BARCELONA – Cross-Community Session: GDPR
Wednesday, October 24, 2018 – 09:45 to 12:00 CEST
ICANN63 | Barcelona, Spain

BRUCE TONKIN: Okay. We'll get started so that we can make best use of our time available this morning.

My name is Bruce Tonkin, and I have been asked to chair this cross-community session on GDPR. The concept of cross-community sessions is really to bring the community together to try and see how the community as a whole can focus on important problems and solve them. And so in this cross-community session we have representatives from several of the parts of the ICANN organization. We have representatives from the GNSO, which is responsible for policies with respect to gTLD domain names.

On the contracted parties house, we have Nick Wenban-Smith from Nominet. Nick is the general counsel at Nominet and is also a data protection officer. Nominet is involved in both country code names, in their case .UK, as well as generic top-level names such as .BLOG.

On the Commercial Stakeholder Group, we have Flip Petillion. I think I got that right. And Flip is from a firm in Belgium that provides dispute resolution services and is often involved in resolving disputes that relate to domain names.

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

From the Noncommercial Stakeholder Group, we have Professor Milton Mueller from Georgia Tech in Atlanta, Georgia.

From the Security and Stability Advisory Committee, we have Greg Aaron. Greg is the vice president of iThreat Cyber Group and is involved in sort of threat intelligence and investigating the use of domain names for online abuse.

From the At-Large Advisory Committee, we have Hadia Elminiawi. Hadia is the director of the DNS Entrepreneurship Centre in Egypt.

From the Government Advisory Committee, we have Ashley Heineman. Ashley is responsible for Internet policy within NTIA in the United States. And the GAC has the difficult challenge, I guess, in that when looking at issues such as privacy, it needs to look at how that's handled across ALL the different governments that are members of the Government Advisory Committee and find solutions that are globally relevant.

We also have a representative from the law enforcement stakeholders, and that's Chris Lewis-Evans. Chris is involved in the U.K. National Crime Agency and is responsible for sort of managing Internet investigations.

And on the data protection side, we have Cristina Monti. Cristina is in the unit for International Data Flows and Protection within the European Commission's Directorate-General for Justice.

So we have a very strong panel. All of these panel members have been involved for many years in, I guess, balancing some of the challenges across the need for protecting personal information.

I thought it was worth just trying to set a little bit of context. And it's probably relevant to go back to the RFC-1591 which was written by Jon Postel in 1994. In fact, it's about the 20th anniversary of Jon's death. He died the 16th of October, 1998. It's interesting to see words that have been written more than 20 years ago, but they are worth going back to and reflecting on.

And in the RFC, Jon stated that the managers of top-level names are the trustees for the delegated name that they have been provided but they have a duty to serve the community.

He also said that the concerns about rights and ownership of domains is inappropriate. What is appropriate is to be concerned about the responsibilities and service to the community.

And so registered name holders that hold domain names within top-level names, they have a responsibility to obey the law in their local jurisdiction. Some of these registered name holders are natural persons, and the context of registered name holders are often natural persons.

And then it's also the case that the personal data of these natural persons is protected under various privacy laws around the globe.

If we look at where ICANN fits into this, we can see from a mission of ICANN is that ICANN has a narrow mission, which is coordinating the

allocation of names in the root zone -- I'm picking the part of the mission that's relevant to this topic. But it's the assignment of names in the root zone of the DNS, in other words, who gets to operate these top-level names. And it coordinates the development and implementation of policies concerning the registration of domain names in gTLDs.

But there's a very clear carve-out that also says that ICANN shall not regulate services that use the Internet's identifiers or the content that such services carry or provide. So ICANN doesn't do that.

So, therefore, it's up to others and generally it's up to law enforcement authorities and other public enforcement authorities to take action and hold name holders accountable if they use names in breach of the law.

And in turn, these authorities often rely on private sector organizations such as cybersecurity organizations that collect information about an incident that would allow appropriate investigation.

It's also interesting to reflect back on the derivation of WHOIS which has, I guess, brought us all together to talk about how do sort of look at the next generation of the information we provide in a registry. I went back and read the RFC -- the original RFC of WHOIS, which is 1982.

And it was actually a directory service for the individuals that were using the ARPANET at the time. And it required their name, their address, their phone number, and their mailing address, email address. Interesting, it didn't even get called email back then. It was called a network mailbox.

And then as it evolved, it became a source of contacts for the admin and technical people for the domain names of a few well-known large institutions. And in that case, it was very clear who the legal entity was accountable. It was just hard to find the relevant person amongst the hundreds of people that worked in those organizations.

Now it's a very different world. We've got hundreds of millions of domain registrations. And rather than large institutions, these are often registered by individuals and many of them act as sole traders. But we still have a need to identify the legal identity that is accountable for the use of the name. And we still need to be able to contact the registered name holder to resolve problems.

One thing that's often forgotten is that it's often the registered name holder is the victim, not the perpetrator, of activity using a domain name. Commonly people get their websites hacked. They get their emails hacked. And when you are investigating a problem, often the registered name holder knows nothing about it and actually needs help to resolve the problem. So it's not really necessarily that the registered name holder has caused the problem that has resulted in the use of the name.

I think it's worth reflecting on similar public registries, and there are several that are probably similar -- have similar characteristics to Internet domain name registries.

One is company information registries. So A lot of countries have laws that require those doing business to register as a business and register a company; and the information that is collected as part of that process

is often the personal data such as their name, address, phone number of natural people that are -- natural persons that are directors of the company.

Another example is car registration registries. This is where the registry will contain information about the vehicle such as what color it is, what make it is, what model it is, but also personal data on the owner of the vehicle which could be a company could own the vehicle or it could be a person, natural person.

And I think car registration is a similar analogy to ICANN in that if you think about a car registration body that manages the identifiers, the unique identifiers that are basically screwed onto the back of the car, sometimes you can -- they can be personally identifiable. So some people choose to have personalized number plates in some countries. But if somebody wants to be contacted, they'll generally paint that on the side of the vehicle if they're a business. But you don't typically see individuals putting their personal name on the side of a vehicle.

And then if you look at who's responsible for what's done with the vehicle, generally your license to use the vehicle, you can drive it anywhere you'd like. You can pretty much anything like you like inside that vehicle. You can put any goods inside that vehicle. You can put any people inside that vehicle. But the agencies that are responsible for issuing the number the plate doesn't care about any of that. All they care is that they can identify the person that owns that vehicle.

And it's other regulatory agencies, so if you have got a car parked in a car park and someone notices it, it seems to be full of drugs, then the

police will then investigate and then they will go to the registration authority to get information about that car.

If you're involved in a car accident, the first thing -- and let's say someone crashes into your car and then drives off, the only thing you really know about that person is their number plate. From that number plate, you can -- as a public in some countries, certainly I know in Australia and the U.K., you can put in the number plate and it will retrieve information from the registry with information about the car. It will tell you what make the car is, what model it is, what color it is, but not who was the owner of the car.

But that would allow you to make sure that you've got the right car because you might have only vaguely remembered the number plate and you can't quite remember the last couple of digits. You can check to see that you've got the right car as a member of the public.

Once you know you've got the right car, then you would take that information to law enforcement and say this person crashed into me and drove off. And then it's law enforcement that can get information about the natural person that is potentially the owner of that car.

So it's got a lot of analogies with our situation that ICANN doesn't care what's inside a website. ICANN doesn't care what's inside emails you send. That's for others. The only thing we do care about is that we can collect information about the parties that hold that domain name, that we can contact those parties, and it's up to others to take enforcement action on the use of those domain names.

Phone number registries are similar, too, in that they often have names and addresses of natural persons and most countries allow natural persons to opt out of having their name and address being public.

Country code domain registries have -- similar to the gTLD scenario. The difference, though, is that they are operated within a single jurisdiction. And most country code registries in Europe have obviously updated their implementation of their directory services to comply with GDPR law. So we can learn from those and see what they've done. But we still need to find a solution that works globally rather than in a single country.

If I look at the example of Nominet, just to give an example of how they've managed this, they display a fairly minimal amount of information in their public WHOIS. They have authenticated access for law enforcement agencies within the U.K. but not law enforcement agencies outside of the U.K. to access the registry for automated access.

And then they also have a form on their website where a legitimate user can apply to gain access to information, and they have to state the purpose for which they are gaining that information. And then Nominet individually assesses each case. And based on who it is that's asking for the information and what the purpose, they make an assessment of is it a lawful purpose. And then they'll provide that information to the party that's requesting that.

So they've developed a solution that they believe meets the law in both the U.K. and Europe more generally.

Regional Internet registries also, mostly regional Internet registries have information about the organization which is probably a telecommunications company or an Internet service provider or in some case large organizations that have I.P. address ranges. So most of the natural data relates to the contacts within those organizations.

But gain, RIPE for example, which is based in Europe would need to have a solution that's compliant with GDPR.

So there's a lot of, in IETF terms, working code out there. These are systems that are operating today and meet the laws in the countries they operate in and need to meet privacy law requirements.

If you look at how privacy laws evolved, many countries have laws that protect personal data. And really these have been updated in the advent of highly accessible and scalable information systems. Previously if you wanted to get information about a company, you would have to physically go to the company office and probably look at microfiche. And it would probably take you several hours to actually just retrieve one record. Now, you can actually access that record from here. I'm sitting in Barcelona. I can access the U.K. company registry. So they're much more accessible than they used to be.

And then the amount of information they contained is vastly larger in that if you go back a couple hundred years ago, if you look at births, deaths, and marriages, that information was typically held in each church. There was no centralization. You would have to go to the church where the person was born or died and that's where the record

was. Now, the records are much more centralized and the quantities are in the millions now.

So really the trend globally has been to progressively update privacy laws. And in Europe, I noted that in the 1950s, I guess after the second world war, there was a concern and a lot of misuse, I guess, of personally identified information happened during the war. And so these concepts were starting to be considered as part of a basic human right.

Then in the 1980s, Europe had a convention of protect automatic processing of data. So I guess this is when large-scale computing became prevalent in the 1980s.

By the 1990s there was a data protection derivative -- directive, sorry. But this was implemented in a range of different ways in each country. And the challenge for businesses was they would have to look at how the law is applied in each individual country in Europe. So there was a lot of business cost to that.

So the general data protection regulation in 2016 was to provide a uniform approach to all the countries and so a business could build an implementation once and that would apply to all the countries within Europe.

So it's essentially a standardization of privacy law. It wasn't exactly something new. Sometimes I hear people say, Gee, we've suddenly got this privacy law in 2016. Actually, we've had privacy laws in Europe since the '80s; but GDPR is a standardization of those laws.

So the challenge for ICANN is that we need -- this again applies to most privacy laws -- a clear definition of the purpose for what -- of collecting data. I think it's important here to distinguish the purpose between collecting data for the public registry which as we saw in Jon Postel's 1591 -- it's basically a service for the community -- from distinguishing that from collecting data for the business purpose of, say, the registrar. Registrars offer lots of services. They offer Web hosting, Web design, marketing services. They collect all sorts of information for their own business use.

But what we're concerned with at ICANN is the collection of information that will become part of the public registry, so effectively part of the public record.

We need to decide what's collected. We need to decide what fields are available for general public display, if it's unauthenticated; in other words, we don't know who is accessing the information. What fields should be available for legitimate users for lawful purposes? How would you authenticate those lawful or legitimate users? And our challenge is to come up with a solution that works across the globe.

We have data about natural persons located in pretty much every country in the world now. And we've got users that are often located in different countries to where the data is held.

And we've got different laws that apply both to the people, the natural persons, but also there's different laws that apply to the organizations that hold data. So that's -- that's much more challenging than

developing a solution for a particular country or even a particular region of countries.

It's useful to just refresh the privacy principles that are in GDPR. Again, these principles are common with many privacy regimes, but the concept of transparency, that the user should be told why the data is being collected, how it's going to get stored, how it's going to get processed, how it's going to be released to third parties.

The concept of a limitation on purpose. You should only be collecting data for legitimate and specified reasons.

Data minimization which is limit just to what's necessary. So if your -- and this is where you hear different discussions here. So for a registrar, a registrar that is collecting information to allow them to provide an email service doesn't actually need a postal service. Because the registrar never delivers the mail by post. It delivers the mail electronically. So if you ask a registrar that doesn't have any other ICANN requirements, it would just say well, we -- what we need to do is collect the credit card. That's good enough for us. But for a public purpose, you might want to collect more information, and that's for the community to decide as to what information should be collected.

Accuracy, the data must be kept up to date. In the GNSO there's a standard that says every year the registrar must remind the registrant or registered mail holder of the data that's held in the public registry, in the WHOIS, and that customer has the opportunity to update that data. So that's an attempt to keep the data up to date. And then obviously registrars provide services to allow customers to come in at any time

and update their data. So I think on the accuracy side we basically are GDPR compliant because we have an ability for people to update their data.

Storage limitations is that if in the normal customer situation you would say, as soon as that customer stops paying with a credit card, you don't need to store any of their data anymore because they're no longer a customer. But a public registry usually has longer term storage because if it's dealing with some legal issue, might be a tax issue, most company -- countries require certain information to be held for numbers of years to allow the application of tax law, for example. So storage limitations is identifying what do we need as the ICANN community for how long information should be retained. Maybe both during the registration, then after the registration has lapsed, what information should be retained.

Integrity and confidentiality is basically security, that the data must be secure.

So I think one of the things that I've heard often in these panels is people sort of state what they think are requirements, and I think they've being stated numerous times. So rather than, you know, trying to get each panel member to try to restate them, I've just summarized some high-level ones here. Certainly one of the assumptions I'm hearing this week is we have to back our policy development process. You know, there's a temptation to find that it's too slow and to pull resources from that process and focus it elsewhere. But if ICANN's to work, we have to make sure we resource and contribute and help

people in that policy development process. So my opening assumption is that will be successful and they will produce a policy.

Any solution that is produced must obey data privacy laws. GDPR is just one of them actually. There's multiple.

Any solution must allow law enforcement and public enforcement bodies to investigate and hold the name holders accountable for the use of the domain name.

Any solution must provide protection for people that are at risk. So often I hear anecdotes where it could be there's been a -- a marriage breakup, there's some sort of violence involved that the party that's -- that's had to move to another geographic location and they want to protect their geographic location basically to protect themselves from violence. So we've got to think about those kind of scenarios, that this data can cause real harm if it's released to the wrong person.

RDAP, we hear a lot about that. Again, I think it's a no-brainer. The technical community basically believes that RDAP is sufficient for the purposes of which most of the discussions have envisaged. But RDAP is just a language. It's just a way of exchanging information. RDAP is not a solution. It's just a language that we've chosen to use to exchange information. But it has some powerful features. Some of those powerful features is it does support the concept of having information distributed instead of centralized. And it has standard information flows which overcome some of the problems with the old sort of thin WHOIS model where there are lots of different implementations.

It's very similar to EPP which is a standard that was developed to allow registries and registrars to communicate. But it's not a substitute for policy. You have to have policy then RDAP can implement that policy.

The other assumption here is that registries and registrars are accountable for the data that they hold. They collect information for a range of purposes, not all of which relate to the domain name, and they're accountable for how it's processed and how it's disclosed. So they have to take responsibility as well.

So I guess the opening question for the panel then is, having considered the background, you know, consider other public registries, how the problems of protecting personal data have been managed within those registries, how the concept of having legitimate users accessing information that's not available to the general public, what protections need to be in place, et cetera, understanding the context that privacy laws are developing globally, our challenge I guess is to come up with a timely solution. And the question for the panel really, the first question here is, what are the impediments that they see within ICANN after a week of discussion of this topic, what do they see are the barriers or the impediments to finding a solution, and what do they think they can do to overcome those impediments? And what can each of you do? And we've got a room full of people. There's hundreds of people in this room. How can you help -- help the policy teams, help the people that are in the different stakeholder groups, reach a successful solution?

So I'd open it up for the panel for their views on how do we find the best solution and overcome any impediments. Ashley, go ahead.

ASHLEY HEINEMAN: I'll jump right in. Yeah, I'll start at the high level and not really get into, I think, a lot of the details that we're talking about. I think a lot of the impediments, at least that I've faced, you know, in the last year or so, is people coming to the table with preconceived notions about what the other side is thinking and doing and what their motivations are. And also what else I've also learned is that once you actually sit down with individuals, particularly individuals who represent different views and prospectives and interests, that once you actually start talking through the issue, we're actually not as far apart as we think we are. But I think we need to have more opportunities to actually talk and be constructive and be working towards a common goal and avoid the situations that we tend to find ourselves in where we are stating our positions. And we're not really working to find common ground. And I'm optimistic that we can overcome them. I've seen them be overcome. But I think this is just such a long-standing issue that has so much baggage, it's hard to check that baggage at the door and just work together constructively. Thanks.

BRUCE TONKIN: Yeah. I think the challenge you have there is that people question motivations and they go, well, you were only put in that position because you have this particular view, and the reality is that most people's views are reasonably balanced when they're talking in private

but sometimes they come to these public forums and they'll just state just one extreme part of that. Perhaps one way of dealing with that is just ask lots of questions. So instead of jumping in when you are having a conversation with someone from another stakeholder group, don't just say, here's my position and I'm right. It would be, ask them more questions about why they think what they do, and then you might be able to find more middle ground. But yeah, definitely, I think stronger facilitation and maybe schools for people in asking questions as opposed to stating positions could help. Milton.

MILTON MUELLER: I think the main impediment is very clear to me as an EPDP member and that is there is a very strong hope in certain parts of the community that we can somehow recreate the old WHOIS or somehow get access to the data with the ease and freedom that they had before. And, of course, over the 20 years that WHOIS existed, there was a build-up of very strong interest in equity in access to that data. Entire businesses were based upon it. And so what happens in the EPDP frequently is, we end up having a debate about access and everything becomes subordinate to this interest in access, even when we should be discussing something else.

So I think the obstacle can be overcome if we simply concentrate first on the first step, which is finalizing the temp spec and understanding what is actually going to be collected and what are the purposes and what particular data elements are needed and when they need to be transferred, and we should be able to agree on that if we set aside the

question of access to the next step, which our charter actually requires us to do.

So if we don't confuse ICANN's registries and registrars purposes in collection data with third-party legitimate interest in accessing data and we concentrate on fixing part one, answering the gating questions in the charter, and then moving on to access, I think we will make progress much more rapidly. But if every purpose discussion and every collection discussion becomes a proxy battle over access, which we can't actually solve yet, we're going to be spinning our wheels for a long time.

BRUCE TONKIN: So just a quick question for the audience. So Milton, you stated there's a fear that people think that we should really just return to the old world and return to the way WHOIS was. How many people in the room think that's a viable solution, that we return to the way WHOIS was? One person. So I think we've put that myth to bed. No one thinks that's the case. So we -- we are moving forward. And I think you're right, Milton, that if you -- if you think about it, if you go back to the principles around any privacy law is, what's the purpose that you're collecting for and what's the information you need to collect to meet that purpose. Absolutely that's got to be an opening starting point. Yeah. Flip.

FLIP PETILLION: Thank you, Bruce. Actually I would like to remind everybody of what Cherine Chalaby said on Monday morning. He said, we have to search

a balance between what we collectively need and individually want. I think that was brilliantly put. And that is what the GDPR is about. I think we need to, everybody, remind ourselves, remember ourselves of what the GDPR is. Where it comes from. What the aim is. And frankly, when people were discussing the draft GDPR, they were never thinking of what we are dealing with today. They were really thinking of protecting people for receiving advertisements and spam, et cetera. But not the problem that we are dealing with today.

What we need is everybody in the discussion should really think, do I understand what the real goal is here and is what I want in balance with the interest, not the rights but the interest of others. I don't think, as some people seem to present it, it's not a choice between the best and the (indiscernible). We have an unbalance now. And that unbalance is clearly uncomfortable for quite a number of people in the community. We need to bring the balance in an equilibrium again. And once we understand that, then we will have much better discussions. This is what it is about. The balance.

BRUCE TONKIN: So your view is, accepting the -- the community needs to accept that there needs to be a balance. Is that right?

FLIP PETILLION: Absolutely. The whole model of ICANN is based on a consensus, Bruce. It's about trust. We want to create trust for everybody. And the trust is

the basis of the consensus. And the consensus is the base of the balance. Balance of interest.

BRUCE TONKIN: Okay. So let's have a show of hands. Who thinks that what we should be focusing here as part of our community work is getting a balance between being able to protect the information and being able to provide the information? Looks like a pretty clear majority. So that's good. So I think we're saying that WHOIS as it was, we can't go back, but we're also saying to move forward, we've got to find a balance. And there's very strong support in the room, I think, for doing that. So I think again, that's one of the assumptions that we have, that all of us have, is that we've got to balance those interests.

How do you think we get to that balance? What's the -- what's the -- that's the hard part.

FLIP PETILLION: With a lot of good will and not only thinking at what is applicable in the GDPR but also outside. Like law enforcement, protection of consumers, very important topic, protection of children. There are all the laws that are applicable. Not only in Europe. Don't forget that we have an eCommerce directive in Europe which actually provides for a mandatory provision of contact information of the holder of the website. So at first sight that goes diametrically against what is in the GDPR, but it's not. It's not because every single piece of legislation in Europe, be it a regulation, be it a directive, always will provide that the

implementation and the application of the regulation or directive must be in a balance. A balance with other pieces of the regulatory framework that is applicable. So we have to really see the entire -- the global picture.

BRUCE TONKIN: Yeah, I think the more that in the policy discussions you can reference the specifics of some of those other laws, because again, they're just examples of how this balance has been achieved. As I mentioned in the example registries, they've all got their balance. They've all got their balance between providing enough information to the public to allow them to understand, you know, who's responsible for a particular record, but also an ability to get the more detailed information when it's really necessary. Hadia.

HADIA ELMINIAWI: Hadia Elminiawi for the record. So in my opinion, the challenges -- I would like to talk about the challenges from a practical point of view because by now we all know that the registration data is not open anymore. It's a closed gated registry of data that will be available to -- for disclosure, based on third parties legitimate interests. So I would like to -- and speaking about the balance that you were talking about, we need to acknowledge, of course, that there -- that balance is and will be required. But it's also we need to know that we are not the ones that are going to do this balance once it comes to disclosure, once it comes to implementation. And then setting this aside and --

UNKNOWN SPEAKER: WHOIS?

BRUCE TONKIN: We won't be doing that balance? So you're saying, you don't think we will be doing the balance?

HADIA EL MINIAWI: No, we acknowledge that the balance is required and you should balance the needs between the third parties or the -- the people with legitimate interests and the registrants' rights. But when it comes to the implementation and the disclosure, we are not here that's going -- we are not going to make this balance case by case or we are not -- we are not the ones that are going to implement this or make this balance right now.

So in some cases, you know, the -- the -- so we acknowledge the principle, we acknowledge the facts, but in a practical -- from a practical point of view, when it comes to the real implementation and disclosure of the data, we are not the ones that are going to decide in this case the balance is successful or not. So we need to keep this in mind, in my opinion.

And then I would like also to tackle the challenges from another practical point of view. So whatever work we do or policies that we are about to come up with, need to be practical, implementable and, of course, in addition to GDPR compliant but practical and implementable

is also very important, to come out with a policy that no one would implement and it's not practical to implement. It's a challenge. And in my opinion, to tackle this, some requirements are necessary. For example, industry standardized processes. This is required for the registry, registrar, and registrant network, accreditation services and how are we going to do this.

And who is going to do this? Also other challenges related to the -- taking the liability risks of the contracted parties. It's important to -- so, if you have a policy that does not take this into consideration, you will have no one implementing your policy, right?

So, in my opinion, these are all challenges that need to be tackled now rather than after, so in parallel with whatever we're doing now, with the policy work that we're doing. And, hopefully, we are going to reach consensus over something that we are all happy with.

But then comes how do we implement this? And I think working on this now rather than later is what is required and is the biggest challenge, in my opinion.

BRUCE TONKIN: Yes. What you're saying, in terms of getting a timely solution is the policy right. And Milton is pointing out we need to have enough of a community focused on getting the policy right. But, to get an ultimate solution, you have to be thinking about implementation as well so that we don't suddenly start thinking about implementation after the policy

work is finished. We've got to be thinking about it in parallel. I would agree.

Nick.

NICK WENBAN-SMITH: Thank you. Nick Wenban-Smith. I'm here as a representative of the contracted parties. And I think it was very nice that somebody actually mentioned the risk to the contracted parties.

And, when I look at this question, I like that the word "timely" is an inverted commas. Because it's now October 2018. And this law came into place in May 2018. So a timely solution would have been minus 12 months away.

But I think, broadly speaking, although it was extremely late in the day and very rushed in terms of what we had to do, the temporary specification was something that the contracted parties are broadly happy with. So, as soon as we can get through the EPDP process to formalize that, the better. And then we can talk about access.

But, in fact, we've all had to imply our own access policies already. Because, since May the 25th we've had to comply with the law. And that includes access.

So one of the very interesting challenges of GDPR is it is about principles. So you have to balance out the principles of legitimate interests with the privacy rights of the data subjects of all the people that we've got. And that is quite challenging. We have, through

necessity, in the absence of any global formal policy, to do it all ourselves. So you will have a sort of a patchwork quilt, unfortunately, of different policies for disclosure.

And I know what we do in the U.K. is legal because we get hundreds of access requests. And, actually, I've had some complaints. And the way that you know that you're compliant in terms of data protection law is through the rearview mirror. If somebody doesn't like what you're doing, they complain to your data protection authority. And they write to you as the data protection officer for your organization and say, "We've got a complaint."

And I've had a complaint about disclosure of data to an intellectual property rights enforcement body. And that complaint was rejected. So I know that my process for disclosure is basically robust enough to at least start to stand the types of challenges we get from data protection subjects who quite rightfully exercise their rights to make complaints if they don't like how they're data is used.

So we're starting now to build up a body of experience with dealing with actual post-GDPR implementation experiences. So I think we need to build those into the solutions going forward. Because what we do know is that we get requests which we cannot comply with. So we get about -- in the last three months we've had about 750 requests. So we uphold 96.5%. But some people just don't give any reasons. That's clearly not a compliant request, so that also needs to be built into these systems.

BRUCE TONKIN: So what you're saying is -- like what Hadia said -- is there are decisions that need to be made locally based on facts at hand on providing access to a particular piece of data. But there also needs to be compliant mechanisms for both sides, presumably, so that the party requesting the data has a way to lodge a complaint if they're not receiving service. And the data subject, if you like, has got to be compliant with that information that's held or released.

NICK WENBAN-SMITH: The mechanism is already set out in the legislation. It's already there.

BRUCE TONKIN: That's nice. Excellent. Greg.

GREG AARON: Thank you, Bruce.

Part of the conversations that are taking place this week are about those responsibilities that the GDPR is putting on everybody. And that's a good thing.

It's about accountability in some ways. But it also becomes a discussion about managing risk. Everybody has those responsibilities. And, of course, there are sometimes penalties associated when you don't meet those responsibilities.

Of course, the problem with managing risk is that it sometimes becomes a discussion of cost.

What must I do in order to protect the data appropriately? What risk will I incur when I perhaps have some of it shared?

And that discussion of cost I think is undergirding part of the conversations.

One of the problems is that everyone is evaluating the risk and what the law says. And those evaluations are very uneven. We even see that amongst the European ccTLDs, the RIRs and so forth where they're making different decisions based upon what advice they get and their appetite for risk.

And that unpredictability is something that we're slowly starting to discuss and figure out. Because, ultimately, we want a system in which there can be some surety and confidence that the data is being handled appropriately by everyone involved, those who collect it and those who may receive and use it.

And that's the balance point we need to get to. Because, ultimately, for cybersecurity people, it's important for us to use that data. Because we have people to protect. And the law says we need -- you know, we can have that access, if it's done properly.

So we want to find that appropriate balance. But we have to get to that point where we find a way to make it happen.

BRUCE TONKIN: Let me just jump to someone else. Chris.

CHRIS LEWIS-EVANS: Thank you. First I'd like to highlight the progress we've already made within this group. And I think your first question to the audience was really good. Because I think, if you'd asked that same question at ICANN 61, for instance, I think there would have been a vastly different response from the audience.

I think that change in acceptance of what is needed is because of the understanding of the different requirements required from all parts of the community within ICANN.

Both from the data protection side and also from the parties that are entitled to gain access through their legitimate purpose and legal basis. And, really, that understanding has come about from understanding people's requirements rather than people's solutions.

And I think in the EPDP, where the most progress has been made is where we've talked about what each parties' requirements are rather than what their solutions would be to answer their requirements.

And I think that's really the best way of getting a good understanding of everyone's real requirements and then be able to provide that balancing act that, you know, we've already talked about. And it is really about understanding those requirements that enables you to make a good balanced decision.

BRUCE TONKIN: Which is the purpose that Milton is referring to, actually. What's the purpose that you're collecting the data? And then what data do you need to make that purpose, basically?

CHRIS LEWIS-EVANS: Exactly. And I think, to come to a timely solution, I think we really need to focus on those requirements and then balancing those requirements with an understanding of everyone's needs as well.

BRUCE TONKIN: It's interesting. If you look at IT projects -- and people do reviews of IT projects -- the number one reason an IT project doesn't deliver is because they didn't spend enough time getting the requirements right. So I think that's a common theme that we're hearing that we have got to get those right. Cristina.

CRISTINA MONTI: Thank you. Cristina Monti, European Commission. Echoing also some of the remarks we already made.

If we look at the way forward and what are the impediments, I think it's to also recognize that these issues have been here for a long time.

And maybe one thing that the GDPR managed to achieve was to really bring forward the issue and oblige all of us to come forward with a solution in a short time frame.

So I think that a lot has happened. We saw from the audience that nobody nowadays thinks that privacy is not important. Data -- everybody agrees that data -- personal data is something valuable. And those who handle personal data should also be held accountable for how they use and handle the data.

And I think that even also hearing the ICANN environment, a lot of progress has already been achieved in the sense that now at least we have all our communications channels are open. The WHOIS reform issue is now on the agenda in many high-level discussions also outside of ICANN. So I think that, in this sense, progress has been made and discussions are moving into a more mature phase.

And now we're focusing on the actual solutions. And here is where the real issues come. Of course in the operationalization of the principles that we saw is where the trick lies. And I think that, if, in one way, the multistakeholder model that we have here at ICANN is proving challenging because you have many different interests -- and sometimes discussions can be very polarized -- I really believe it is only the multistakeholder environment that it is possible to find a sustainable solution.

Also I think that in this very moment we know that steps have been made to ensure that the WHOIS registry is GDPR compliant. But, again, we are not still at this stage of a predictable and final solution.

And I think that this has an impact on many players, as we know very well. And sometimes I think it's neglected the aspect that even the individual registrars or individual users are not aware of how their data is managed, who to contact if they would like their data to be corrected, and so on.

So, even from that perspective, we are now in a situation where we are sort of in the middle.

BRUCE TONKIN: I think that's a good point you make about individual users. Because my experience is most individual users don't know about the existence of WHOIS, for example. Most people in this room do, because most people here are professionals in the IT industry or have been to an ICANN meeting before and heard about it.

But the average user doesn't think to use WHOIS. The average user would probably, if they have a bad experience on the Web site, they'll probably report it to their consumer affairs department or some other group without even knowing these services exist. And they're certainly not aware that their information has potentially been published somewhere. Making that transparency stuff, I think, is an important principle. Yeah.

CRISTINA MONTI: Absolutely. And just to complement as well and to relate to the issue about risks that was raised, I would like to make the point that the GDPR, which builds on rules that have been there for a long time, actually, should be really understood as an incentive for all players who have to do -- have to deal personal data to do that in a lawful, transparent, and accountable way. And the GDPR now, even for players outside of Europe, the situation has improved in a way that there will be now much more uniformity in the way the rules are applied because you have mechanisms now in place to do that.

So, before the GDPR, you had many different national legislations. And with the GDPR you now have much more uniformity. So, for a player outside Europe, it's going to be much easier than to deal with these issues. So I just wanted to also make this point. Thank you.

BRUCE TONKIN: Certainly raising a level of standardization globally, I think. Hadia, and then I'll come back to Nick.

HADIA ELMINIAWI: As mentioned before, challenge is a misconception. I would like to note quickly that we are not collecting data by any means for the purpose of those with third party interests or those of interests that -- those who have interests in accessing the data. Because this is a misconception.

I've heard people saying you are collecting data for law enforcement. You're collecting data for cybercrime. You're -- required by those people.

And I want to assure everyone here that the data is collected only for the purpose required for -- to satisfy the service, to fulfill the service. So yeah.

BRUCE TONKIN: Which is the data minimization principle. Only collect what you need. Identify the purpose and collect what you need.

HADIA ELMINIAWI: And third parties will eventually have access to whatever is being collected for those purposes.

BRUCE TONKIN: Sure. Nick and then Milton. I want to be careful we don't get down to the weeds of a particular data elements but get the principle.

Nick?

NICK WENBAN-SMITH: I was going to say there is a risk, and the risk is all borne by the contracted parties. That's one of the things that drives us toward a more conservative policy. I think there's a broader point. I don't really have much personal fear of everyone speaks about the very large financial penalties which are potentially going to come through. And, really, for responsible organizations that is just not a serious consideration for me.

I'm much more concerned in this age of digital citizenship that actually a reputation for handling data appropriately and legally in compliance with the law is actually a competitive advantage now between our contracted parties. That is actually a higher order sort of reconsideration, from my perspective. It would be nice to try to get some of that into this as well.

BRUCE TONKIN: I think what you're picking up there is trust.

A lot of people now are losing trust because they found they provided data for a particular service they take. And then they, unbeknownst to them, data is being given to a third party or being used in a way that they didn't understand.

I think a key thing, coming back to the high-level goals of ICANN, is we've got to have people trusting in the domain system, trusting that they can register a domain, and trust that we'll look after that data properly. Otherwise people won't register domain names. They'll go use social media instead. I think that's a really key point.

Milton.

MILTON MUELLER: I want to pick up on something that Ms. Monti said. This is a very high-level issue regarding the role of ICANN as a global governance institution and how it relates to states and governments and their laws. Because I think that's one of the key issues that we're dealing with here.

So I was not a big fan of European data protection regulation prior to the GDPR. But I have to confess that, in retrospect, I think Europe did the world a favor by setting a standard.

So in the regulatory and governance fields we have something called "the California effect." And that was when the State of California set pollution standards for cars that were much more stringent than the rest of the country. And the manufacturers had to decide do we make a California car and a different kind of car for other jurisdictions, or do we just make one car? Essentially, that's what's happening now with

the GDPR and privacy is they've set a standard. And I think the issue is -- as a global agency, can ICANN meet that standard? Or will we get into a set of competing standards?

For example, if the United States decides they don't like what Europe has done, will they set a different and conflicting standard, and will we have a more fragmented system? I think that's one of the big issues that we have to be aware of as we're talking about compliance with the GDPR.

And I just use the United States as one example. Any other large jurisdiction could create the same problems. Could be China. Could be India. Could be maybe Canada? I don't know.

But you get the point is that we are dealing with a very tricky and very important issue of the status of ICANN as a private sector based global governance agency, which I think most of us here support, versus a state-based system of territorially fragmented sovereignty in which we could have multiple systems.

BRUCE TONKIN: Yeah. And I think, if you looked at the history of GDPR that was effectively happening within Europe in that each country was talking the high-level principles but interpreting them differently, which was a cost to businesses. And I can imagine a business might go after a large market and meet the requirements of Germany or something. It's a large market. But, if you're a smaller European country, they would go I can't trade there because their privacy laws are too complicated.

So I think there was a benefit in unifying that people can see a large market. Just as California -- if it was one of the other U.S. states that perhaps had a small population and they set an emissions standard, it probably wouldn't have mattered. But California is a massive economy in its own right. Car manufacturers would build cars for that market. And then the others get the benefit of that.

Yeah. Flip.

FLIP PETILLION: Thank you, Bruce. Flip Petillion. I just want to add something coming back to trust.

There is trust when you give information, but there should also be trust when there is a request for information. And everybody should actually show commitments to contribute to that trust. And I think Nominet has been giving a good example. We saw another example by Mr. Noss from a particular registrar. And these are good examples of commitment, of willingness. In Europe we would call it good faith. It's really a will to come to a workable solution. And I just wanted to throw that in.

BRUCE TONKIN: Yeah, and one of the key points of access to data, too, is that when a party requests access, they then become accountable after they've got that data, and need to be held accountable for what happens to the data. So it's not just you have access to a piece of data, now that accessing party can do what they'd like with it. So that accountability has got to be part of the trust framework as well. And people that

access data and don't use it appropriately lose their access. It's fairly simple.

I might jump to the audience at this point. I've got a couple of other questions that I'd like to ask the panel, but given this is people in the community more generally, I would like to open it up for any question for the panel, and particularly sort of addressing this point, really. How do we get to a timely solution? How do all of us help reach that solution?

I'm not quite sure how we're doing questions here. I can see one in the front row, anyway. Let's start here.

HOLLY RAICHE: Just a question. In terms of purpose, you have to test the purpose in terms of ICANN, but the ICANN remit is fairly broad. I've heard arguments that the remit is only about technical and about technical issues. I think if you're looking at ICANN's mission, there's more than that. If you get the data from somebody, it isn't just to provide a technical surface. It's to do things like enable transfer of the thing, it's to do dispute resolutions. When you look at purpose, I would be concerned if it isn't at least broadly drawn so that the mission is, in fact, the management of the whole system and its stability.

BRUCE TONKIN: Yep. Good things. Any comments from panel members? Ashley?

ASHLEY HEINEMAN: Yes, and I think it's been a long slog but the EPDP has come to recognize that. In terms of developing our purposes, I think we've captured just about everything that you've mentioned, and that's a good thing. I don't think we're quite finalized yet, but there is recognition of that, particularly with respect to security, stability, and resiliency of the Domain Name System.

BRUCE TONKIN: You have another question? Oh, we work with these things. So number 1, then number 2.

UNKNOWN SPEAKER: I am number 1.

BRUCE TONKIN: Now I'm getting the system.

RACHEL POLLACK: Rachel Pollack with UNESCO, and thank you for the very interesting discussion.

At the last ICANN meeting that I went to in Copenhagen about a year and a half ago, the European -- sorry, the Council of Europe had brought in data protection commissioners to help facilitate the discussion between data protection commissioners and members of the community and that was quite enlightening. And I understand that they have -- There's a bit of an echo. I understand that they have

released a guide earlier this year on data protection issues within ICANN. So I wondered if any of the members of the panel had -- have looked at that, what they think. If they foresee again to have these discussions with data protection commissioners to ensure that any model that is ultimately adopted is, indeed, in-line in a sort of structured, systematic way.

And then just to make a plug for my own organization and not directly related to ICANN, but we have published two studies looking at issues of freedom of expression, privacy and transparency. I think that talk about that balance between these varying human rights and how -- how to strike a balance. So I would recommend that you -- that you take a look at the UNESCO series on Internet freedom.

Thank you.

BRUCE TONKIN: Just a quick comment, just with respect to data protection commissioners. So ICANN did reach out and see if we can get some speakers there and involvement in the panel. They actually got a parallel event this week. There's some sort of European data commissioner event, so that was unfortunate.

But to address the question -- Yeah, Hadia.

HADIA ELMINIAWI: So responding to your question, definitely we did take into consideration all the correspondences with the European Data

Protection Board and all the letters and advices that have been provided to ICANN. So this -- When doing this work, in developing the policy, we did look at everything that was provided, and we took it into consideration.

BRUCE TONKIN: Great. Cristina.

CRISTINA MONTI: Just to maybe clarify and complement the question. Of course we are aware of the guide provided by the Council of Europe, which is a useful document; however, it goes into the principles part. And here we are dealing with the GDPR, and the Council of Europe is more in charge of the Convention 108 which is a different kind of instrument. And this should be kept in mind.

And about the data protection authorities, you're right, they couldn't come to this meeting because there is a big international, global meeting taking place now in Brussels, but I would like also to reassure and stress that European data protection authorities are aware of these discussion, they are following the progress that has been made, and they have been providing guidance as long as they were asked to provide insight on specific issues, and I think that they are quite open to continue this discussion. And this goes also to the fact about this fear of fines.

I would like to remind that data protection authorities, yes, have increased powers, but they have a whole range of tools at their

disposal. So before getting to a fine, I would expect them to use the other tools they have, like issuing warnings or this kind of -- issuing an order. And, therefore, I think that they are showing also willingness for dialogue in this sense. And I think this is very important.

BRUCE TONKIN: Yeah, I think that's a very valuable point. So in other words, the starting point of compliance or enforcement is a cooperative approach, which is helping people understand what their requirements are, in a way. And then only if they're ignoring you that you'd escalate it. Yeah.

Number 2.

UNKNOWN SPEAKER: This question is for Nick and it's from one of our remote participants. Contracted party experience on access is very valuable. What numbers of third-party access requests has Nominet received since May 25th from non-law enforcement? Are you publishing a transparency report with these requests, disclosures, time frames and appeals? Is the CPH considering publishing these?

BRUCE TONKIN: Over to you, Nick.

NICK WENBAN-SMITH: Thank you for the question. And it is, perhaps, a sort of more empirical approach to policy development to look back and see what the actual experience has been.

So we always had a data access policy even before the GDPR, because we had some data elements that we didn't publish in our public WHOIS. This is for the .UK country code which is the biggest -- one of the bigger country codes. So we have 12 million domains, and that sort of gives you quite a good idea as to numbers.

We have seen an uptick in requests for data. So prior to May 25th we did not in any case publish email addresses or phone numbers in our public WHOIS, so people could still request that through a data release process, and we had a handful of those a month. And post GDPR, we have had -- so we are collecting the numbers and looking at them very carefully. It's one of my little hobbies of data analysis. So, yeah, we get a set, almost 800 requests for individual domain name registration data in three-month period. And actually what I'm going to do, I think, is we're going to have a May the 25th plus six months and then do a little report about what our experiences have been, because it's still quite early days.

But we -- When we receive requests, we obviously analyze them, and we actually even form the data subjects that the data has been requested and if we've agreed to the request or not. So that's part of the transparency as well.

So there's a number of different reporting elements that happen in each individual request, but I think, yes, absolutely going forwards, we

will be looking -- looking certainly on an organization basis. And within the contracted parties we have very active discussion groups on all of these sort of topics and collecting our information and expertise together and trying to use that to actually look at the actual experiences and try to work out what is working well, what isn't working well. And I would say the numbers have not been so large in terms of data requests that some people were suggesting. That's partly because we do provide national law enforcement agencies with quite a lot of data without having to make individual requests. But -- So I'm a bit nervous, and I know the RDAP solution is technically to provide access, and contracted parties generally thoroughly support that, but I am quite worried based on some previous experiences with -- with the way that ICANN has actually implemented things that we might end up with a very complex and expensive implementation system which is far overengineered for overengineered for the actual number of requests that people are receiving. And you should remember because although the .UK is a big registry, we also are the national registry for the Welsh domains. They have a few tens of thousands of domains and we have received zero requests for data. So to implement something for those -- And that, by the way, for the new gTLD program, would be quite representative of many of those new gTLDs.

So to implement something very complicated with a lot of costs and overhead for something where, really, actually it doesn't justify it in terms of the scale and the cost of implementation. So that would be something else to -- to look into, because I would be interested to know,

amongst the smaller registries, have they actually received any requests at all.

BRUCE TONKIN: So just to restate the number, I think the question was leaving aside law enforcement, if I heard correctly, 800 a month; is that right?

NICK WENBAN-SMITH: 800 in three months. A quarter.

BRUCE TONKIN: 800 in three months. So 800 a quarter. Thank you.

Mic 1. I think you need to get yourself a number.

UNKNOWN SPEAKER: Thank you, Bruce. I want to ask you something because you made a statement regarding of one of the principles of the GDPR regarding accuracy, and you said, more or less, the issue is solved because there are in place accuracy standards to update once per year from the registrant all the items in WHOIS that are referred to. And this is an ongoing discussion also we have in the EPDP. And I think this is not far from having a good solution there, because the question is how can you serve a purpose if you have inaccurate or fake, or whatever, data? How can you serve a purpose? And I'm not talking only from the point of view of third parties that won't have this but also for the contracted parties or ICANN or whoever who wants to have this information -- for

example, to contact somebody -- and finds out that this data that they have in their -- in their position are not accurate or are obsolete or whatever.

So I think this is an issue that we put under the carpet. I understand that there is a lot of cost, maybe, involved or it's a tedious problem, but I don't believe that we have reached a satisfactory solution so far.

BRUCE TONKIN: So this is on the authentication of the data that goes in. Yeah.

Any comments? Milton.

MILTON MUELLER: Yeah, I think the ghost of the old WHOIS is still haunting many people, and the accuracy issue is a good example of that.

So we had indiscriminate access to personal contact data, and both good people and bad people, for obvious reasons, put inaccurate data into the WHOIS because they knew it was going to be published. Once that data becomes shielded from indiscriminate public access, then the accuracy problem is a completely different one. Yes, there will be people who put false information still, but that will not be the case for most of the legitimate registrants.

So -- And furthermore, the discussion of verification of data is a orthogonal problem to the principles regarding what we're collecting and why we're collecting it. It's a separate policy issue. There's a whole set of policies that already exist regarding accuracy, as we all know, and

it -- this is a good example of the impediments to progress, is that people start attaching things to the process of deciding what we're collecting and how we're complying with GDPR that are really orthogonal to GDPR compliance and could be addressed through other policy processes later on.

BRUCE TONKIN: Okay. Number 2.

FIRDAUSI: Thank you. My name is Firdausi.

I would like to ask maybe for the example about the conflict regulation. For example, if we refer to the legal principle like specialist (indiscernible) or like (indiscernible). So one is the specialist regulation will repeals the general one, and the other one is the newest one will repeal the oldest one.

So if we look at the example , for example, because there is some purpose for investigation, so if we look, for example, between GDPR versus RIPA, which is Regulation Investigatory Power Act, so how does this legal principle can be implemented? Or maybe there is another legal theory that can be implemented. And also, because given the GDPR applies not only in EU but also outside of EU, so in practical, how is the government from other region or maybe another region who have similar institution, like EU, for example, in southeast Asia ASEAN, do you comply with this? Is it more like we create multilateral agreement or

maybe it's more like a bilateral agreement or maybe just case-by-case (indiscernible) legal assistant?

And also because there is some -- I think I hear from the panelists talking about the awareness of the privacy as well from the consumer, and so on. So what do you think the role of the privacy officer or data protection officer in the future? Because it means this -- by EU setting the standard of GDPR, I think the needs for many companies around the world to have privacy officer or data protection officer is even more urgent.

Thank you.

BRUCE TONKIN: Thank you. I'll get a couple of responses to that. Let's first ask Nick. So do you ever get responses or requests for data from parties outside the UK that are under different legal jurisdictions? And how do you manage that as a data protection officer?

NICK WENBAN-SMITH: Thank you for the question. I think -- well, we have a standard process and it doesn't matter where you are. So we do get a few requests from outside of the UK. Most of our requests are from within our jurisdiction, and I think that's partly because that's where most of our registrations are based and it's partly where our legal standing is, it's where our government and local LEAs, the people we have the best networks. But we do have many registrars outside of the UK, and we have many

registrants outside of the UK. So the same policy applies. It's a global policy.

And I think when we look at how GDPR has worked in practice, it's quite nice that there has actually been a high degree of standardization across what we do.

So, yeah, it's the same -- same -- same regardless of who makes the request.

BRUCE TONKIN: So since you aren't here in this, because you're located in Europe, that you're bound by the European law, and so you're basically applying that law to any request you get from outside. That's what that sounds like.

NICK WENBAN-SMITH: But in terms of how we implement it, in terms of access, it's the same policy for everybody. It doesn't have to be, but it's much simpler for us to do it that way.

BRUCE TONKIN: You try to standardize on it.

NICK WENBAN-SMITH: Yeah, absolutely.

BRUCE TONKIN: Perhaps, Ashley, if you could comment from a different government or a government outside of Europe how you think registrars or registries should take into account other laws, maybe U.S. laws that may be different from GDPR.

ASHLEY HEINEMAN: I won't speak for the U.S. because I'm not really in a position to do so. I'm here to speak for the GAC. But what I will say is that I think we need to be careful about referring to the GDPR as a standard for global privacy and data protection. It's -- There's a lot of data protection regulations out there. I think -- you know, not to be too flip about it, but I think what's really made -- brought this to the fore as an ICANN issue is the fact of all the risk and liability it put on the contracted parties.

So I think the hope is that a lot of what's in GDPR been generally within the same kind of regiment of other data protection laws, but we also have the conflict with national law procedure that still exists. How that's going to come into play is one thing. But I think what's of interest to governments, too, is -- in terms of how this all gets implemented, is the ability of law enforcement outside of the European Commission, because it's very clear that the GDPR permits, you know, a certain, you know, I guess easier justification for access for European law enforcement. It's not entirely clear if that applies to the rest of the world's law enforcement. So that is a consideration.

Thanks.

BRUCE TONKIN: Thank you. Okay.

Number 1.

UNKNOWN SPEAKER: Janis Sordie (phonetic). My question is about your comment on receiving 800 requests in three months.

So before GDPR, how much requests did you receive a month, if you know, for the past couple of years? Because that would be, I feel like, more interesting data on the real requests that people have in general, the general community.

NICK WENBAN-SMITH: Thank you for the question. So it's not exactly the same month on month because sometimes you get a big request from a particular agency which is doing something. Say, in the run up to Christmas, there's more investigations. Anyway...

I think the scale of the change in requests has gone from the order of ten to 20 a month to around a third of 800, which is 250 a month. That's the scale of the change.

BRUCE TONKIN: I'm assuming, Nick, has there been broad publicity about not just your own services but GDPR generally in the U.K.? Like, is there an awareness for individuals about this?

NICK WENBAN-SMITH: Actually, that's a really interesting question because the most significant thing about GDPR is that it hasn't really, I don't think, substantively changed the law in the U.K. But what it has been -- in terms of the understanding of each individual person and the rights they now have as citizens has been sky high. In terms of the BBC website, I looked in the run-up to GDPR and they had, like, front-page news stories. It was -- on the 25th of May, it was top of the headlines of everything and everybody is aware of it now.

BRUCE TONKIN: It's that rise in consumer awareness.

Yeah, Greg.

GREG AARON: Yeah. So since GDPR came into effect in May, we're slowly starting to understand what the effects are. And we're starting to see some information come out about usage and requests and so forth.

One of the recent things that happened was that two organizations that are composed of cybersecurity professionals and network operators was done. It was a poll by the anti-phishing group in M3AAWG and their memberships include -- security companies are responsible for protecting networks, banks, educational institutions, and so forth.

And they asked the members: Are you making more requests or fewer? How's that going? And about 300 and something respondents gave some information.

One of the things it says is that some of them no longer know how to make requests. It's partly because every organization that holds the data does things differently now. They have put their own procedures into place using different mechanisms. That's actually dissuaded them, they say, from making requests.

So if the number of requests is small, it may or may not tell us about the demand for the data because some have given up on using WHOIS data through the currently available mechanism because it no longer tells them what they need to know. So I think in the coming months, we'll learn a lot more about how the effects have come down on people.

BRUCE TONKIN: Thank you.

Number 3.

DIRK KRISCHENOWSKI: Hello, Dirk Krischenowski from .BERLIN and .HAMBURG and vice chair of the geo top-level domain group.

We have done recently -- and published this on CircleID and our website, geotlds.group -- a study of 39 geo TLDs. So coming back to the question about how to perform small registries in terms of GDPR. And out of the 39 were 25 European geo TLDs and 14 non-European geo TLDs. And the results of our findings were that while E.U.-based geo TLDs registries take GDPR seriously and have enacted measures to protect citizens' personal data, the number of requests to access the

data is vanishing small. And these requests are being dealt with efficiently.

The study of the geo TLD registries show that there's no evidence-based need for a universal access model based on how GDPR is working in practice. Please look at this study. It's quite interesting. And it says how many requests there were, such the requests from May until September have been under 15 in the 39 geo TLDs which have over 700,000 domain names registered to give a relation on that.

BRUCE TONKIN: Thank you, Dirk. I think it's great that people are sharing data. I think it's something that everybody can do that's running operational registries, is sharing the data, as Nick has done and as Dirk has done. That really helps policy development. Good.

One.

JOHN LAPRISE: Hi, John Laprise, ALAC. And I am going to take off my ALAC hat and put on my day-job hat. I work in a market research in a marketing department in the U.S. And I'll answer Bruce's question earlier about U.S. effects.

I was on a recent Webinar for work where while many companies in the U.S. are aware of GDPR, less than half are moving towards adoption. They're taking a "wait and see" attitude. And in many cases, it's the case of -- in the U.S. we have the expression, "You don't have to outrun

the bear, you just have to outrun the other guy." So that's the position many U.S. companies are taking as a wait and see and hope that the E.U. does not come looking at them.

But market research in general in the whole industry is quite up in arms for this. And we have other -- there's a new California data privacy initiative that's also going forward along the lines of GDPR. And so there's a lot of work in progress there.

BRUCE TONKIN: Okay. Thanks for that input.

Two.

THOMAS DE HAAN: Yes, thank you. Thomas De Haan, Dutch, GAC rep.

Just I would like to come back to Nominet's intervention, I think, which is very useful to look at the current mechanisms in place. Of course, it's within the jurisdiction of the U.K. so a little bit less complex than worldwide scale.

But so my question is: You refer to requests -- individual requests for data access. What about bulk access or limited bulk access? For example, in Netherlands, also one of the biggest ccTLDs in the world, they have come to an agreement with local authorities to have a limited bulk access. I don't know the details. They can tell more about it.

But is this mechanism also in the U.K.? And, basically, the question comes down: Does your instruments or the ones in place, do they really meet demand there is? Thank you.

BRUCE TONKIN: If I can just intervene in the question slightly, just in terminology, there's bulk as in does the entire database get provided to another party? And then there is being able to do automated queries. And I think they're a little different. But I will let Nick answer perhaps both of those questions. So do you provide bulk access, in other words, give an entire copy of your database to law enforcement? And do you have automated access, and what sort of query rates do you get on that?

NICK WENBAN-SMITH: Thank you for the question.

So in answer to the bulk access point, we do allow U.K.-based law enforcement agencies bulk access. But we need to be clear what access we're talking to because it's not the entire dataset.

The registry has a lot more data than we share with law enforcement. And then there's a lot less data which appears on the public WHOIS. So there's different sort of layers like an onion. But certainly the arrangement we came to on a domestic basis with our law enforcement was that they would get access to exactly the same WHOIS data that was available publicly prior to the 25th of May. But they do this through a secure log-in individualized with checks, and we don't just sort of give it out to anybody. These are agencies we know the way things

organized are. We have a National Crime Agency. They coordinate these sorts of things.

But in terms of local trading standards, there's also the local trading standards throughout the whole of the country. That's done through one point of access, through our local home authority.

BRUCE TONKIN: And then automated access?

NICK WENBAN-SMITH: We don't have automated access, right.

BRUCE TONKIN: Milton?

MILTON MUELLER: I think this is a good discussion about access, but I just want to point out that we're talking about access, right?

And let's be aware of, number one, we have a lot of interesting data that's being collected about the actual effects. I think the geo TLD information is very interesting. There's been a survey of ccTLDs. It's good to hear from Greg about the security researchers.

And I think you're getting an appreciation for how complex -- when we were hearing from Nominet about the different levels and types of access how complex this issue can get.

So, you know, there is a case to be made. Dirk has made a case we don't need unified access. There's a reasonable case to be made that we do. This is an issue that we have to grapple with.

But, first, we've got to decide what is in our WHOIS, what is published, what data elements we're collecting. And please don't confuse those issues.

And we should be able to get the first part done. I think it's relatively easy within three months. If we don't get it done within three months, we have a big problem. We don't -- the policy time line runs out and the whole multistakeholder process looks like a failure. And there are, as I said earlier, vultures circling that would like to see us fail, that would like to step in and make governmental interventions and maybe start fragmenting the process.

So let's fix the temp spec, formalize it as a policy, and then have a very interesting and rich debate about access.

BRUCE TONKIN: Yeah, one of the things from a software development principle is to do software development drops. So you get a piece done and you drop and you release that and then you get on to the next piece.

So to some degree in terms of being timely is try and get that sort of purpose, what data are you actually collecting and actually get that dropped because that then sets that. And then you can actually start looking at some of the other things. Otherwise, you sort of go around and around in circles. So I think it's a valid point.

Number 3.

BECKY BURR: Hi. I'm Becky Burr, and I'm speaking in my Neustar chief privacy officer.

I just wanted to follow up on John's comment about half of American companies. I think many people saw that Microsoft, when it rolled out its GDPR platform for data subject requests, rolled it out globally. They have now reported that on a per capita and absolute basis they're getting more requests and fulfilling more requests from Americans than from any other place in the world. That's certainly consistent with our experience.

The fact that everybody in Europe was aware of GDPR on May 25th also was felt around the world. So my experience is, at least this American company and other companies that I deal with, are actually raising the game, complying with GDPR, and moving very quickly as a consumer response.

BRUCE TONKIN: Thanks, Becky.

Number 1.

AMRITA CHOUDHURY: My name is Amrita Choudhury from CCOUI, India.

I might be certain wrong in certain facts, but correct me if I'm wrong. I believe there are 339 approximately million domain names registered.

And what I could hear is there are about 1200 million names which are under the E.U. domain. That is less than half of the global domain register, which is under E.U. jurisdiction.

While there's a lot of discussion happening at ICANN as to how the domain names can be GDPR compliant in terms of the WHOIS registry, is ICANN also looking at the -- you know, the laws of the other nations? Europe is an area. However, there are other regions, also nations. Are their interests being protected?

Second issue is: We have nations who are fairly developed who have a certain amount of understanding.

We also have nations which are emerging, for example, India, we have domain names which are being sold by various companies, organizations from Europe as well as U.S. and even India. The registrars and registries might not have the same amount of understanding, capability.

So what -- is there something being planned in terms of developing their understanding so that the end consumers also can be -- their interests can be taken care of? Because we are sitting here, we are talking but, however, the new Internet users or domain buyers are not all that tech savvy, especially from the emerging countries.

BRUCE TONKIN: I think there's two questions in there. One question is: How's laws in other countries being taken into account? So there's obviously laws in India.

And the second question is how is the awareness being raised amongst people in other parts of the world to these issues.

Maybe -- I will do the second one first. I will go to Hadia from because Hadia is from ALAC, so I'm assuming ALAC is doing things to raise awareness in different parts of the world.

HADIA ELMINIAWI: Yes. I speak as a member of the EPDP. So one of the recommendations hopefully that's going to come out of the EPDP team is making a recommendation to raise the awareness and educate the registrants.

And I think this would partly be tackled maybe by ICANN and also by the registries and the registrars because I do think also that it is in the best interest of the registrars that the registrants are aware of what's been -- what's happened in the new policies.

We are considering actually in our work the other privacy laws, actually now because the EPDP team is entitled to look into the temp spec compliance with the GDPR. But that doesn't mean -- hopefully, of course, there will be no conflicts with other privacy laws.

But currently we are not doing such work like looking at other privacy laws.

BRUCE TONKIN: Thanks. Ashley.

ASHLEY HEINEMAN: Thank you. Speaking on behalf of the GAC, so, yes, in terms of our engagement in the EPDP and other activities going on with respect to WHOIS, we've been trying our best to make it as -- "generic" is probably not the best word, but to make sure whatever we do recognizes that there are other data protection laws out there.

We're hopeful that we can do this kind of using GDPR as a construct because that's what's kind of forced our hand. But wherever possible, we are trying to make this not specific to GDPR. I think that's important, if nothing else, out of respect of other laws throughout the world. So that's what we're trying to achieve at least. Thanks.

BRUCE TONKIN: Thanks. Cristina.

CRISTINA MONTI: Also I wanted to offer some comments on these questions that are recurring about the tension or possible tension between different laws in different jurisdictions and the global nature of the Internet. So we know that this is a challenge, and we know that this is a challenge that we will keep being confronted with not only on data protection but also in other areas. And that's why it's so important that we get it right here at ICANN because this is going to be a test case also for the future.

As far as data protection is concerned, in general, I would also like to stress that what we see -- and maybe here I'm more optimistic than my colleague Milton Mueller. We see a trend towards convergence. Those principles that are enshrined in the GDPR and which are based on the

protection of fundamental human rights are, I would say, common sense principles. And it's about managing well your data.

Then as I was saying at the beginning, the devil is in the detail and in the implementation. And it's there where we have to focus our attention.

And it might well be that not all answers are there. And we might well discover that we need to come up also with creative solutions to make the system work and to stretch the limit of what we are dealing with. But that's why we have the processes in place, we have the stakeholders around the table, and we should be able to make it work.

Maybe also on -- my view on the different processes, I understand that there is, you know, some -- stakeholders would like to have the sequential sort of approach and others, you know, have the sense of urgency to get to a final solution.

I personally don't see, you know, problems in having parallel process; but it's clear that you have to have a clear understanding of the issues. And sometimes there are misconceptions that keep recurring.

And, therefore, it's really important to pay attention to what the others are saying so that, you know, in these different working groups, we all together collectively work toward a solution.

If there are issues that not cannot be solved, let's together identify how are we still going to bridge that gap.

BRUCE TONKIN: Great. Thanks, Cristina.

I want to just jump into another question, and then I will come back to the audience. Just another question for the panel.

One of the things from a policy development point of view is there have been some other policies in recent years developed that relate to this topic.

One of those is the solution that registries and registrars had implemented to protect the privacy of personal data was the introduction of what they called -- sometimes called privacy services or sometimes called proxy services.

But this is where they substituted information into the WHOIS which was either of a separate company, which was referred to as a proxy, or it could be the name and address of the registrar, for example, instead of the name and address of the registrant. And then they basically operated a forwarding service. So if mail was sent to the address that was in the WHOIS, it might get forwarded to the end user.

So one of the concerns around the growth of these privacy/proxy services was they're doing a great job of giving consumers the option to protect their personal data. But what wasn't clear is under what circumstances does the personal data then get released to law enforcement and have this law enforcement and other groups gain access to that data.

So there was a policy development process that ran on that topic. But now that we're dealing with this really fresh, then the question for the

panel is, how do we -- do we need to go back and revisit those policies? Do we need to take those policies into account when we're developing the policy around -- in the EPDP.

The other topic that happened a few years ago was the concept of a thick WHOIS. So some of the registries, most notably .COM, the central registry basically has information on the domain name, like the DNS information, and then it has information on the registrar, and then you have to go ask the registrar for information about the actual registered name holder. So it's a distributed system. And so the view at the time a few years ago is, it's hard to have to query all of these separate systems, because the data formats were all a bit different. And the only tool at that time was port 43 WHOIS. So the policy development process said, we should have all the information in a central registry so that it can be queried in one place. But what's emerging with the regulations around a lot of countries is restrictions on transferring data across borders. The general view these days seems to be that, you know, if you're operating a registrar in Australia and you've got Australian customers, that you keep your data in Australia. Likewise, if you're operating a registry in Germany or Ireland or some other country, you keep the data about your customers in the country where the registrar's located and then only release that data through appropriate, you know, standards and conventions.

So really the question for the panel is, given that we have these two policies that exist, they could be in conflict with the work that the EPDP is doing. And I mentioned in the panels views on how do we take into

account the work that's been done so far and do we need to sort of go back and update it or look at other approaches? Ashley?

ASHLEY HEINEMAN: I'll speak very briefly because I'm not probably as best place at least for my law enforcement colleagues and others. But I just wanted to note, being on the privacy/proxy implementation review team, it's had quite a bit of impact in that things have pretty much stopped at this point. Which is of concern to particularly those who want to gain access to this information. It's also of concern because as we're entering this GDPR enforced world, privacy/proxy is an option available to masked data and there needs to be rules around that as well. So if nothing else, the impact being in that it's stopping implementation work. Thanks.

BRUCE TONKIN: Thanks, Ashley. Others want to talk on this topic? Milton.

MILTON MUELLER: Not so much on privacy/proxies but on thick WHOIS. My understanding is that thick WHOIS would no longer be necessary under -- once we come into compliance with GDPR and have implemented RDAP, that the need for RDAP would pretty much be superseded by the existence of -- excuse me, the need for thick WHOIS would be superseded by the existence of RDAP, and you wouldn't have any real rationale for having the data held by the registry.

BRUCE TONKIN: So just to elaborate on that, why is that the case may be? People are not necessarily familiar with RDAP, so why would RDAP solve that?

MILTON MUELLER: It would provide a kind of a federated database by which people who wanted access could get it without having to move it to -- and store it in two different places, the registry and the registrar. This is my understanding. I could be wrong about that, but -- and I thought the rationale for thick WHOIS was kind of weak in the first place. It did facilitate the transfer of domains from different registrars to another, but it seems like we should be able to do that without having thick WHOIS. And then in line with GDPR, the principle of sort of minimizing the transfer and collection of data would seem to dictate that you want the data to be sitting with the registrar that actually collects it.

BRUCE TONKIN: Okay. Greg.

GREG AARON: One of the things that we've seen in our experience over the last few months with the temporary specification is that while GDPR covers certain kinds of data, the temporary specifications is allowing the redaction of additional data that's not covered under the law. For example, GDPR does not cover the information of what are called legal persons, incorporated entities. But that data can be redacted under the temporary specification and that gives people less information to work with.

So one of the things that the SSAC has said is, make information available under the law, that's very important, but do not overapply the law. Give access in a balanced way to the extent allowed by the law. And that's two different things.

So with proxy data, there are people who are not subject to GDPR who could still avail themselves.

BRUCE TONKIN: So they're not natural persons, essentially.

GREG AARON: Like if I'm an individual in, say, Brazil, I'm not under GDPR if my registrar is not there, but maybe I still want to use proxy protection. There's an overlap then in these two cases.

I'll also state that the SSAC has stated that thick registries are a good idea for some articulated reasons for security and stability, and they don't have anything to do with the -- some of those don't have anything to do with the provision of the information, so I disagree with Milton.

BRUCE TONKIN: Nick.

NICK WENBAN-SMITH: I don't mind taking privacy/proxy services. So I think the implication of the question is that -- and this is a big assumption -- that what is in the temporary specification which allows for the redaction of personal data

stays as a permanent policy in due course. But if that's the case, then I think the question is, if people's personal data is not going to be exposed in a public WHOIS, what's the point of privacy, right? And in systems -- and there are many systems in Europe where privacy has been built into the registry operations and some people can't benefit from personal data protection as has already been pointed out, there's nonetheless always been a demand for privacy and proxy services. Sometimes it's just for administrative convenience. Sometimes for commercial confidentiality. Somebody wants to launch a new brand, they don't want them to know it's them. They register new names through proxy services. So there is -- I think it's early days, we don't know yet, but I'm pretty sure there will be still be some sort of demand. But I'm pretty sure also it will be at lower level than previously.

BRUCE TONKIN: Hadia.

HADIA ELMINIAWI: Yeah. So I agree with all what was said. I would just add that under the existing or prior to the GDPR proxy services providers, legitimate proxy service providers were also entitled to or permitted to give out the data under certain circumstances. So -- so I'm not sure if actually we do need proxy services right now. Thank you.

BRUCE TONKIN: Chris.

CHRIS LEWIS-EVANS: Thank you. Yeah, this thing about privacy/proxy services, that highlights one of the questions from earlier actually is, within that services there was no uniform way of requesting data from those services. This probably led to a lower level of requests to those people providing those services. So I think it was .BERLIN asked the question about, you know, we're not seeing many requests. And I think so there was an RDS2 review and the phishing -- anti-working phishing group and M3AAWG review. They've all indicated that there is a very lack of knowledge about how to gain access. And I think that is hiding a lot of the problems that we're seeing. So really at the moment, I know we're, as Nick said earlier, quite a way down the line already since GDPR started, but I really don't think we've seen the full impact of the temporary spec on the requests and request levels. So I think any numbers are helpful, but I don't think it's necessarily relevant.

And I think as Milton has said it, it's creation of that policy first that allows us to get a uniform access model in place and it's getting that policy right to then give us, you know, a really good model and a lawful model to gain access to data.

BRUCE TONKIN: Okay. Cyrus from ICANN just sort of comment I guess on the implementation of the privacy/proxy policy.

CYRUS NAMAZI: Thank you, Bruce. My name is Cyrus Namazi. I'm part of the global domains division of ICANN. I just wanted to make a clarification on the policy implementation work that we undertake in GDD and clarify that we haven't stopped anything. In particular, I think Ashley mentioned that privacy/proxy work. The clarification is that I think we've come to the realization that at this instant in time, there is not sufficient clarity to put in the appropriate legal framework, frankly, to essentially advance the accreditation model in a manner that we think is justified in terms of the -- it's the efficiency of work and it's applicability. There is lack of clarity because of GDPR on how to deal with some of the components of what an accreditation model -- which is not too dissimilar, frankly, to the registrar accreditation model -- would look like. And considering the fluidity of the situation and the fact that the dust hasn't quite settled on how to interpret some of the implications of GDPR, we're essentially pacing the implementation work with the speed at which the facts are coming in that can be counted on so that we're not wasting time going forward with something that has a good likelihood of changing in not too distant in the future. And this is not really, I think, limited to privacy/proxy. We're facing a similar situation in implementation of thick WHOIS, which is actually at its implementation phase. The policy has been defined, in fact ratified by the board, quite some time ago. And in that particular case the sort of piece that's holding us back is the registry and the registrars coming to an agreement in terms of how they should handle the agreement between themselves, between the registry and the registrars. The Registry/Registrar Agreement, the RRA.

There are other programs. We have 13 of them actually in the organization that are related to registration data services, all of which are in some shape or form going to be impacted as we get better understanding of GDPR, its impact and, you know, how the policy work and the services that are related to RDS may have to be changed in the future.

BRUCE TONKIN: Yes, I think, Cyrus, you're kind of highlighting really a point that I was making earlier about what I call a timely solution because what we're seeing is -- and using thick WHOIS as an example -- that policy development was done actually years ago. It was probably five years ago. It might have been longer. Probably -- might have been even when I was on the GNSO Council, I can't even remember. But -- so it's been there a long time. But I think the thing is that the world's moving on. You know, the regulation in this field has changed quite dramatically in recent years, and then it's causing a rethink. But I think as an community and as an organization, we have got to be a bit more agile in being able to respond to developments as they occur. And so I gather that the challenge, particularly on thick WHOIS now, is, you know, how does it -- is it still the right thing to do, given the changes in privacy law, particularly GDPR? And, you know, it feels like the effort's got to go in getting this PDP right and getting the requirements right, understanding why we're collecting data, get some of those requirements right. Because a lot of these things have been sort of done kind of piecemeal, and now we're really coming back to the fundamentals, which is revisiting why are we collecting the data. And

certainly when I was first involved in ICANN around about 2000 the focus of WHOIS was to allow competition, actually. It was a way to make smooth transfers between the one registrar that had most of the domain names at the time, being able to make that information available to other registrars to help transfers. I mean, if you're going to describe a purpose, that was the purpose back in 2000. And, you know, I don't think we've really sat back as a community now and got everyone's input on what that purpose should be.

So that has to be the fundamental thing, is getting the purpose right. And then privacy/proxy is essentially an access discussion. And the thick WHOIS is really a data storage discussion. Because the technologies around now, I mean, you don't have to store everything centrally. You can achieve the same thing, as Milton said, by having -- you can have a WHOIS page or a request page on the ICANN site. It can send the request to the relevant registrar. The registrar can apply their local law in responding to that request, basically.

CYRUS NAMAZI: Thank you, Bruce. I think you highlighted another component of sort of this changing environment. Because as you likely know, we're sort of in the throes of implementing RDAP, which is a completely different platform that the sort of old and outdated WHOIS protocol. And that, in fact, lends itself to sort of compelling us to ask the questions that you were highlighting. You know, where do you store the data, how do you get access to it? And I think with RDAP we can actually sort of coming into what I consider to be a 21st century platform that's scalable, that

can actually change with the sort of the -- the dynamic fluid landscape of privacy laws around the globe and help us develop the type of system and registration data services that can actually move in a timely manner with the changing of times.

BRUCE TONKIN: Thank you. Okay, we'll go back out number 1.

VOLKER GREIMANN: Thank you. Volker Greimann for Key-Systems and Central NIC. I would like to come back to one of the -- what I consider red herrings that has been raised earlier on the panel which is the distinction between legal entities and personal registrants. I think that distinction is not wrong. The temporary specification is not overprotecting or overreaching in a way because of a fundamental misunderstanding of what the GDPR actually protects. It does not protect personal data per se. It also protects the personal data that may be included in the data that's provided by a legal -- a legal entity. So if we have a registration from a company and that company chooses to provide the personal data of one of their employees in the email address, in the telephone number, in the registrant data, that is personal data. We cannot make that distinction as a registrar. We do not know if a registration by a legal entity contains private data. But that private data must be protected the same way as a personal registration data would be.

So having that distinction of whether a registration is made by a private entity or a legal entity is absolutely useless for the determination of

whether that data is to be protected under the temporary specification or not. Thank you.

BRUCE TONKIN: Thanks, Volker. And number 2.

DEAN MARKS: Hi. Dean Marks for the coalition for online accountability. I wanted to refer back to something that Ms. Monti from the commission said, that the GDPR builds on rules that have been there a long time. At least with respect to the privacy/proxy policy development process, that wasn't something that was back for many years ago. That's something that came to a conclusion in 2016 when the GDPR was already on the books. There was a great awareness of the privacy law concerns that were at play when that PDP work was going forward. And so I don't understand why it's been put on a pause to seek clarity when everybody in this room agrees that the GDPR does not answer all the questions. The GDPR in and of itself doesn't bring clarity to all the details. And again, as Ms. Monti said, this multistakeholder process is a good place to strike the balance. We had a balance struck in the privacy/proxy services PDP. It was unanimously approved by the GNSO Council. It was unanimously approved by the ICANN board of directors. It's a great step forward in striking that balance. And when will that clarity ever be brought to fore, Cyrus? I believe that by going forward with the privacy/proxy service, the multistakeholder community would be actually helping to establish the clarity. And so I believe ICANN org is doing a great disservice to the entire multistakeholder community.

BRUCE TONKIN: Cyrus, perhaps you could get a bit more specific in some examples of what's essentially your impediments to implementing it. Just be a bit more specific which might help the --

CYRUS NAMAZI: Yeah. Thank you very much. I actually left the hot seat so that I wouldn't have to continue taking over the panel discussion, which was not the intent. And Dean, I completely appreciate what you're saying. And again, I want to clarify, we haven't stopped the policy implementation work which we've been working with you and others in the IRT for some time. And it's not even a question from my perspective, from our perspective on the org side, of the relevance of the policy. That's not a question that I need to get into. It's for the community to decide on it. It really has to do with coming up with the appropriate legal framework to implement it. And we have run into this actually with my data -- the data escrow agents and the agreements that we have with them. And at the moment, it's more or less the type of thing that we do not feel that we have enough confidence with that framework, the legal framework, that would be necessary to implement it.

It has nothing really to do with the relevance of it. I think there actually a need for a privacy/proxy service post the GDPR world, so to speak. But, again, it's not for the org to decide on.

BRUCE TONKIN: Okay. Number 3.

SEBASTIEN BACHOLLET: Sebastien Bachollet will be speaking in French. You're going to say, "as usual."

The question about the difference between a physical -- an individual physical person and legal person.

That surprises me. Of course, there is a different. As a person, a physical person, I have a name, an email address. And, if I need to give my information, I can give them. But an organization, a business can publish that information. It's his choice. We need to protect a physical person. And the legal person can organize themself so they will not be -- sensitive information that will be published. All of us can -- we could at least have information ourselves. So it's normal for a physical person to obtain the information.

UNKNOWN SPEAKER: I agree with Sebastien. We can read the text of the regulation. You will understand that very well. The text does not have to be interpreted.

BRUCE TONKIN: Yep?

PETER KIMPIAN: Good morning, everybody. I'm Peter Kimpian from the Council of Europe. And I will be very brief today.

It is only to say that the Council of Europe Committee on data protection just adopted a guide on ICANN and privacy, which was published this week. And I know that we are concentrating on GDPR. And we are waiting for an opinion from EPDP. But the committee Council of Europe has and data protection has all the members of European Union plus member states, parties like Russian Federation, Turkey, Mexico, and African countries as well

So there are some indications and guidance and common understanding and international privacy standards on this, especially when it comes to the last topic, data subjects and the other definitions as well and principles. Thank you very much.

BRUCE TONKIN: Okay. Anyone want to comment on that? No? Okay.

All right. Is there another question down the back there? No?

The other question I had I think we've probably already covered a bit is how can we ensure the conformance of the solution with other privacy laws? I think we had that question in a few different ways. So we probably covered that one.

Other than that, maybe going back, having heard a bit of the discussion and comments from the audience, I know, Milton, you're saying there were some examples of how we can easily get distracted into other areas.

Does the panel want to make any further comments on what you think we can do to, you know, get to a timely solution, I guess? What can the community help the policy development process with? What can we do to make it effective?

Flip?

FLIP PETILLION: Raise awareness. I think this discussion has clearly shown that people with data and sharing the data are clearing helping moving forward this discussion.

And it helps people get aware.

We had a meeting where Goran was visiting us yesterday. And he said something very interesting. He said, "I wished we had actually addressed this long before," which is very true. But this is the fact. I mean, we have to live with it.

But that had me -- made me think of the future. And I'm happy to launch an idea. I just want to think in the direction of how he was thinking.

And I was wondering what we are missing now that will come to us in the very near future and is related to access.

Suppose we have access and we solve the issues about access. What does that mean for ICANN as an organization? Does that mean it will take on more responsibility in the future?

You know, we have for 20 years a very successful UDRP system. And that is helping out the IP rights holders. , more particularly, the trademark holders. That is one solution for one particular concern.

I'm wondering if there are other concerns that we should address and for which we would need similar approaches in the future?

For example, what is really concerning is harm to consumers, harm to people, harm to children.

It's only an example, but it's a very important one.

Frankly, I would prefer today to receive a bit more spam but knowing that we might fight the infringements and the harm more, pending the EPDP.

BRUCE TONKIN: Okay. Any other communities?

Ashley and then Cristina.

ASHLEY HEINEMAN: Thanks. Representing the GAC. I think this conversation about not getting distracted, I think -- yes, there are certainly areas where we can avoid being distracted that will help us be more timely in what we do.

But, that being said -- and in particular this panel not being limited to the EPDP, I think from the GAC perspective, we are very supportive of the universal access model conversation that's been initiated by ICANN.

And we're very thankful that it was done, in large part because it allows us to start the process of thinking about it. It gives us the framework to do that. And it also gives us the opportunity to start identifying and getting answers to important questions.

Now this isn't to say that we're starting the technical development or anything of that sort. That will come in due course.

But getting questions like the ones that Goran posed to the European Data Protection Board I think will only help us more formalize our thoughts and our views moving forward. So, just again, I think it's not wise to characterize the universal access model conversations as a distraction. It's, I think, an efficient way to begin a conversation of another hurdle that we have to deal with. Thanks.

BRUCE TONKIN: Cristina and then Greg.

CRISTINA MONTI: Very briefly, I just wanted to highlight from my perspective the most important thing moving ahead is to have clarity, clear agreement, and transparency about the different processing activities involving the WHOIS system and their respective purposes. This is really the basis.

Once we have this agreement on the different processing activities, then it will be very much more easier to address other aspects. And I would suggest also to keep these different processing activities

separate. Because different legal base might apply. So I think having this sort of clarity will really help us advance in the right direction.

So this is my suggestion.

BRUCE TONKIN: Thank you. Greg.

GREG AARON: It is important to think about the future regarding to the current situation because we weren't thinking far enough ahead. So looking forward is important.

The EPDP group is working very hard on extremely difficult and complex questions. And it's probably a good time for the GNSO and the organization as a whole to think about what happens in 2019.

That group will get as far as it can. But the temporary specification will come to an end at some point, and that group is working very hard. And we'll see how much of its work it gets through, but it may not get through its entire project plan.

So, rather than being caught flat footed, let's make sure that the work continues and that the people doing the work have the resources that they need to finish it.

BRUCE TONKIN: Hadia.

HADIA ELMINIAWI: As an ALAC member, our main concern and our main interest is in making the Internet or keeping the Internet a safe place for everyone. So, basically, detecting and preventing fraud or DNS abuse -- and DNS abuse is something that we regard of great importance.

And, having said that, I will again say that it is very important to look now on -- to look now at industry standardized processes and the accreditation services.

Because, if we're done with a policy and those things are not in place yet, how much time do we need to wait until we have something really implementable and practical in place? So thank you.

BRUCE TONKIN: Okay. I think we've got a question in the audience. Number 1.

RUDY DANIEL: Rudy Daniel. I'm an ICANN 63 Fellow from the Caribbean. A general question is: GDPR: Has it, in fact, mandated ICANN and the community to get its house in order with respects to the WHOIS thus defining data elements and the subsequent access and the methodology of access with respect to applicable law and moving into the future, especially as the v6 is being adopted more and more?

BRUCE TONKIN: Anyone want to comment or respond to that?

Milton.

And thank you as a fellow for standing up and asking a question. That's appreciated.

MILTON MUELLER: So yes. Definitely the GDPR forced ICANN to get its house in order. I think Greg said something about we didn't look forward and anticipate what was going to happen. Some of us have been telling ICANN for 15 years that the WHOIS was illegal under data protection law. And they just -- it wasn't that they didn't know this. It was that they could get away with not paying attention to that warning.

So it's more political than it is a failure of foresight. And the penalties of the GDPR effectively forced us to rearrange this whole thing.

Now just to sum up in terms of the way forward, I totally agree with Ms. Monti that the job number one is to identify the purposes and the data collection necessary to get those purposes. Then we define what element of that data is going to be displayed publicly in the WHOIS and which are not, which are going to be redacted. Then we can work on access.

It's not so much that the Gorans and the CEO's attempt to explore legal access regarding the unified access model is a distraction as much as it is premature. And we may indeed -- we don't really know what the model will do until we have that first job done.

So I think the main reason I've questioned the discussion about a unified access model is because I think it raises the hopes in the minds of many people that somehow this access model is going to recreate the old WHOIS once they get themselves accredited. And I think that that is a distraction in the sense that it detracts people's attention from focusing on what we're actually going to do with the WHOIS that we have now and rather than, you know, thinking about, oh, how I'm going get access and not worry about what we're doing with WHOIS now.

RUDY DANIEL: I'm just wondering if the universal access model is a quick fix.

MILTON MUELLER: It can't be a quick fix. It's extremely complicated. It's complicated legally. It's complicated technically. It's complicated policy-wise.

So, no, I think that's the main justification for initiating the discussion now, is that it's not going to be a quick fix. It's going to be complicated.

And to give him the greatest credit, Goran is trying to get some of these discussions under way. But at the same time, he's kind of pushing the direction of the conversation in a way that may not be the right direction. So we simply have to defer the access issue until we're finished with the first part, which, again, should be quick. It shouldn't be difficult for us to solve the first problem.

HADIA ELMINIAWI: In short, we don't know if it is a quick fix or not because we are simply not discussing access now and will not be discussing access until we are done with the gating questions. Thank you.

BRUCE TONKIN: All right. I think I might wrap it up there. I'd like to thank the panel. And I think at the very early part of the meeting was a constructive conversation because it's essentially their understanding each other, asking more questions as we start with the early discussion. As Ashley kicked off in terms of getting to a speedy outcome I think is that we quickly understand what the issues are, and then we can solve those issues. That's a positive step forward.

I think we've heard that we're not going back to the old WHOIS. Very little support for that concept. And I think the concept that we need to balance protection of data subjects as well as providing access to legitimate users, I think, seem to be very strong support around the achieving balance as well, I think, both in the audience and in the panel.

So thank you all for attending and we look forward to a successful outcome of the PDP.

[Applause]

[END OF TRANSCRIPTION]