PANAMA - Cross-Community Session: WHOIS/RDS Policy: Post-GDPR Development and Next Steps
Tuesday, June 26, 2018 - 15:15 to 16:45 EST
ICANN62 | Panama City, Panama

BRIAN WINTERFELDT: All right, everyone. Good afternoon. Welcome to this cross-community session on WHOIS or RDDS policy focusing on post GDPR developments and moving forward with RDDS policy development in this post GDPR world. My name is Brian Winterfeldt. I am president of the Intellectual Property Constituency, and I'm here today in my neutral capacity as moderator of this cross-community discussion.

As everyone in the room is well aware, European General Data Protection Regulation, or GDPR, has precipitated significant changes to the registration data service, currently known as WHOIS. Most recently on May 17th of this year, the ICANN Board adopted a temporary specification that went into effect on May 25th, the effective date of GDPR, implementing an interim GDPR compliance model for WHOIS.

However, the temporary specification can only be in effect for up to one year per the terms of the Registry Agreement and Registrar Accreditation Agreement, and its adoption triggered an expedited policy development process, or EPDP, to create a new ICANN consensus policy concerning gTLD registration data directory services to replace the temporary specification.

The EPDP has been the subject of much discussion already during this meeting, and I'm sure we're going to be continuing to discuss it. And we will be dedicating a portion of today's panel to talk about the work at the GNSO Council to scope and draft a charter for this EPDP.

This is going to require a significant community effort as attempts over the years to reach community consensus regarding updating the WHOIS system has historically been rife with challenges, shall we say. With the adoption of the temporary specification and the launch of the EPDP, the community has a new opportunity with specific milestones to try to devise an alternate model for a next-generation registration data directory service that meets the needs of various stakeholders with legitimate interests in domain name registration data while also respecting applicable privacy and data protection laws. This will be in many ways an important test of the ICANN multistakeholder model.

With that, I'm very honored to facilitate today's cross-community discussion. In this session we hope to engage with the community to discuss the impact of GDPR, key policy changes resulting from the temporary specification, and how to move forward with developing a final consensus policy that moves beyond the temporary specification toward a more permanent solution for the RDDS.

Following this session, we'll have a second cross-community session specifically focusing on accreditation or authentication and access to nonpublic WHOIS data. We ask our panelists and community participants to try and limit the discussion in this section to the temporary specification, the EPDP, and suggestions about the policy process since there's going to be a whole subsequent session on access and accreditation later this evening.

With that quick overview, I want to quickly introduce our panelists today. First I'd like to introduce Ben Wallis who is a regulatory policy analyst with Microsoft. Ben has been integral in Microsoft's efforts concerning GDPR compliance and related policy issues, including the impact of GDPR on Microsoft's platform and cybersecurity practices.

I'd like to also introduce Susan Kawaguchi, a long-time volunteer at ICANN who is currently serving on the generic names services organization or GNSO Council at ICANN as a representative of the business constituency. Susan previously chaired the ICANN Policy Development Process Working Group on registration directory services and prior to that was a member of the Expert Working Group on WHOIS.

Susan is currently a consultant with Aptitex (phonetic), and before that she head roles as head of domains at Facebook and eBay.

I'm also pleased to introduce Stephanie Perrin who is a data protection expert and the president of Digital Discretion, a privacy consulting firm. She's been an ICANN volunteer since 2013 and currently serves on the GNSO Council and as a representative of the Noncommercial Stakeholder Group.

Elliot Noss is president and CEO of Tucows, Inc., and is here representing the Registrar Stakeholder Group. Elliot has been a leader in the Internet industry for over a decade. He champions areas of vital interest to the service providers and Internet users, including privacy, ICANN reform in registrar matters, and the implications of emerging technologies.

I'm also pleased to introduce Laureen Kapin who is counsel for International Consumer Protection at the Federal Trade Commission in the United States, the leading consumer protection and privacy enforcement agency there.

She also serves as co-chair of the GAC's Public Safety Working Group.

And last but absolutely not least we are joined by Goran Marby, ICANN CEO, and John Jeffrey, ICANN General Counsel.

Today's session will primarily be a question-and-answer format where we'll be asking various questions to our panelists. I'll direct some of the questions to specific panelists, but there's a chance for other panelists to jump in. There's also a chance for audience participation. If the audience has questions, there should be folks with roving mics who will be able to help facilitate that.

So with that introduction, I think we might go ahead and jump into our first question.

The first question I'm going to direct to Susan Kawaguchi.

Susan, what have we experienced and what have we learned so far with regard to the current environment a month after GDPR has gone into effect?

SUSAN KAWAGUCHI: Thank you, Brian, and that's a good question. Unfortunately, we're seeing a diverse response to the GDPR. I probably looked at over 200 WHOIS records last week in prep for the meeting, and to see what, you know -- what was going on and which registrars were doing what.

It was a varied response. There are definitely redacted registrations, and -- and appropriate, probably, to comply with the temp spec, provide country, registrant, org if that was provided to the registrar. And -- what is it? City. I'm always focused on the country. Definitely when I have seen anything remotely close to Europe, those are redacted records. If you see -- if you go to a third party not directly to the registrar, sometimes you'll see a redacted record, but then go to that registrar, and if it's in the U.S. or within specific countries, you would get the full WHOIS record. So my experience was I was still getting about one-third of the records based on geographic location. For some reason, Venezuela seems to be thrown in with the EU on this. I'm not sure why. And -- I just saw several of those for Venezuela fully redacted at the registrar, which I thought was interesting. Don't know Venezuela law, but...

The other problem that I'm seeing, though, is there's a variety in how the redacted data is treated, and to me it caused a lot of confusion as to is this a privacy/proxy service registration? Is this redacted? Is this complying with the GDPR? How is this -- how is this really working?

There -- I guess my time is up. Really quick, and different responses in requesting data, the underlying data, the redacted data.

So we get -- you know, it's a lot of different responses and a lot of different results.

BRIAN WINTERFELDT: Great, Susan. Thank you so much.

Ben, do you have anything to add on this?

BEN WALLIS: Actually, I was saying the same things as Susan's talked about, this sense of confusion and fragmentation. And Microsoft is keen to understand the impact that the changes are having, but at the moment, we're struggling to navigate this, the confusion of this new environment and work out exactly how we can quantify it and measure the impact that the changes are having on us.

BRIAN WINTERFELDT: Great. Thank you.

My second question I want to direct to Stephanie, but I believe others on the panel may want to answer as well. Stephanie, I'm hoping you can share with us some of the benefits you're seeing with GDPR compliance, and perhaps some of the challenges you might be seeing as well.

STEPHANIE PERRIN: Thanks very much, Brian. Stephanie, for the record.

I think it's actually a little early to see the benefits yet because we're only a month in. So I -- I don't think we're seeing the impact of people's response to this. I think at an ICANN level, in terms of the response to an issue that has been looming for the last 20 years, at least we have -- now have a concerted focus on developing sound policy. So I see that as a positive output.

But in terms of our individuals reaching out to us in our noncommercial constituency and saying, yes, thank you for this new concealed WHOIS, we're not seeing that.

Thank you.

BRIAN WINTERFELDT: Great. Thank you, Stephanie. Any other panelists like to jump? Laureen?

LAUREEN KAPIN: So in terms of privacy, certainly the GDPR has brought many benefits. There are a lot more attention paid to how data is treated. Companies have been spurred to really think hard about the data they collect, the data they share, security for that data. All of that is a great benefit, and the FTC certainly, as an agency, really concerned about privacy, is always happy to see companies being more mindful of how data is treated.

That said, if I were going to do a word cloud in terms of challenges, words that we've already heard are diverse and varied. I'd say those are the mild words. And then we have confusion and fragmentation. So we have this -- this cloud of uncertainty, I'll call it, in terms of -- mainly in terms of access and how users with legitimate interests can access this data. There is no centralized system. There is a requirement under the temporary specification that access must be given in a reasonable manner, but there's no definition of what constitutes reasonable. And in a concrete way, what law enforcement and other users with legitimate interests -- for example, cybersecurity researchers, Jane and Joe Public, as I like to call them, and IP rightsholders -- anyone with those legitimate interests is essentially being told now please go to the, 2000 or so more contracted parties and figure out what you need to do to deal with them. And that is not a way to have reasonable access in a way to actually be able to do your job in an effective and timely manner. And of course that's particularly important for law enforcement, which is charged with protecting the public safety and, more specifically, works on the safety of the Domain Name System against malicious activities.

BRIAN WINTERFELDT: Thank you, Laureen. I have Ben.

Would anybody else like to add on this point? Elliot next. Ben and then Elliot.

BEN WALLIS: Thanks, Brian. So I wanted to take the opportunity to be clear that Microsoft embraces the GDPR. We see privacy as a fundamental human right. And we see the GDPR as a major step forward in enhancing privacy rights of the individual. And we have been hard at work over the last two years to ensure that our products and services are compliant and that we can help our customers with their compliance issues.

And Microsoft also believes in the fundamental importance of maintaining a stable and secure Internet, which is clearly a central purpose for ICANN. And WHOIS data is a vital tool for us in enabling us to protect our company, to protect our customers, and to protect the public at-large. I mean, WHOIS is very much an important -- serves an important public interest. Just as we as a company see privacy and security as public interest elements that need to be balanced rather than choosing one over the other, so we see the GDPR -- there's no conflict between complying with the GDPR and using WHOIS data for the legitimate purposes of cybersecurity and other legitimate purposes. We don't see a problem with the GDPR per se. Our concern is more as what we see an overcautious approach to compliance by some of the contracted parties and by the temp spec and by an incomplete compliance model. It's incomplete until we have an accreditation and access solution. Thank you.

BRIAN WINTERFELDT: Thank you, Ben.

Elliot.

ELLIOT NOSS: Of course there is fragmentation. There was no standard set by either the E.U. or us as a community. Companies went out and did what they had to do to comply. But I don't want to speak about the few here, I want to speak about the many. John and Jane Q. Public, as Laureen likes to call them. There were 20 million new gTLDs registered in the first quarter of this year, so let's say 7 million and change -- 7 million or so in the month since GDPR implementation.

Those 7 million registrants will not receive spam, will not be inundated with phony renewal requests, will not receive unsolicited phone calls in the tens.

Cumulatively, probably from this one month alone, we will see tens of millions of less spam to those registrants. We will see hundreds of thousands, maybe millions, of less unsolicited phone calls and probably a million dollars or more in scams that those registrants would have been victims to because of that public information.

Today there is tiered access. The most important thing for all of us who are in this process is to agree that this is probably the greatest test of the multistakeholder model in the last 20 years.

Whether we work together to solve it or whether we fight over every little inch of every little issue will determine the success of the multistakeholder model and of ICANN.

And I want to say that we now have an opportunity. So rather than fixing on a problem that we all agree we should solve -- tiered access exists today -- we should work together to solve it. Thank you.

BRIAN WINTERFELDT: Thank you, Elliot.

We're going to move into our next broad topic which are -- which is: What are the thoughts and experience of the community so far with regard to the temporary specification?

I was actually hoping, Elliot, that you could start us out by talking about how registrars are implementing the temporary specification.

ELLIOT NOSS: Yes. Being left to our own devices, that means we had to retain our own legal advice. We had to implement at a product level. I will tell you that for registrars, it's very important to also understand that many of us, certainly in our shop, we had to start working on this six months before May 25th. We -- before all of the sirens were ringing and the community was trying to get out a temp spec, that temp spec would not have mattered to our May 25th implementation. It might have mattered if we were lucky to our August 25th or our September 25th implementation.

So today I think registrars overwhelmingly, certainly when measured by percent of registrations, are doing the best they can. And most importantly, you know, I think -- have continually recognized the need for tiered access, the need for commonality and reduced fragmentation and continue to encourage people on the other side of the aisle on this issue to work with us on taking what's going to be in the market until we have a community standard around this stuff and improving it day by day. Because I, like everybody else here, wants a common solution, especially with one that has legal protection for the contracted parties.

But I think it's important that we all understand that we're going to be dealing with our -- what we have today. And the best way that we can solve the problems of next week and next month and probably next year are to start working together now on the particular needs.

We have a tiered access implementation. All of our tools aren't up. We have had very, very few requests for access, something around low double digits, until, of course, preparation for this meeting where we were inundated just over the last day or two with a couple hundred requests primarily from one or two parties.

So, again, I encourage us all to work together because what you see today is not what it should be in a week or a month or a year.

BRIAN WINTERFELDT: Great. Thank you, Elliot. I appreciate your call for all of us to work together towards solutions. I think that's really important.

Stephanie, do you want to go ahead? And then I have Laureen.

STEPHANIE PERRIN: Thanks very much. Stephanie for the record again. I think I have some seconds in the bank that I didn't use last time.

I would just like to say there's actually nothing new in terms of the data protection requirements in the GDPR. "Nothing" may be an exaggeration but very little new. So that in the view of those of us in civil society, we think that ICANN has not been in compliance with data protection law for, low, these 20 years.

Having said that, we are not going to catch up in the four months, six months, whatever we have, in the expedited PDP that the GNSO Council has -- is initiating to review the temporary spec. I think we should set our expectations in a realistic fashion.

This is a difficult problem, and it will require an awful lot of sustained effort. Thank you.

BRIAN WINTERFELDT: Thank you, Stephanie.

Laureen.

LAUREEN KAPIN: Thanks. First of all, I'm going to agree with Elliot in that it's a great thing that a vehicle that has perpetuated spam and created certain risks for phishing and those types of abuse, to the extent that these changes in the WHOIS have had a benefit by reducing that, that's terrific.

On the other hand, to segue to a different point, Elliot has stated that they've seen very few requests. And one of the reasons that our law enforcement colleagues have reported to me to explain at least in part the lack of requests is that all your front-line law enforcement and investigators see when they are looking for information that previously they could get with the press of a button, so to speak. What they see now is redacted for privacy. What they don't see is, "Please contact registrar X for more information" or, "This is how you should make a request if you have a legitimate investigative need for this information."

So part of the issue here is that people don't know what they don't know. And it's a real flaw in the current system that I think could be very easily fixed, which is that we should be improving our communication about the fact that, yes, this information is nonpublic but it can be requested and here's how to do it. And what I would advocate is that registrars and registries should have this information in the WHOIS record. Let the people who need the information know how to get it.

ELLIOT NOSS: Briefly, I want to say two things. One, the email address for abuse is in the record. It isn't called out in bright, shiny lights.

Two, I want to congratulate you because you have now become the first person to put in a feature request; and that is exactly what we need to be doing as a community.

[Laughter]

I have got my product people out here, and I think that was a fantastic idea because the last thing we want is confusion.

You know, it goes further and let's take what you said and extend it because when you are talking about those front-line law enforcement officers, you know, I can't tell you how many organizational hours we've spent educating those front-line officers around what the difference of a registry and registrar and a website, et cetera is.

So all of you are in a much better position than we are to help educate your communities about these changes. If we can help by providing you guys with information to do that, that's fantastic. And, you know, again -- I'm -- I'm being a little glib when I say that, but I mean it. That is exactly the kind of feedback that will make all of this better. Thank you.

BRIAN WINTERFELDT: So I would just like to build out that we are building bridges in our cross-community panel and it's a beautiful thing to see.

[Laughter]

Susan Kawaguchi.

SUSAN KAWAGUCHI: So hopefully this will build bridges and not burn them. But I'm a little curious -- and this is just sort of a side note -- is why an anonymized email address would prevent spam. I just don't get that. Web form, I will agree with you. But an email address is an email address. So either those emails aren't being delivered or you put a spam filter in which is -- was always the possibility before.

The other process -- other issue is -- and I'm really glad to hear, Elliot, that you will take suggestions and, you know, sort of take on our --

ELLIOT NOSS: Laureen is already the first. You can't --

SUSAN KAWAGUCHI: He won't take suggestions from me, but that's okay.

ELLIOT NOSS: Would be happy to.

SUSAN KAWAGUCHI: The problem is that it's such a fragmented process. You go out there and, yes, you can email the abuse address. But I sort of received responses that were, like, in five different categories. Very few responded with information. That was success.

Others responded with I'm not even sure what. The response was not responsive. It was sort of like, "here's our phone number," you know? And I tried calling.

And then go get a subpoena and then also we do have a Web form or this or that. So then it's like, let me create for the enforcement that I do as a consultant, let me create a spreadsheet. When it's this registrar, I have to go here -- and I have been trying to use the ICANN lookup. I will go here to look it up and then go, okay, that's the registrar. Then I go here to the registrar and look that up. And, oh, let me find their policy on how to do this.

So I agree, I think as a community, if we can all come together quickly on a standardized access process that we're not hunting and pecking throughout the Internet here on how to make these requests, then it will be easier for everyone. Less confusion for our part. Less, you know, clutter in your email boxes from confused, you know, researchers.

BRIAN WINTERFELDT: Great, thank you so much.

I want to go on to the next question under this topic. Now that we've talked a little bit about the temporary specification, some of the positives and potential opportunities or challenges with it, I'm wondering -- and this is not to any specific panelist, so everyone can let me know if they would like a chance to answer this: What does an ultimate model of compliance with GDPR look like? And how do we get there? Goran Marby.

GORAN MARBY: One that the community agrees upon.

BRIAN WINTERFELDT: Very succinct answer.

Laureen.

LAUREEN KAPIN: Well, I would like to point to the GAC advice that has been emphasized in both Abu Dhabi and San Juan about certain components that we think are very important.

It's a given that the GDPR protects personal information, and the information of legal entities does not have the same protection. And in our view, the current temporary specification tilts the balance in a way that isn't -- that isn't required by the GDPR. So we think that that is a very important adjustment that needs further consideration in any final and ultimate model.

We also have a concern about the current perspective taken on email addresses. There's an anonymized email address, but from a law enforcement perspective and a cybersecurity perspective in addition, law enforcement and cybersecurity researchers need the ability to detect patterns, to find out if there's one individual who keeps using the same email address. And that is part of the WHOIS data that can actually help law enforcement and cybersecurity researchers detect patterns of use -- of abuse. We believe that needs to be reconsidered.

And, indeed, the anti-phishing working group has provided some input on a way to encode that information so that it is not -- so it is not disclosed to the public but the information can still be maintained for investigative purposes.

And, finally, we also believe a final system needs to take into account the unique needs of law enforcement for their queries of information to remain confidential and for their ability to request information more than once, maybe twice, maybe 100 times, 100 queries if it's a particularly severe situation, to be able to make those queries in order to do their important work to protect the public. A final system should include good analysis and thinking on all those issues.

BRIAN WINTERFELDT: Goran.

GORAN MARBY: I might should have added, "which is compliant with the law." And to the specifics when it comes to the GAC advice, and which we are very happy about, to have received, that during the implementation of that, we realized which is really to the heart of the problem that the GAC for the governments says one thing and the DPAs said something else.

And for the contracted parties and for ourselves as a joint data controller, it becomes sort of problematic if the DPAs are actually the ones who actually do interpret the law has a different opinion than the governments. We were in the middle.

But we have been trying to follow as much of all the advice we got. But in the end, it's actually the DPAs or the court who sets the standards which is implementable. Thank you.

BRIAN WINTERFELDT: Thank you.

Stephanie is next.

STEPHANIE PERRIN: Thank you. Stephanie Perrin for the record. My bio was a tad brief. I think it's probably important to note that while I'm a consultant now, I retired after 30 years working for the Canadian government in the field of data protection, since 1984, on implementation. And this whole business of balancing of the fundamental right of privacy with the legitimate needs of law enforcement to get access to data, to protect the public, to have serious organized crime, for instance, to have their own queries absolutely protected and anonymous and untraceable, that is an issue that anyone who works in data protection -- or rather, shall I say, a suite of issues, is deeply familiar with. This is one of the central problems in data protection. How do you do this?

So I think one of the problems with leaving compliance with GDPR to the last minute is it gives us less time to work on some of these very difficult problems.

I am working on those problems. I have a research grant with the University of Toronto from the Office of the Privacy Commissioner of Canada to research standards for third-party access to data because this is third-party access to data, whether it is consumers trying to track down information about websites or whether it is law enforcement looking for information or whether it's pattern recognition. And there are many privacy-enhancing technologies that can be applied here as they are in things like health data and epidemiological data to enable this work without releasing the personal information until you have a hit. And that's what we're working on right now. Thank you.

BRIAN WINTERFELDT: Thank you, Stephanie.

I have Ben and then Elliot.

BEN WALLIS: Thanks, Brian.

So I was asked to come to give a cybersecurity perspective, and cybersecurity is one of the reasons that Microsoft uses WHOIS data. We work to disrupt some of the most difficult cybercrime issues facing society today. To give you an example of the scale of that, over the last six years, our Microsoft digital crimes unit has drawn on WHOIS data to disrupt malware associated with approximately 397 distinct I.P. addresses.

So if we're asking what should an ultimate compliance model look like, I wanted to give a few examples of how we use WHOIS data and how that's undermined by the temp spec as it currently stands.

The first example I wanted to give relates to a link between cybersecurity and trademark enforcement. Attackers often create companies -- create domain names that are similar to major brands, and these domains are then used by hackers to communicate with malware on targeted computers. And so by looking up WHOIS data, companies can sue for trademark infringement and take over the offensive domains, and then they can observe and strategically disrupt hacking operations. And that's exactly what Microsoft did last year when we won a case against Fancy Bear. You might have heard of Fancy Bear. It is a -- thought to be a state-sponsored cyber espionage group responsible for attacks European and political institutions. And so we've used tools like reverse WHOIS where we can identify some malicious domains by Fancy Bear and then we can go and find out other domains that they are using. And tools like reverse WHOIS and the ability to look at current and historical WHOIS data on an aggregated basis are under threat under the temp spec, and that undermines our efforts.

BRIAN WINTERFELDT: Thank you.

Elliot.

BRIAN WINTERFELDT: Yeah, I want to reinforce Stephanie's point about pseudo-anonymity and really stress again, particularly to the security community, that registrars are unlikely to come up with a pseudonymous set of tools that going to be sufficient quickly. That's a place where, community or externally, help should be provided.

And then I want to talk about anonymity, because I think that's going to be the toughest pill to swallow in an eventual solution. People have been anonymous in their use of WHOIS for -- since its onset. That is now over. There is no way to determine legitimate interest without identifying who you are.

There is no way to determine if you're a lawyer or a consultant who is representing a company, whether that's legitimate without establishing agency. These are not burdens or roadblocks. These are simply efforts to comply with the law that probably should have been in place from the launch.

We need remember that WHOIS is an anachronistic set of data that is public only because of history.

The third thing I want to talk about in an eventual solution is cost recovery. And very briefly, you know, the community is too quick to just download burdens on the contracted parties. I think we all want to step up and participate here, and we need reasonable cost recovery.

Of course if there is an external third-party solution that has legal protections for us, that goes away. But again, I want to stress, I think we're all going to be dealing with what we have in the market for a significant period of time, which is why I think we need to be comfortable across the breadth of those issues and work together.

Thanks.

BRIAN WINTERFELDT: Great. Thank you so much, Elliot.

The last question on this broad topic. Ben, I was hoping you could talk about your thoughts on how best to engage European authorities to ensure the proper application of GDPR to WHOIS, and then I'll open it up to other panelists, and then we'll move on to the next big topic.

BEN WALLIS: So, Brian, I'm glad you came to me next because I just wanted to take the opportunity to correct the record. I think in my efforts to demonstrate the massive impact of our work on cybersecurity, I seriously understated it.

When I said 397 distinct IP addresses, I meant 397 million distinct IP addresses.

[Laughter]

And I would be very grateful if that was corrected in the record.

[Applause]

So to the question, how can we best engage with European authorities. So firstly I'd like to emphasize the role of the GAC, who have been -- who have worked very well and given some very helpful input into this process over the last year. So I think it's important that the GAC is involved in the community processes as we go forward with the EPDP and with the other elements of this work over the next 12 months. And we have to remember that the GAC is -- is a very precious interface to the European institutions and to the member states, which Goran and his team have identified with their framework for a unified access model as bodies which need to be persuaded, and that this is the right stepped forward; that accreditation and access in the ways that the ICANN community is going to develop are legitimate under the GDPR.

So my first point would be to recognize the role of the GAC. And the other thing I would say is that now that the ICANN Org is taking leadership around a solution for accreditation and access, I think we need to engage fully with it, on all efforts to come up with an accreditation and access solution, so that we can best equip Goran and his team in their engagement with the Data Protection Authorities, the European Data Protection Board and the member states.

Thanks.

BRIAN WINTERFELDT: Thank you, Ben.

Stephanie.

STEPHANIE PERRIN: Thanks very much. Stephanie again. We're all being very urbane on this panel I must say. So I feel a duty to say there are 126 data protection laws in the world now. 126. Many of them will be falling in line with the GDPR to avoid determination that they are not adequate.

So how about we stop focusing only on the GDPR and we focus on compliance with data protection law? Because, yes, the GDPR has fines, but ICANN is an accountable organization. Surely we don't only comply with law when there's a fine.

BRIAN WINTERFELDT: Thank you, Stephanie.

Goran.

GORAN MARBY : Thank you. Just a small comment. I know words are important here. And I noted Ben didn't say that the temp spec was the cause of the problem. It's actually the law itself who sets that. But that's what you meant, I suppose, Ben. Thank you.

The other thing is that I don't think -- my intention, I can always not try taking leadership in the discussion. What we're trying to do, going into an area where -- and this is repeated many times, is that up till now, compliance with GDPR has been fairly easy, because what we've done is that we've agreed -- and I think it's -- I mean, the multistakeholder model has proven that in very short period of time -- and, yes, we started too late -- we actually came together and came up with the calzone model which then ended up as a temp spec. And kudos to everybody who got involved in that one.

But now we're entering into a phase where the law doesn't specifically permit what we would call the unified access is now becoming more problematic.

And I want to say in the relationship to the question about how to engage with any institution around the world, the only reason anyone listens to ICANN is you. Because ICANN, as an institution, is important. And that is because of the work you've done. Otherwise, we would be no (indiscernible). No one would listen to us. And the fact that we were able to have this engagement with the European Commission, the Data Protection Authorities and, to some extent, the member states in the EU that led us to having the guidance we got from the DPAs was because of the multistakeholder model. And we have to remember that going forward.

So the big risk I see going forward is that we don't come together in the multistakeholder model and continue this discussion how to solve those issues, because that makes our voice bigger.

We are now entering a process where we are trying to find more legal information how to do a unified access model. That is my only aim. I don't have an end game with it. I'm only to provide the community with something that is quite hard. Now, more legal surrounding about it.

And because what I'm trying to do with the legal (indiscernible) of that is because we all need it. And now J.J. is probably going to correct some words I did as well.

Thank you.

BRIAN WINTERFELDT: J.J.

JOHN JEFFREY: I'm not. On a separate topic relating to the question, the question was how can we best engage with the European authorities. And I think the key word to the question is how "we" can engage. That's all of us, to follow up on what Goran was saying. It's very important.

I mean, Stephanie's point about 126 data protection laws. Why are we paying attention to the European ones? Because they've come to the forefront and they've become a barrier to WHOIS, in some ways, being the way it was before. That's heightened the level of that discussion into our community and allowed us to have these discussions about the balancing and in different way that, frankly, didn't result from the previous decade of work from WHOIS.

So this is an opportunity for us to have that discussion, but it's an opportunity for all of ICANN, not just ICANN Org, to engage with the DPAs. One of the reasons we're being so careful in our discussions with the DPAs and with others is to make sure that all of the conversations are documented. We're sending letters that are showing what questions we're asking. We're submitting materials in open, and we encourage all of you to be part of that discussion by participating and by talking to your -- the Data Protection Authorities that relate to what you do.

BRIAN WINTERFELDT: Thank you so much.

The third topic we have is the thoughts on the EPDP. How the community should move forward with regard to it.

We're fortunate enough to have two councillors on the panel us with, both Stephanie Perrin and Susan Kawaguchi, who have spent the entire day discussing the EPDP. We have allocated 15 minutes at the end for Heather, the GNSO Council chair, to give a formal update on the work of the Council. But I was wondering, Susan and Stephanie, if you wouldn't maybe share some thoughts with us. I was hoping, Susan, maybe you could start with talking a little bit about what you believe the proper scope is and timing of the EPDP, and then I have the next question for Stephanie.

SUSAN KAWAGUCHI: Thanks, Brian. We did spend all day talking about the charter for the EPDP and found ourselves many times getting into, you know, sort of discuss -- starting the PDP ahead of time. You know, just the Council discussing the differing opinions.

The scope we have got to find quite yet. But we made some headway. We spent almost two hours talking about that. And it will be a very, very intense work -- working timeline. We're aiming for Barcelona to have part of the work done, at least. And -- and that is -- does not leave us a tremendous amount of time for public comment or implementation before next May.

So we've also talked about composition and -- of the team, and agreed. I think came to a reasonable conclusion there. But we need the community's involvement. You know, the GNSO Council can provide the charter, but actually all the hard work will be up to the community, and to come to agreement and sort of cross some bridges that we've been unable to cross before.

BRIAN WINTERFELDT: Great. Thank you, Susan.

Stephanie, do you have anything to add on that point? And in particular, I wanted to also ask you what you believe the key issues are that the community will discuss during the EPDP.

STEPHANIE PERRIN: Thanks very much. Stephanie again.

I think it's appropriate at this point to -- because as Brian says, we've been at it all day, and I'd like to thank the meetings team and our hosts here. This is a great facility. And in particular, I'd like to thank them for the plenty full supply of coffee. Otherwise, I wouldn't be speaking.

This is an enormous challenge, as I think I mentioned earlier. We've left this for 20 years. Our first representation from the data protection community was in 2000 when they created a paper on WHOIS -- "they" being the international working group on data protection and telecom. So to attempt to do this in four months is heroic and possibly stupid. I think we have to set ourselves up for success. We have to limit the amount that we attempt to chew off. We have to be willing to put certain things in a bucket and push them out and handle them sequentially.

We do not have the bandwidth in this community to manage a number of parallel processes in my view, and so we are just going to have to face a few facts; that there is a cost for not doing things in time. That would be my position.

Now, your second part of that question, Brian, was?

BRIAN WINTERFELDT: The second part of the question was what you believe the key issues are the community will discuss during the EPDP.

STEPHANIE PERRIN: Well, I think one of the key issues that the community cannot get into is implementation issues. And during today's meeting I suggested that the excellent work that was done a couple of years ago -- I know Chuck was one of the -- Chuck Gomes was one of the co-chairs. I think there were three of them on this working group that addressed policy and implementation issues and how to distinguish.

There's a lot of things mixed in in the temporary specification. If we are looking at policy, then let's look at policy. Let's not try to build implementation before we've made policy decisions.

Now, there will be parties that don't like that, and I'm busy in my standards thing working on implementation issues. But we cannot expect the community to engage simultaneously in too many processes if we're going to do the job properly.

Thank you.

BRIAN WINTERFELDT: Thank you.

Susan, do you have anything to add? And then Laureen.

LAUREEN KAPIN: Thank you, Susan.

In terms of participation, of course the GAC is uniquely situated, as the advisory body that issues advice on matters of public policy, to have a seat at the table in this EPDP, not on the sidelines. It would be far less effective for the GAC to just be consulted at the end of the process, or even along the way to say, "Well, what's your feedback?"

As we all know, the people who have a seat at the table shape the landscape, and that is where the GAC needs to be. Right in the fray, so to speak. The civilized fray, I'm sure, based on the discourse at this table today.

Second, in terms of the scope of the EPDP, I'm very mindful of the practical considerations that Stephanie has raised about setting up the EPDP for success, particularly when it's such a condensed period. However, I think it's very important to emphasize that the temporary specification does already deal with access. In Appendix A, the registration data directory services, there is a provision that says they must provide -- contracted parties, that is, must provide reasonable access to personal data to third parties on the basis of legitimate interest.

So that is already there. And then there's a caveat, "unless those interests are overridden by fundamental rights of the data subject." This is already there. So to me the real question is to what extent is the EPDP going to deal with this access issue? It is not a question about whether they should be dealing with this. They have to deal with it. It is in the temporary specification.

So to what extent is the issue? And I would say whatever is left over in terms of access and accreditation, about what is reasonable, about how to put meat on the bones of this requirement when currently there is very little, whatever is left over, that could be -- and, indeed, should be -- the subject of a separate temporary specification as soon as possible, because these are crucial issues that must be resolved.

BRIAN WINTERFELDT: Thank you.

Goran.

GORAN MARBY : Yes. I actually -- I want to say that I think the GAC has a very special role in this and a very important role, and we should actually be very grateful for having the GAC because within the GAC, there are 28 member states of Europe who are not on the sidelines of this discussion. They are actually the ones who wrote the law. They are the one who decided by the law. They are the one who has in the law certain abilities to make decisions as well.

And also, we are blessed to have the European Commission in there who physically wrote the law. Unfortunately that part of the European Commission doesn't come to ICANN meetings. We invited them many times. But -- So, there is -- the GAC in this actually have two roles. One of the roles is to be the support and giving us advice, but here is also a channel for us as a community to reach out to the ones who actually makes the decision in the European governments. Thank you very much. And we are lucky to have them there.

BRIAN WINTERFELDT: Thank you, Goran.

Elliot and then Susan and then we are going to move on.

ELLIOT NOSS: I'd like to pick up on Laureen's point around tiered access in the spec. I think that the spec need do no more than reinforce the statement that's in there. And I like to be hopeful and I like to dream. So my dream in this regard would be that by May 25th, 2019, we have tiered access working in the market that includes all of the large registrars, that includes the significant majority of the smaller registrars, that has worked through a lot of the difficulties that we'll all have to work through with use case after use case after use case.

You know, I really want to encourage you guys -- I feel like so much of your energy and effort, it's all great information but there's nobody on the other side of that issue. We all agree that fragmentation is bad and we all agree that tiered access is necessary. We work with cybersecurity community every single day in our business. We want to help you guys.

So if I could take all of that energy that's going to -- I don't think there's anybody in the room who doesn't feel that way and start to turn it into the process that I really believe that by May 25th, 2019, we could have something that is working and live and existing well before this EPDP comes in for landing.

BRIAN WINTERFELDT: Thank you.

Susan.

SUSAN KAWAGUCHI: Well, I would like to see your dream come true. I think the time line has to be a little more speedy. You know, we can't wait for that information till 2019. But if the registrars are already working on access and we can all learn those -- what that access is and what the requirements are and make sure that it's something that I.P. interests can respond to and it's a reasonable solution, then I think we can work together on that.

I also wanted to address Stephanie's comment, you know, to -- we've been working on this for 20 years. That's true. I mean, I haven't been working on this for 20 years. But it seems like 40.

[Laughter]

We have also done some really good work. I think the community has really put their heart and soul into this, and I don't think we should just toss this all away in this new EPDP. And we have the RDS working group. No, that didn't work but, boy, did we talk purpose. Man, we discussed that forever. So we should pull some of that and try to come to agreement and decide -- cross those bridges and say, okay, We can all agree on this purpose or that purpose and then fix the ones that we don't agree on.

The PPSAI, there's a process for revealing the underlying contact information. The community has agreed on that. That's been implemented. Why don't we use that as part of our resource for solving this problem?

So I really think we should look back, see what we've done, throw away the bad stuff and keep the good stuff.

BRIAN WINTERFELDT: Thanks, Susan. Appreciate that contribution.

We're going to move to the next section. We're going to give each panelist two minutes to give sort of final thoughts on the subject matter, hoping each panelist -- I will start with Stephanie to my right -- can share with them what they feel the most important consideration is for our community moving forward on this issue.

STEPHANIE PERRIN: Stephanie Perrin.

I think to me the most important issue is that we do this thing right. I agree with Susan, there has been much good work. But harvesting it from the sea of documents that have accumulated over the 20 years is going to be taxing. We need to compromise. One of the reasons for failure of the last exercise that Susan and I were on, that was the RDS working group, in my view was the unwillingness of people to move off their positions.

We all have firmly held beliefs. We have to be willing to move and compromise and come up with agreement.

I also believe very strongly in fact-based policy. We now do not have the time to do the research that we need to get the facts and the data to support our various positions. We have a very eclectic collection of research at ICANN on the matter of WHOIS. It's a bit here and a bit there. We need facts on what the volume is.

We will find out over the next year how Elliot's implementation of RDAP is working. And it's one of the many reasons I would like to push that out until the end of the year and allow the contracted parties to figure this out.

I don't believe that having another expedited policy is going to accelerate that.

I also have a deep concern about ICANN's accountability in its process. We believe very strongly in the multistakeholder model. We'd like it to succeed. We do not want expedited policy process to replace the community policy process, no matter how flawed that has been on this particular issue. So I think that's probably an important point to end on.

BRIAN WINTERFELDT: Thank you, Stephanie.

Ben.

BEN WALLIS: Thank you.

So for cybersecurity, from Microsoft's digital crimes unit and our threat intelligence center, fast automated access is critical. We need to be able to react quickly to security incidents and take down malware as quickly as possible to reduce the amount of harm that can be caused. And having to make individual requests significantly slows down and hampers these efforts.

And it just gives more time for the malicious actors to magnify their actions.

So we need to quickly get back to the position where there is broad, persistent access, frictionless access to WHOIS data for those with proven and clear, credible, legitimate purposes.

Now, for me maybe the biggest problem with the temp spec is -- that I see that is an incomplete solution. Microsoft, we accepted that the GDPR meant that some data was no longer going to be publicly available. And back in February, I think, we welcomed it when ICANN said that accreditation would be a key feature of the compliance model.

So we were very disappointed when the temp spec didn't include this key feature. And I see last week's publication of the framework for a unified access model as a positive step. I think it's a very welcome sign that ICANN Org is dedicated to delivering this final piece of the puzzle.

But the one thing I want to end on is that the development and the implementation of an access model cannot come too soon. There's an acute need for some sort of temporary solution, just as the temp spec provided a temporary solution for other elements of complying with the GDPR. And so until we get some temporary solution, there's going to be continued fragmentation and an incomplete compliance model. Thank you.

BRIAN WINTERFELDT: Thank you.

Elliot.

ELLIOT NOSS: First I want to announce the second feature being delivered. I understand that later this week the registrars are going to release a one-pager trying to help the community reach abuse contacts.

I want to really stress that I think that we need to move from "we need" or "I need" to understanding that we are working together on common problems.

I think that we have to take the opportunity that the GDPR has provided as a forcing mechanism, to take what's been a 20-year stalemate and turn it into a positive outcome for the balance between privacy and legitimate interests.

I want to be clear that none of the unified access models that have been presented to date have any participation whatsoever from the contracted parties, from the groups that actually have to deliver on this stuff.

So from a unified access model perspective, from the contracted party view, we are nowhere. We are just starting, which is why I come back to what I have harped on a number of times already. We have to pay attention to what's in the market now and make it better.

You know, Ben may want ICANN to issue a temp spec around equal access. But if it doesn't comply with the GDPR and our legal opinion, we're not going to implement it.

We said back in Copenhagen, if we have to choose between litigating with ICANN or litigating with the European community, we choose ICANN. We make that choice grudgingly.

And, finally, I fundamentally believe we don't have to make that choice. I hope that everybody up here and everybody out there sees that what we all have to do is work together and turn this into a win for the community and for multistakeholderism.

Thank you.

BRIAN WINTERFELDT: Thank you, Laureen.

LAUREEN KAPIN: So the word of the day for me is "balance." The GDPR bakes into it a balance between privacy and other legitimate interests, including law enforcement, cybersecurity, crime prevention, I.P. rightsholders, and Joe and Jane Public.

And the word of the day, "balance" doesn't just apply to the GDPR, it also applies to all of the stakeholders at the table. And I'm encouraged to hear from a variety of folks at the table that there's a willingness to get beyond -- or moving beyond entrenched positions and having a really candid discussion of what are your real concerns and goals and how can folks be pragmatic about that and give a little to get a win for the community. I think that is all to the good.

I think we've already talked about what's very important for law enforcement. But I do want to emphasize in terms of balance one thing which we can't be especially generous about, is timing. Because the current system is so fragmented and so one-off, go to this registrar and comply with their system, go to that registry and comply with their system, that is not sustainable.

So as much as we should be balanced and considered and subject to negotiating real positions and interests, a real priority is to deal with this question of access as soon as possible because without that, there isn't even adequate compliance with the GDPR, which mandates that there has to be an adequate system for third parties with legitimate interests to get access to this information. And currently that just is not there.

That said, for my last word is that the public safety working group and law enforcement stands ready in a sincere and flexible way to really grapple with these issues, with all the stakeholders in the ICANN community. We want to work with you to solve this issue within the tight time frames we have.

BRIAN WINTERFELDT: Thank you, Laureen.

Susan.

SUSAN KAWAGUCHI: Thank you, Brian.

So I'm not arguing against data privacy. I agree to the data privacy. I want my own privacy. But there is -- balance is needed, and I agree completely with Laureen. There is a reason people -- you know, it's like I don't look up WHOIS records for fun. There is --

[Laughter]

There is a compelling reason to look up that WHOIS record and go, Okay, this is what I have to do to take these measures. And most of this right now I'm relating to my former employers and brand enforcement I have done for 20 years.

Those -- you know, I didn't even look up domain names records for -- that contain "eBay" in the domain unless they were using it in a manner that was not fair use. So there was already abuse or at least confusion.

And I know that to stand here and say, look, I represented these two big brands, eBay, PayPal -- several big brands, eBay, PayPal, Facebook, Instagram and some others, that I was really protecting the users. And I know that sounds shallow, but that is truly what I was doing because I saw that all the abuse that went on. It usually didn't hurt the brand. It hurt our users. It was the $99 a month for the support sites that -- eBay support or Facebook support that somebody charged to somebody's credit card.

But that said, I agree the world has changed. There are data privacy laws everywhere now. Let's agree to those. But don't overcomply.

You know, businesses, Facebook, eBay, Microsoft, they don't have data privacy rights. Their information should be out there. If you are a commercial -- if you are taking somebody's money, your information should be out there.

So what we're looking for -- and if best practices would work in the industry right now to get us the information we need to protect users, then maybe we don't wait for the policies. We work on best practices together and get some standardized WHOIS data in so we're not trying to figure out what it really is saying.

And bulk access with maybe these new technologies. And I'm not versed in technologies that can protect data, but if they're out there, we're working on the Internet. Let's use these new technologies.

BRIAN WINTERFELDT: Thank you, Susan.

Goran.

GORAN MARBY: As me and J.J., I think we have two minutes combined, don't we? And I will spend 15 seconds.

So I want to go to this from another aim. We need to learn how to work together under a law. Some of the things that's been talked about up here are actually features in a law.

We might think they are good or bad. We might think that this also insane or not enough, but it is the law.

I'm thinking of buying a T-shirt "It is the law." And if we don't as a multistakeholder model actually accept it is the law -- especially when we receive legal guidance from the DPAs -- thank you very much -- that actually provided us with that guidance and take that into account before we proceed, then we will endlessly, endlessly, endlessly, endlessly talk about things that is pointless because there are some increased level of legal certainty in what we have done from the DPAs.

We also know to some extent what the legal uncertainties are. And then the question is: How should we check them?

We're not trying to -- we're not trying to move the needle when it comes to unified access model, which is what it is. We are only trying to figure out if we can have one. That's what we're trying to do. We're asking the questions.

And the reason I'm doing this like the way we're doing it is because we want to do it in an open and transparent way. I want you to know every single question I ask of the DPAs so you also, like we did in the Calzone model -- and I promised my team never come up with any name whatsoever on any project in the future.

[Laughter]

You probably think that's a good idea.

So you also, as we did last time, if you don't agree with the questions, we will provide those questions to the DPAs as well. And in the documents, you can see that we actually have contradictory questions in the document.

So we need to learn how to work under laws because there are more laws, as has been pointed out here. Only in Europe there are the discussion about eEvidence, ePrivacy, NIS directive -- I think I got all those acronyms right -- the E.U. cybersecurity strategy that actually names the domain name system, WHOIS system. And many times when I speak to governments around the world, it is about potential laws that can have an effect on the Domain Name System. We don't always see that it will have an effect on the Domain Name System. We will learn seizure of domain names for eternity. There are proposals. There are actually countries who have -- in Europe has those laws. We need to figure that out.

BRIAN WINTERFELDT: J.J., would you like to take a turn. You are more than welcome to have two minutes.

JOHN JEFFREY: Thank you. I'm glad I didn't give up my two minutes.

I think there's a very important thing for us all to think about when we're talking about WHOIS. And if you look back across ICANN's 20-year history, there is no WHOIS policy but there is ICANN being literally purpose-built to, in fact, in part preserve WHOIS. And so that's what we're faced with.

And until there is a policy that replaces what ICANN did with WHOIS, we believe that part of our function is to preserve a nonfragmented WHOIS in the best way possible. That's the approach we have taken to it all along. And now we are striving for that legal certainty around that, applying it against 126 data protection laws, including GDPR, and looking at how WHOIS fits into that and looking at how you as our community can participate in that discussion and bring WHOIS to the right level, bring a unified access model, if that is the right thing, to the right place without naming it anything funny and really create a position where we can provide little certainty with the contracted parties. We cannot waste ICANN's time and resources on trying to determine whether the courts or data protection authorities or others agree with ICANN's position but having as much certainty around that as we can.

We think this is an opportunity for us to clarify those data protection laws that relate to WHOIS and to provide for certainty to our entire community around this. And I think with you we can strive to attain a higher level on that. And this is something that will happen with any luck within the period of time that we have time to develop that policy.

BRIAN WINTERFELDT: Great. Thank you so much.

We have about 15 minutes left on the panel. Heather has asked us to reserve five minutes at the end for her to give an update of the EPDP work at the council level, which gives us ten minutes for Q&A. I would like to open it up to the floor. There are ICANN staffers who are going to assist us with microphones. So please put up your hands and get their attention.

We're going to start with Number 2 since it's the only number I see to pick from.

STEVE DELBIANCO: Steve DelBianco. The question would be with regard to the temp spec, I heard there were at least a few elements where perhaps was overcompliant. But I didn't hear the panel discuss whether they think the EPDP should revisit these three factors. And one would be whether registrant email can or cannot be disclosed publicly, since EURid does it now. The second is should it be applied to legal persons or only to natural persons? And the third Laureen mentioned of geographical applicability to all citizens of the world or only those that have that connection to Europe.

So since this panel is about that and the next panel is about the accreditation model, what do you think need to be done about those three questions in the EPDP?

BRIAN WINTERFELDT: Any of our panelists like to jump in on that?

Elliot.

ELLIOT NOSS: Yeah. I think, first, there's more than that. We -- I think everybody here or many people here know we're in litigation with ICANN around one divergence. We have two others that -- you know, that were outside of the temp spec now. And, you know, we'd like to see those resolved in a way where an authority answers those questions.

You know, I think that you raised questions that also should be answered by authority. You know, at the end of the day, I think that with a couple of them, it's really about the incredible complexity in dealing with it in the field. And, you know, I have no comment on the last one. But, you know, what I would say, I deeply believe is the better we do around a successful, unfragmented, tiered access model, the less relevant those distinctions become.

Thank you.

BRIAN WINTERFELDT: Laureen, and then we're going to go to the next question.

LAUREEN KAPIN: Sure. And I'll keep this brief. It strikes me that if something is in the temporary specification, it is up for grabs in the policy development process. So if there is disagreement, if there are refinements, if there are improvements, that should be the real work of the EPDP. And because this is a complicated law and a law that has gone into effect recently, there's going to be a range of interpretations. We know this from the divergent paths that the ccTLDs in Europe take. There isn't one unified approach. So even though we all strive to follow the law, there are many questions about what the law requires and what it means. And I think that's going to be part of the work, and why it would be great to have a DPA perspective to give some advice and guidance to the EPDP as it conducts its work.

BRIAN WINTERFELDT: Great. Thank you.

Number 1.

MILTON MUELLER: Hello, it's -- Is it on? Okay. This is Milton Mueller at Georgia Tech, Internet Governance Project. I have a question about -- It's not on. Okay. There you go.

So my question is about the GAC, the role of the GAC, which was highlighted by Goran and others. I'm very confused about this role. I'm looking now at recent GAC advice regarding the GDPR, and I basically see two key statements. Number one is that WHOIS may not be maintained to the greatest extent possible, and number two, certain data elements may become hidden.

Now, I read those statements as the GAC saying, gosh, I wish we didn't have to comply with the GDPR, because the reason those data elements are hidden is because of the GDPR, and the reason WHOIS is being restrained is because of the GDPR. Yet this is odd because the GAC seems to contain at least two dozen European governments who are, in fact, supposed to be bound by their own law and who made that law. And I take you back to what Goran said, which is GAC says one thing, the DPA says something else.

What does this tell us about the role of the GAC in this process? Can we rely on the GAC to actually represent what the law is? Or is the GAC assuming the role of a legislative body that is modifying international law in line with the wishes of whatever interest groups are influencing it at the moment?

[Applause]

BRIAN WINTERFELDT: Laureen, would you like to take that?

LAUREEN KAPIN: Sure. I have to confess I'm not recognizing the language that you are quoting, so I'm just going to go right to the source and actually read aloud these full statements.

What the GAC has said in its San Juan advice -- I don't have my reading glasses on but I'll do my best. Oh, you're so kind.

And that's to -- Oh, these are great.

[Laughter]

Let the record reflect -- and don't take this out of my time -- the record reflect that I've been assisted by my colleague from the Registrar Stakeholder Group.

More bridge building.

LAUREEN KAPIN: More bridge building.

So the GAC advised, and I believe this is a direct quote also from ICANN leadership's advice: Ensure the proposed interim model -- in this case we'd be talking about the temporary specification -- maintains the current WHOIS requirements to the fullest extent possible.

Now, I don't see that as anything inconsistent with the law or especially controversial.

"Also to distinguish between legal and natural persons, allowing for public access to WHOIS data of legal entities which are not in the remit of the GDPR."

Again, the GDPR itself focuses on protecting personal information. So I'm a little baffled by the statement. The GAC's advice is consistent with the GDPR and, indeed, we have folks from the EU Commission who are advising us and objecting if we go beyond what the GDPR says, because governments are not in the business of wanting to advise people to break the law, but the GAC itself is in the business of protecting the public interest and trying to strike the right balance that the GDPR itself bakes into the process.

[Applause]

BRIAN WINTERFELDT: Thank you, Laureen.

GORAN MARBY : I would like to make --

BRIAN WINTERFELDT: Goran.

GORAN MARBY : With all respect for the -- the importance of the GAC and their advice, compared to the advice from the DPAs, unfortunately the Board could not accept the full advice. And that is the -- That's one of -- that's one of the problems.

So we have a -- It could be so that the governments in the concept of GAC do one interpretation of the law, and that's fine. It's just the DPAs, who are the ones who are in charge of that according to the European system, did another interpretation of the law.

Thank you.

BRIAN WINTERFELDT: Thank you. We have time I think for one more quick question. Number 4.

GREGORY MOUNIER: Hello. Thank you, Brian. Gregory Mounier from Europe.

I have a question for Elliot. If we all agree that some actors with legitimate interest to access nonpublic WHOIS data, and if we all agree that tiered access is necessary to balance privacy protections and legitimate interests, could you please explain why in the Tucows data access system it is still necessary to have privacy and proxy services in place which will hide the information that you're claiming those actors with a legitimate access interest should be able to access?

Thank you.

ELLIOT NOSS: It's a great question. I think there's a couple things. First of all, what you see today in terms of tools and implementation is kind of the -- we're still sweeping the beaches after GDPR. But there is going to be a very different role for privacy protection in a post GDPR world.

It is still usable for people who want to create a higher standard of access. So in other words, if somebody -- you know, we've got private data now, and that privacy protection may create a higher standard of access to get that. So maybe security researchers, as an example, in doing reverse lookups will see pseudonymous data that will show this as privacy protected. That tends to have a higher standard.

The thing that I think also needs to be understood by the community is I think that, you know, the PPSAI work was great and talked a lot about -- almost got to the finish line and talked a lot about, you know, sort of when you should pierce the veil. I do fundamentally believe that we're going to see the protections of privacy services which won't go away are certainly less useful but have some use today. That veil will be more permeable than it was before.

And so what you're going to see is, again, you know, kind of rules and practices and learning happen on the ground through the next few months' period. I have no question about two things, though, directionally. Privacy and proxy will be less prevalent, one, and, two, privacy and proxy is likely to be more permeable.

Thanks.

Oh, and one last thing. Those of you really interested in this topic, I do have a session tomorrow morning at 9:00 in Salon 7. So we can keep it going.

Thank you.

BRIAN WINTERFELDT: Great. Thank you so much.

We have five minutes left in our session today. I'd like to turn the microphone over to Heather Forrest. I apologize to those of you we can't get to your questions live, but I encourage you to maybe come approach the panels afterwards, and we have the next panel coming up.

Heather, in your role as Council chair for the GNSO, I'm hoping you can share with us a quick update on the EPDP charter discussions that Council had extensively today.

HEATHER FORREST: Thank you, Brian. Very much so.

Heather Forrest. Good afternoon to everyone. This is a wonderful opportunity. I'm mindful, let's say, that I should be as brief as possible in the hope that you get another one or two questions in before we wind up here.

So in the spirit of accountability and transparency, let me provide you with an update on where we stand in the GNSO Council right now.

First of all, to say thank you to everyone who has provided input over the last 48 hours or so. We had a very productive session in this room yesterday evening raising a number of different issues that will find their way into the chapter and the initiation request, which are the two documents that will commence the EPDP.

We came away from that session yesterday evening with a very long list of detailed feedback and input into the drafting process and began to analyze those -- those pieces of input today in our session, which took place, as Stephanie and Susan have rightfully pointed out, from 9:00 a.m. until just prior to this session. In fact, we had to wind up as quickly as we could to get Susan and Stephanie here.

So what is happening now is that we have identified certain points around which we have coalesced. Many of those let's say relate to the points or draw from the points that were elicited yesterday in the cross-community session. We are putting together some draft text in a charter, some strawman text, if you like, particularly in relation to the topics of the composition of the team, the leadership of the team, the working methods of the team. And I believe there's probably one more category of things.

The one area that --

Budget?

HEATHER FORREST: Thank you.

The one area that we need a bit more time on is scope. We've had a very extensive discussion this afternoon on the scope of the effort, and we'll continue to think about that. So we won't expect necessarily draft text on that in the next 24 hours.

What happens next is this. The Council will meet this evening for half an hour, I believe 6:30 to 7:30 in a closed session that will prepare us for the GNSO Council meeting agenda that underscores our meeting from 1:00 to 3:00 tomorrow. Our GNSO Council meeting is public. I encourage anyone who would like to be there at 1:00 to join us. On the table tomorrow afternoon is a motion to approve a charter and initiation request.

Now, you can tell from what I've just said that we don't have those documents finalized to be approving at this point in time; however, we may well have a text that we're at least in a position, let's say -- I'm not sure how far we'll get. We have the session tonight, we have another session tomorrow morning, and then we have our Council meeting.

So I anticipate we can make further progress than we have. I will tell you from a very personal note I leave the sessions today feeling very heartened, and it's largely the result of all the feedback we have received from all of you in the room today. It's a rich and complex process, and it's a continuing process, and we very much appreciate all of the support that we've had from the community as a whole, from the GAC, from the Board, from ICANN Organization.

So on behalf of the GNSO Council, I thank you for all of that input and look forward to providing further updates going forward.

Brian, thank you.

BRIAN WINTERFELDT: Thank you so much, Heather.

I want to thank Heather and all of our panelists today. I think this was an excellent cross-community discussion. Really appreciate everyone's time. A reminder we're going to have a 15-minute break and then we're going to have the second cross-community panel on GDPR that will be focusing on access and accreditation work that will be starting in this room at 5:00.

Thank you again to all the panelists, and appreciate everyone joining us today.

The next session begins promptly at 5:00.

[END OF TRANSCRIPTION]