete, verified WHOIS similar to the NIS 2 directive. We think that that was a really solid step in the right direction. And I won't go into what NIS 2 covers, but I think many in the room do. And also, we think it may be important to incentivize cooperation with those that are investigating impersonation attacks at scale. So there needs to be incentives for cooperation. And then, similar to what I mentioned at

ICANN, we need to disincentivize cyber- squatting by shifting the costs from the brand holders to abusive actors or by enhancing the remedies and damages that are available under applicable law.

So these are just a couple of the examples of things that we've identified as things that could help address the issue at scale.

Next slide, please. There's other considerations. Obviously, we want to make sure that we need to account for legitimate criticisms and make sure that any solutions are tailored to prevent powerful players from abusing the rules to silence lawful protests. So we're very mindful of that and suggest that businesses and UN entities would need to adopt remedy and risk management approaches to be consistent with the guiding principles on business and human rights.

And then the last slide. I've provided a link to both our blog and the Adversarial Threat Report. I'd be happy to take questions here or after in the hallways because as you can tell, it's very important to Meta to share this information and to talk about potential solutions. Thank you.

MASON COLE: Thank you. Margie.

Questions for Margie, please?

[Gabe]?

[GABE]: So, Margie, I think from what I saw, especially regarding the impersonation sites that impersonated your small and independent media, from what I think what I heard you say, most of those impersonation sites involved domains that were maliciously registered lookalike domains; homoglyphs, in other words. And I just want to confirm with you that you mostly saw the malicious registrations then, as opposed to, for example, other sites that were compromised by them, used to host that?

MARGIE MILAM: I haven't gone through the entire list of domain names, but we did see a lot of that. There were also URLs separate from the domain names themselves. But because we're here at ICANN, focusing on the domain name aspect as it relates to the type of squats, the cyber-squatting, that in the end is used for these impersonation attacks.

MASON COLE: Okay, Steve and then Brian.

STEVE DELBIANCO: And Damon.

I put this into the chat, but in the BC's comments on the DNS abuse contract amendments and advisories, we specifically said in the advisories that ICANN Compliance puts out that tactics like you just exposed that are happening and ramping up are perfect for ICANN Compliance to be issuing an advisory to all of its registrars and registries., so they're alert to the concern, and maybe even suggesting a few mitigation techniques that they can take. I don't see anyone from Compliance in the room, but we're going to want to share that with them. And I realize they're not focusing on the advisory until they get the DNS abuse amendments approved.

But this would have been something that's probably inappropriate to jam into the contract amendments too hard to get that done, and they would be out of date the minute they're finished. But dynamic, evolving tactics that criminals are using is perfect for ICANN to be pushing out advisories.

So let's all continue to work with Compliance and tell them to update the advisories to reflect the latest work of the bad actors.

MARGIE MILAM: I think Crystal's point about the advisories was spot-on. I mean, nobody wants to push contract amendments if there's ways to solve it elsewhere.

But I do note that in the example we're talking about here (coordinated inauthentic behavior), it doesn't even fall into the definition of DNS abuse. So that's part of the problem. So I can't imagine ICANN doing an advisory on something like that because it's not part of the definition. But I think it's the kind of problem that just highlights why the definition is perhaps narrower than it needs to be or we need to find solutions in another way.

MASON COLE: Okay. Thank you, Steve.

Hold on, we got a queue building. So Brian, Damon, John, and Crystal.

BRIAN KING: And following my previous comment, it's not just Margie on this either. I can tell you from working for several brand protection companies that the average customer of ours would be tracking definitely over a thousand unique domain names that were infringing phishing domains at any given time. A Florida orange juice company grower had over 100 domain names tracking at a time. So this isn't just an Internet company problem. It's not just a Meta problem. That scale exists across industries for everybody.

MASON COLE: We are over to Damon now, please.

DAMON ASHCRAFT: Margie, great presentation. I'm sort of curious. You had mentioned changes to the UDRP. There's probably a lot that Meta would like to see done, but could you just sort of share with us maybe your top one or two changes that you'd like to see to the UDRP, please?

MARGIE MILAM: Great question. Obviously, a lot of brand owners will know this. It's very difficult to even know who the owner of the domain name is. To be able to get a WHOIS reveal before you file your UDRP is one. And typically you also don't know how many other domain names that particular account has that's infringing on your brand. So to be able to get a list of all of the other domain names that are associated (at least that infringe on your brand; I mean, you could limit it to that) would at least enable you to do one UDRP covering, whatever, 1,100 or however many there are, as opposed to accidentally filing multiple against the same person. And then an ability to suspend a domain name for DNS abuse during the pendency of the UDRP would also be one if there was some ability to do that as opposed to waiting till the three months passes.

DAMON ASHCRAFT: Thank you.

MASON COLE: Good. Okay, John, I got to skip you and go to Crystal. She's going to leave. Crystal, go ahead.

CRYSTAL ONDO: Thanks. Crystal from Google. One thing. The UDRP question. There is the URS, which you can do at the registry level, that is cheaper and slightly easier to deal with. So I know that doesn't mean you get the domain at the end, but to take down problematic things, just consider going to the registry for that.

What I was going to say is registrars have been doing a better job of talking about coordinated attacks that they are seeing. I have not seen this, I think, because it's content, right? There's going to be some pushback. But registrars typically are more open these days to hearing about what you're seeing and then coordinating amongst themselves. We've seen really a lot of bad things happening recently specific to phishing and fraud and these things. But I think there is an avenue of communication to be had with at least the large registrars that come to these meetings, get in front of them, do this presentation. A lot of them will do the right thing and take down entire accounts. They don't want this kind of stuff on their platforms, especially the bigger players.

So I think not only educating this group about these things, but educating the registrars would be really helpful and actually resolve things in a quicker way than going about PDPs and all these things. If you're seeing something happening now that's different than what is happening, bring it to them and talk to them about it.

MASON COLE: Okay. John?

JOHN MCELWAINE: Margie, with the CIB attacks that you're describing, it looks like sometimes there's going to be a third party's brand that is really being the result of the unlawful behavior that you're seeing and needing to investigate. I presume you've had some success, probably limited, in getting some direct registrar compliance to turn over some of the records, maybe none. It's an unusual situation, but I think we might want to (and I don't know if you know; I don't and I'm on the small team) [do is find out] whether the new RDRS system would have the information field for you to be able to make that type of request to even have it considered. And that might be something that we can hear about in the next session. But I don't know if you could talk a little bit about that topic of having to utilize a third party's brand to complain about unlawful behavior. Thanks.

MARGIE MILAM: It's hard to get things taken down for your own brand and then for us to go and ask for something to be taken off, that's a [news organization …] You really need the brand owners to do that. And if it's a domain name that isn't our brand, we're less likely to get the WHOIS information. I mean, it's difficult anyways, but it would be even more hard for me to say who registered WashingtonPost.ltd. They're going to say, why would we give you that information?

So it's this really difficult problem of investigating. And then some of the news organizations are very small. They don't have the resources to deal with this. So that's the persistent nature of this. Those domain names stay up, they just keep coming at us and we see the network continuing against us and other platforms.

MASON COLE: Hang on, Michael, we got a queue. Jan and then Vivek and then Michael. Jan, go ahead.

JAN JANSSEN: Thank you, Mason. Margie, there was one of the slides which showed a substantial decrease in some of the illegal activity, and I was just wondering whether you have any intelligence to put those figures into perspective, because I can imagine rhetoric saying, like, you see, there's a decrease. But on the other side there are a lot of efforts that your company has been taken to make sure that illegal behavior is addressed. So that could be part of the reason. You can have seasonal events like elections going up where you see an increase in illegal activity trying to influence people. You can have other platforms that are more lenient towards certain behavior where you could see a shift in criminal activity.

So I was just wondering, is there any intelligence that you can share to put those figures into perspective? Because otherwise I can really hear other people of this community try to create a different rhetoric.

MARGIE MILAM: It's hard to figure out why the significant drop. We spent a lot of resources in those years to move quicker, faster, against this types of fraud and deployed that kind of like multilevel strategy of all the things that I shared on the slide, including leading litigation. So I think that some of the litigation plus increased attention to the issue was part of why it dropped. But we don't have specific explanations yet as to why it was so significant.

MASON COLE: Vivek?

VIVEK GOYAL: Thank you. Vivek Goyal, a member of the BC. I think what we are seeing is just tip of the iceberg when it comes to DNS abuse. In India, there are about 800 million people who are accessing the Internet, many of them for the first time, and many of them are doing it in their regional languages. So if we think that we are getting very good at capturing abuse in say, Latin alphabets, think about when people actually start using IDNs. And there is a whole mass of abuse going on, especially for people who are using the Internet for the first time. So these are people who believe that a Saudi prince wants their help to move gold. It's their duty to help them. They are not experienced in that. So a lot of companies and brands are trying to get people to access them in a regional language. I know Meta has a large push in India to produce content on regional language to make it popular. So does every other brand. And we will see such a large scale of DNS abuse that this will seem like pocket change. Thank you.

MASON COLE: Thank you, Vivek.

Michael?

MICHAEL [FLEMMING]: Real quick. Going on with the topic of being able to identify registrants of a number of different domain names and have registrars or registries go after them, a fundamental issue for us, and I think for all of us in both CIB and consumer fraud is the accuracy of the records given to and accepted by the registrars and registries. Whether or not those organizations or individuals are carrying out these programs, they know they're going to be looked for and they know right up front that if they take on a false face, they aren't going to be found. There won't be any sort of way to reach them for any of the disincentives or anything else that we may come after them, which is a real problem.

And another thing. While you were talking (I know we're all aware of this), the UDRP review that's upcoming essential that we have not only a voice, but begin and pull together the information and the data that we have on these problems so that when we're met with a “Oh, that's a problem of content, not domain names," we can point out that it is a problem of domain names. Content is irrelevant in a lot of ways and it's how that content is reached through the domain names, through the fraudulent name that's being used. So I think it's important that we keep our eye on that prize, however it's coming along in the next year.

MASON COLE: Thank you, Michael.

I think that—oh, I'm sorry, did I miss somebody? Oh yeah, please go ahead.

UNIDENTIFIED MALE: I'll try to be short. [inaudible] they come from Serbia. Serbia has a very large percentage of the population that uses Facebook, and Facebook is the most used vector for the attacks when DNS abuse is concerned. Basically a lot of users are affected and Facebook is very bad at seeing those views.

My personal experience (I wear too many hats to say everything, so we'll talk later) is basically I see ads on Facebook that say, "BestNikeOutlet.com. Great prices!" [which connect their phishing cards] and so on, and they report it. And what were the results? None of my report was ever acknowledged.

And it's not just that. The algorithm then considers, "Oh, you're interested in that?" Then the result is I get more commercials for the fake websites on the fake domains. And if I want to track them, it's very easy. I just report it and then I will get all the ads because it obviously comes from the same threat actor that's using the same ad delivery options. And then I get a bunch of redirections to the domains that are just misuses of the names and different variants that will trigger people thinking it's a valid website.

And I think the other problem is that we in Serbia cannot connect to Facebook, to anybody from Facebook, to report this. And as previously said, it is very important.

How do you come to this content? And people are not aware that they come to the website. They are coming to Facebook because they see it on Facebook. They click on Facebook. It opens in the Facebook browser. For them, it's all Facebook.

And in terms of general prevention, that can be done, you are the great gateway to stopping them. Great. In Serbia, you can cut a lot of it, and there is a lot. If you talk to the banks (I talked to one on Friday), they say it's terrible. The number of credit cards stolen through this is terrible.

So basically I understand the problems between the domain registry with the registries' and registrars' notification and so on, but we need to stop it at the front with the users also because we need to break the chain in all the links, not just at the registration of the domain but at the content delivery and all other points of contact with the end user. Thank you.

MARGIE MILAM: There's actually reports as part of these transparency reports. We also have reports on how we take things down those types of things. I'd be happy to share a link to it and answer any questions you may have about that. Thank you.

MASON COLE: Okay, thank you.

I think we need to cut the queue there to conclude our agenda. So, Margie, thank you very much. Very helpful presentation. You got a lot of comments, a lot of questions. That was great. Okay, thank you all very much.

All right. Okay. Devan's way ahead of me. She has the agenda back up. All right, we're going to go back to item number three, which is a quick readout of what happened on day zero when the CPH leadership and NCPH leadership had an intercessional meeting, ostensibly to improve our relationship and find common ways to work together and identify common priorities. And I would say, on the whole, it was a successful day.

Philippe is going to lead us in a quick discussion on that. Philippe?

PHILIPPE FOUQUART: Thanks, Mason. This is Philippa Fouquart speaking. ISPCP Chair. Yes, we thought that for the benefit of the whole membership, it'd be worthwhile having a discussion with everyone here on what happened on Thursday, I think it was, during our day zero. I think there was some recognition across the two stakeholder groups that we would benefit into in having more discussions, and we discussed the practicalities of doing that.

So we agreed on the principle of having an annual day meeting, probably back to back with the ICANN meeting, as well as a dedicated session, probably two hour session, in the other ICANN meetings, as well as other details, I would say, but just as important, having a wiki space that most of us were unaware of and has existed for about, I don't know, four or eight years probably. And we'll have liaisons between the two groups. We discussed a number of ways (mailing lists, et cetera) in which we can cooperate on the substance that I'll be going through very quickly, but also hopefully on things like coordination at council, which for years has been … I wouldn't say lacking, because there's been some discussions, but there's certainly room for improvement in terms of at least sharing information.

I think we've identified a number of areas of agreement, and I wouldn't go through the list, but I think there's some agreement on approaching the issue of NomCom rebalancing with the notion of looking outside rather than inside—shall I put it this way?—i.e., not making it a BC versus NPOC debate, but rather discuss the overall slate or distribution of NomCom seats across the ICANN SO/Acs.

And more on the substance, there were two things that we discussed extensively. There's a recognition that there's, to say the least, room for improvement on our Seat 14 appointment procedure. No one wants to go through the trauma that we went through this year, and I think there's some recognition that revealing the name only a few weeks before the AGM is just evidence that the procedure is broken by definition, even though we can certainly build on the existing procedure to develop a new one. We discussed the various options to do that, whether relying on the expected appointments by NomCom or having some sort of voting procedure to do this.

And I should have started by saying that during day zero, we [were helped] by Paul McGrady very efficiently, who will also be chairing the small team on this particular topic, as well as on the vice-chair appointment.

The Small Team will be tasked with coming up with improvement to the procedure of appointing Seat 14, with helping with the onboarding of our new director, as well as coming up with a common understanding on the appointment of the vice chair.

And we will work, hopefully between now and March and come up as a result. The idea is certainly to do this now, at the very beginning of the term by Chris, rather than considering that there might be second thoughts in the way we develop the procedure. So I think that's very timely.

So I think, Mason, I'll stop here to see whether there are any comments. Hopefully I've covered the gist of our discussions. Thank you.

MASON COLE: Thank you very much, Philippe, for that report.

Before I go to you, Damon, Paul is here with us. And you're right, Paul very ably led that session and got us through the day into a successful conclusion. Paul, is there anything you'd like to add to Philippe's intervention?

PAUL MCGRADY: No, other than we're euphemistically calling it Team 14 to try to solve that problem and some of the other ones. I think that the leadership from both sides of the house are going to get together and talk about how that's going to be staffed. So there's quite a bit of homework for your leadership team.

There was also an outputs link that Andrea, I think, created, which is helpful.

But my main motivation for doing the Team 14 is just that I don't want to do another one of the other things we did this summer, which was very painful.

MASON COLE: Nobody does. Okay. Damon?

DAMON ASHCRAFT: I think one of the things that was really positive that came out of those meetings was we've always had this dispute as to what did we agree upon, and we discussed that, and there was that Wiki page that came up. And I would suggest the next time we have any type of agreement that we quickly reach out to the other side, maybe send them a draft email, say, This is what we're going to publish. Let us know if you have any objections," and then we publish it. We really need to start using that. And to the extent that if we're sitting here two years from now saying we don't remember our agreement and we disagree on it and we didn't do it, well, that's going to be on us. So I would say we really should start using that. And there was no pushback on that Wiki page,

	and I think actually they reminded us that it existed. So that was a real positive, I thought.
	And thank you, Paul. Great job.
MASON COLE:	Mark?
MARK DATYSGELD:	I want to follow up on Damon exactly on the Wiki aspect. I think it was fairly consensual that we actually start documenting decisions and discussions and actually centralizing those, and I suggest we start making use of that right away. Why wait, since it was agreed upon? So for any further moves that we make and anything that develops around that, let's start collecting that data and start ending this fields. And this can be even in relation to other things that do not relate to these bilateral negotiations over things. Anything that we actually reach some sort of consensus on let's start documenting because clearly the historical memory in this institution is very flawed. Things get lost very quick, and if we adopt that as a standard, we might be saving ourselves a lot of pain further down the road. So since this was agreed upon by both sides, why not use it right away? Thank you.
MASON COLE:	Thank you, Mark.
	Any other follow up on this issue, please?

Okay. I don't see any hands. All right, we have one remaining agenda item. Philippe, the floor is yours again for a discussion, a quick discussion, on what's happening in the EU Legislatively.

PHILIPPE FOUQUART: Thanks, Mason. [Well, mine sort of] because I'll put this to Thomas very quickly just to give us probably an update on … Maybe I should backtrack a bit. This agenda item came at a point where we were discussing the outreach of the ISPCP, and that was part of the outreach. Since then the discussion led to a Day zero on NIS 2 as well as a separate outreach for the ISPCP.

So what we thought we would do would be for you to have a summary of that day zero on NIS 2 and what were the main issues that were discussed there, especially for those like us who were at the day zero for the NCPH to benefit from.

So over to you, Thomas.

THOMAS RICKERT: Thanks so much. And Philippe just offered an explanation why I wasn't there for the day zero because we had one running in parallel and some of you have been in the room (Steve, for example). We were sort of crazy spending 8 hours on one article of NIS 2. And certainly, as you can imagine, there were no tangible results, which was not to be expected.

As you know, this is a directive that needs to be transposed into national law. There is a coordination group between member states that has formed to discuss implications of NIS 2 and facilitate the transposition at the national level. This group has also formed two task forces, one dealing with the question of validation, the other one dealing with the question of legitimate access seekers.

And what we did during that day is we heard from Gemma Carolillo from the European Commission. She gave an overview of what Article 28 entails. One of her colleagues gave a general overview of what NIS 2 requires of operators falling under it to put everything in perspective, because for many operators there's much more to be observed than only Article 28. Then we got updates from several jurisdictions on their deliberations between ministries and the industry and what obstacles they have found to be particularly relevant for the discussions because let's not forget that the due date for the transposition is October 23 and there's no grace period for the industry to implement the requirements. For those who are critical or who are essential or … what's the other term? It's been a long day. So for those who have to fulfill more requirements, there will be some implementation required, and the implementation guidance will be issued by the Commission only in October 23. So there's virtually no time left.

So we heard from the national deliberations, then we heard from [Elena]. She reported on ICANN’s role in this because NIS 2 actually makes reference to global multistakeholder organizations whose policies should be taken into account and how that fits in with what ICANN does. And we are appreciative of the European Commission actually having made reference indirectly—I mean, they can't mention a specific organization, but for indirectly mentioning ICANN. Then we heard from various panelists on the role of registration data in mitigating DNS abuse.

So NIS 2 mentions DNS abuse without offering a definition, and it shall obviously serve the purpose of helping in the fight against DNS abuse. But we wanted to put that in perspective, not diminishing the role of registration data. But we do know that, for example, PIR does not use any PII in their abuse mitigation. So do others like CleanDNS or iQ, offering commercial platforms that help mitigate DNS abuse. And we just wanted to explain that that the expectation should not be such that if only we had fully validated registration data, the problems would be solved or halfway solved. It's one part of the fight, one piece of the puzzle, that is important, yet should be realistically considered.

After that, we had a pretty exhaustive discussion, talking about operational challenges that the industry sees. How do we deal with existing domain name registrations with millions of data sets that may or may not need to be validated and how can a risk-based approach can be operationalized?

Again, the question of legal versus natural came up again. NIS 2 now gives operators a legal basis for publishing the data of legal entities, but most registries did not create these two buckets historically, so they can't easily discern natural persons data from that of legal entities.

And then you have the additional layer of complexity when it comes to email addresses, where NIS 2 says it must not be published if there's personal data involved in the email address, but how do you find out whether there's personal data in an email address provided for a legal entity? And that's not to say that no work should be done in that area, but it's just to show that we might need to make a distinction between new registrations, where you can ask the registrant to tick a box ("I'm a legal entity") and then you can easily, relatively easily, implement that. But that's not true for legacy data.

Also, how to conduct the verification? We've heard examples on how cc's do that, but that doesn't easily translate into the g world.

And many others here. I don't want to bore you with details, but we wanted to make sure that we're all on the same page in terms of what this entails. And I think we saw Gemma taking notes almost nonstop. She also offered some responses. And we think it's important that this information trickles down for the EC. Certainly the train left the station, but for those who have to transpose that into national law, it's important that they have this information.

The next step for us is that whilst we had great turnout, there were like 150 people in the room. Not everyone was there who wanted to be there. So we have a recording, and we also had somebody with us who took notes. And this poor individual, Kate, will produce a report, and that is going to be shared with all of you, including the commission and the coordination group.

And we do hope that we have a communications channel open. Whilst Gemma and her colleagues have been confronted with a lot of questions, I made it very clear for everyone that we don't want this to be an interrogation type thing where she has to justify what they did, but that she has an opportunity to respond whenever she feels like. And actually, there were a few moments during the day where she asked for the floor to offer responses, which I think was great. I mean, she exclusively came to Hamburg for this day. And I think that's a great testimony of her willingness to listen and to work with us. And I think we should utilize this communications channel in the months to come in order to hopefully get something that everyone can work with and that serves the purpose of what Article 28 shall achieve.

So I think I should leave it there. I see that Steve wants to get in and also Mason, so go ahead.

MASON COLE: All right. Thank you, Thomas. Steve?

STEVE DELBIANCO: Thanks, Thomas. A compliment and a question. Well-organized and executed event. Very well done, and especially because so many of us were suffering from severe jet lag. But you kept it going. And part of that was the interaction between the European Commission, a couple of member states, and the registrars in the room, many from Europe, many small. And after the brief report from ICANN, at the beginning of the afternoon, ICANN wasn't mentioned again for the rest of the day.

My question for you is, what is the role of ICANN at solving the tremendous problems that the registrars and registries in the room had (verification at multiple levels, duplication of efforts in terms of maintenance or collection verification)? They were very concerned and were expressing that to the commission. The commission reacted just as strongly before Gemma left the room to catch her flight. And it was your organized event. I'd be interested in what you think ICANN should do, since we're here at an ICANN meeting, to follow up on specifically the afternoon.

THOMAS RICKERT: Well, I think I need to offer a little bit of background. I think that in the cc world, we see a couple of examples of validation processes and policies in place that are pretty strict. We've heard about that. And others are cognizant of the fact that they need to do more in order to address the challenges of Article 28. And then we heard, particularly from the Registrar Stakeholder Group that they are of the opinion that we have pretty much everything in place that needs to be done.

And I think that ICANN Org, maybe with our help, needs to communicate more. I mean, we've seen the letter that Elena has produced, but that's basically an inventory of the policies that are in place without speaking to the genesis of those. We had a discussion between law enforcement, the GAC, and other parts of the community that led to the compromise that went into the RAA 2013 and also to discuss[ed] where the shortcomings are potentially, but also where the contracted parties think that it's ready for primetime. And I think that we need to put things into context.

To be quite honest, I did not expect ICANN to play a stronger role during the discussion yesterday. I think that Elena just wanted to speak about the role that ICANN has and have more of a bird's eye perspective. But we certainly at eco think about next steps. And I think while we heard a lot about sometimes glorious detail on how some parties think they can operationalize this, we don't yet have the bird's eye perspective view on how conceptually we make all this work between registries, registrars, resellers, privacy, proxy service providers. Everyone seems to be thinking in their own silos.

And let's not forget, we have the four big tasks in Article 28: maintenance of the database verification, publication of data, and responding to disclosure requests. Everyone in the value chain is responsible legally for having everything delivered. But not everyone should be doing everything, because that would be crazy for everyone to do the same thing. But we don't have any arrangements in place so far on how to share the responsibility, how to maybe audit or enforce if your partner doesn't do the right thing. Let's say the registry says they're going to do the validation centrally, and if they just don't do it and you get issues because of that, how do you deal with that? Do we need to audit? Do you do a self-assessment? Do you do a third party certification of whether something is okay if you want to take a risk-based approach, is your appetite for risk the same as the appetite that others might have in this game? How do we hopefully make the cc and the g world talk together so that a customer doesn't have to undergo multiple processes if they are just stupid enough to put different TLD domain names into their shopping cart? All those things have not really been discussed. I mean, the ideas … DENIC, for example, is socializing its own approach in a series of meetings during this week, which is great, and they say, well, others can follow. But even if they did, that would just be an insular solution for the cc world, and that would not help for the g world.

I mean, that's been a long response, but I think that there's more work to be done. Whether ICAN has a role to play in that, I'm not exactly sure, but I think that needs to be discussed.

MASON COLE: Okay, good question, Steve. Thank you, Thomas, for the answer.

We have two in the queue, and then we're going to cut it because we're almost at time. So first Philippe and then Chris. Philippe?

PHILIPPE FOUQUART: Thanks, Mason. Well, you partially addressed the question, my question was essentially about the coordination with the cc's. Some of them have put together coordination nationally, more about Article 28 probably, but certainly from a registrar's perspective, but other players as well. There's not going to be two solutions but a single one. So I'd be interested in hearing about how that coordination might happen and as you put it, very quickly. Thanks.

THOMAS RICKERT: So we have decided today (we had a meeting with a couple of our members) that we're going to put together a Team 28 which is going to do two things. One is to make sure that we keep informing folks about how to transpose, and the other one is to talk about the coordination between the various players on how to conceptualize and operationalize this. And ideally, the regulation wouldn't ask for all the detail. That should be technology-agnostic whilst we need all that detail in coordinating with each other.

But the problem for us is Article 28 is not the biggest concern for the lawmakers. They find themselves with NIS 2 which basically could make everyone, every homeowner with a solar panel, an energy plant in a critical infrastructure. Those are the things that they are worried about.

MASON COLE: Chris. Yeah?

CHRIS LEWIS-EVANS: Thanks, Mason. Sir Chris Lewis Evans. Just to go to Steve's question, what can ICANN do? I think we heard on the thing for people that weren't there that as long as it allows it, I don't think ICANN are going to get into the verification side. There's good examples from cc's.

I think the only thing that ICANN can do is the flag that we discussed in part of the RDRS discussion around legal versus natural. That's an organization ticking that box and pushing that flag forward. I think that's the only thing that ICANN can do or maybe we can get them to do. So maybe it's worth just repushing that. I can't remember where we got to on that.

MASON COLE: Margie, sorry, go ahead.

MARGIE MILAM: I've taken a look at the comparison between NIS 2 and the policy. I think there's a lot more ICANN can do, honestly. I think it's another temporary spec that aligns the WHOIS policy with NIS 2 [With] things like the Thick WHOIS is requirement, under NIS 2 you have to get the registrar to be obligated to send their information to the registry. That's a policy issue that could be addressed.

The legal/natural is another example of the kind of thing that you need. The industry can try to do it piecemeal, but I don't see how it'll really scale. The way you get to the scale is by working here in the community, getting a new temp spec, and updating it to be aligned with NIS 2. And then you have a global policy that addresses the whole world and there's no need for any further regulation with that respect.

MASON COLE: You got like 30 seconds, Thomas. Then they're going to throw us out.

THOMAS RICKERT: Just to say that, Margie, we agree on a lot of things, but I guess this is not one of those, and it would warrant much more discussion. We're here at ICANN, and some governments are very unhappy with the European Commission having regulated something that they intentionally did not regulate to leave space for ICANN. And if we now did something to honor exactly what the commission asked for, we would need to do the same thing in order to honor other regulators wishes. And I think that the registration data policy has the flexibility for the contracted parties to do things beyond what we have there have in there to address NIS 2. And therefore, I think an EPDP is not required.

But to be continued, I'm sure.

MASON COLE: Very much to be continued for the course of the next year and a day, right?

All right, everybody, we don't have time for AOB. I didn't see anything come up for AOB anyway. So thank you all for coming. It was a long 2 hours, but we got a lot done. CSG is adjourned.

[END OF TRANSCRIPTION]