SAN JUAN – Cross-Community Session: GDPR & WHOIS Compliance Models
Monday, March 12, 2018 – 10:30 to 12:00 AST
ICANN61 | San Juan, Puerto Rico

STEVE DELBIANCO: All right. We're live and good morning, everyone. This is the cross-community session on GDPR. For those that didn't know, GDPR means, I'm glad we did Puerto Rico. No, of course, you know it isn't that at all. The General Data Protection Regulation was adopted by the European Union, European Commission, takes effect in May of 2018 and applies to companies that process personal data of subjects of the European Union, regardless of that company's location. ICANN and WHOIS were not the intended target of GDPR, which I think was aimed at privacy related to financial and medical, among other items. But just like Hurricane Maria was aimed at the U.S. mainland and Puerto Rico got in the way, I think GDPR is making a hurricane pass over top of WHOIS and ICANN.

Now, the purpose of today's session is to have our top executives of ICANN present the proposed interim model that ICANN's come up with and shared with DPAs and then to have seven members of our community give the reaction to both the model and the process of moving the model from now to its final model. I'll quickly -- and then we're going to do a quick reminder on what the community processes are, and then finally

community Q&A. Now, we're starting 20 minutes late, so the hope is that if nothing in this room at 12 noon, we'll be able to make up the Q&A time from the audience at that point.

Let me provide some quick introductions from your left to your right.

We first have Goran Marby, CEO of ICANN.

John Jeffrey, general counsel of ICANN.

Nick Wenban-Smith from Nominet. Thomas Rickert, with eco, the association of the Internet industry and author of the GDPR playbook.

Cathrin Bauer-Bulst from the European Commission.

Patrick Charnley for Coalition of Online Accountability.

Tim Chen with Domain Tools. Next to him Stephanie Perrin with the non-commercial stakeholders group.

And at the bottom of the table is Alan Greenberg of the ALAC, chairman of the ALAC.

And I'm your moderator.

With that I'm going turn it over to Goran to discuss the process for the interim model.

GORAN MARBY: Thank you. So great to see you again. It's only been, like, 30 minutes. So I'm going to be very short.

And the first thing I would like to say is again thank you for all of you who contribute in this work.

As I said earlier on, it was six months ago we really started the process of discussing how to be compliant with GDPR. One of the things we've done over that time is we have --

[Speaker off microphone]

I have actually nothing to say, so it doesn't really matter.

Thank you for your support.

Is it better now? Thank you.

This process started out with the recognition that ICANN as an entity, not only as an institution, has an obligation under this law as some sort of controller.

That means that I, as the CEO, at one point in time have to make a decision how I, ICANN org, has to be compliant to the law. I think something happened there.

When we decided to invent the process, because when the founding mothers of ICANN came up how to do those things, we didn't have a plan how to facilitate that discussion. You've been very adaptive to that. We had a lot of conversations, hopefully, a

lot of transparency. And now we're reaching a very important point. This week we sent over to the DPAs of Europe a proposal for what we think today ICANN org thinks is how ICANN org can be compliant to the law.

But here comes the catch: There are several unanswered questions. And I hope this session can help us with that.

Balances that have not been made from both sides, from everyone, that we don't have the answer to.

Now it's time for the member states of Europe together with the DPAs to up with firm advice before the law is enacted. I would like to say that we have a very good cooperation and dialogue with the Article 29 group. If we don't have that, the simple truth is that our possibility to enforce our contracts will diminish. Because the contracted parties has the right from their own perspective to look upon how the law should be interpreted and move along with that.

That will be a situation that will have a very, very fragmented WHOIS system out there. I don't think that anyone wants that.

So I hope that one of the questions we can have an answer to today is what the European member states are doing to help us together with the DPAs to get that question. We're all in this together. So I'm going leave the rest of the introduction and

then leave over to J.J. to talk through what we call the interim hybrid model. Thank you very much.

JOHN JEFFREY: We'll test this microphone now. Can everybody hear me? Good. Good.

So the first slide will have up -- let's make sure that works, too. Back one. Thank you. It's not behind me. It's in front of me. Very good.

UNKNOWN SPEAKER: Can the technical folks put microphones on the monitor, please. It's very difficult from here.

JOHN JEFFREY: Thank you. So the slide we see up right now has a variety of different models that have been submitted from the community. And we tried to grid those across some of the key factors. Whether or not those changes apply globally or whether they apply only to the European economic area, those models. And on a scale of full public access to only being accessing the data on the -- from due process, from a court position.

And so what you'll see is there's a wide variety of approaches to how we can treat WHOIS under the new GDPR rules that will go

into effect and some of the rules that have been in effect for sometime. But, in any event, there will be changes to WHOIS as we know it.

And the key fundamental change that's now been widely accepted by almost all of the community is that there will be a layered or tiered approach, meaning that there will be -- in the set of data that is collected in WHOIS, there will be a public version of that WHOIS, some aspects of what you can see publicly the same way that you can see all of it now. And there will be a non-public WHOIS that will only be accessible to those parties who will be permitted to access it. And we'll start to go into that as we go through the proposal that ICANN's made about an interim compliance model that will go into effect once it's approved by the community and the Board and will become then possibly part of the contract or will be subject to a waiver as we apply it to the registries and registrars.

This proposal that we're making is not the final proposal yet.

Even it's an interim of an interim, if you will. That is the model that we submitted to the DPAs on Friday along with a cookbook which details as to each individual element what -- why we've selected this particular aspect of each of the models. So we've broken the model into four main categories which many of you who have been following this are now very familiar with. What

data is collected, processed, and retained? How is that the model applicable? And what will be demonstrated or shown in the public WHOIS? And what would only be accessible or how you would access it from the non-public WHOIS. And so we'll go through these very quickly. And, of course, there's a lot in the description of the model that was posted online.

In terms of what will be collected, the ICANN interim model would be full, thick data. And that's after a detailed analysis of each of the fields that are currently collected in public WHOIS. We believe that there could be an opportunity for additional minimization, but that should come from the policy processes that come from the community going forward rather than having ICANN organization limit that now as part of this proposal.

We did find there was some fields that were used only by limited sectors of the community, but we could not find fields that weren't being used for what appeared to be legitimate purposes when we looked at the analysis behind what had been submitted in the comments and in the discussions.

Going on to what data would be transferred from the registrars to the registries, that's the full transfer of the data that's collected, also the data that would be transferred to the escrow agents. And, remember, when we say "escrow agents," we're

referring to those parties, third party escrow holders that are holding the data at ICANN's contract with them directly in a confidential way. And that data is only used in the instances where there is an audit of that data relating to registrars or registries or where there is a need for that based upon the failure or a breach resulting in a non-accreditation or an end of a contract with registrars and registries.

On data retention, this was one of the areas where there was a wide difference of opinion in some of the models. But there was some existing waivers that existed for European registrars with DPAs that would be preserved plus ICANN selected life of registration plus two years to be part of this model. Moving on then to applicability, which is at the bottom of the slide, must the model be applied globally or only to the European economic area?

We believe that there's no question that it should be applied to the European economic area. But we agree that it could be applied or may be applied by registrars or registries globally.

And there are a number of reasons for that that we could elaborate on if there are questions about it. But I think that there's a rationale going to that that relates directly to the need for registries and registrars to be able to differentiate between registrants that are in the European economic area as opposed

to those who are out and some difficulties in being able to establish who those are.

On the registrant types affected, there were also questions and variances in some of the models between whether it should apply just to natural persons or to legal persons. And ICANN's model takes the position that it would apply to both natural and legal persons.

Moving on then to what you would see in the public WHOIS under the new model. Under registrant name in public WHOIS, you would no longer see the registrant's name; but you would see the organization's name, if it's applicable. The registrant postal address would be limited in information only to state, province, and country in order to be able to establish jurisdiction and understand where the party is. But it would no longer include street, city, or postal code.

On registrant email and on admin and tech contact email, we took a middle of the road approach on this. There were some that said we should no longer publish it. There were others that said we should continue to publish all email. And we saw an interesting approach both in the eco model and in the coalition firm line accountability model that listed an opportunity for creating anonymized email or a web form to be able to contact the registrant or the admin and tech contact.

So that is now included in this proposed model. Registrant phone, fax, admin tech contact names, admin tech postal addresses, and admin phone numbers -- and contact phone numbers would no longer be included in the public WHOIS.

Then one more point. There was a question as to whether registrars should be required to provide an opt-in for registrants to publish additional data if they choose to do so inside the public WHOIS, and we're saying that they should do that. That there should be an opportunity for registrants that want to provide more information to be able to do so.

And last, how would -- how would parties who have a legitimate use of the data that is in the non-public WHOIS access it? There was a question about self-certification, whether individual parties should be able to certify that they are permitted to access it and have registrants who are someone at the very front of that process be able to determine that and allow quick access. And looking at that very closely, we think the need to contact the registrant was the key factor in having a quick self-certification process and that anonymized email or web form would, in fact, solve most of those issues. So we believe that a self-certification model may not be compliant with the law when we looked at that.

On the accreditation program, many of you have heard discussions about that already from a number of different calls that we've had and from discussions that have started already this week and will continue. There's a very important aspect to the accreditation model. It's how you show that parties that have a legitimate purpose in accessing the non-public WHOIS can gain access to it. So there's a proposal for an accreditation model. We've reached out to the GAC and we're seeking consultation with the GAC, in particular on two buckets of certification, the first being relating to law enforcement and other governmental authorities to have access. We believe that the GAC would be a good collection point for that data to determine legitimate law enforcement and agencies of governments that could access WHOIS.

On those that are non-governmental, so, for example, abuse, anti-abuse entities, researchers, intellectual property, people who are attempting to protect their trademarks, there would be an opportunity for creating a Code of Conduct, so setting rules about how you could be qualified to be certified and how then you could act inside of that information. What you could do with that information when you have it and how you could be accountable for accessing and using that information appropriately, consistent with legitimate uses.

And with that, we'll move to the next slide, and I'll pause to allow the rest of the people have some discussion.

STEVE DelBIANCO: Thank you, Goran and J.J. Very efficient and effective walk-through of the proposed interim model. And the slide that's up there now is a visual conception that I've prepared and that ICANN generally approved so that we can put it all on one slide for purposes of reacting. And I think you'll notice that the left side of the diagram indicates the flow of information today between registrants, registrars, registries, data escrow, and ICANN, and it's substantially unchanged in the proposed interim model. Where the changes occur are on the right-hand side of the diagram with respect to registrant data that is publicly displayed, that is to say displayed via Web site or port 43 and then the non-public, the new gated access in the way in which governments and non-governments are certified or given the criteria.

Cookbook 7.1, that is to say the very first principle in ICANN's cookbook is this: ICANN org's objective to identify the appropriate balance to ensure compliance with GDPR while maintaining the existing WHOIS system to the greatest extent possible. And that is a challenge, particularly given sort of vague guidance from the DPAs. So with that principle in mind, we've

invited seven community members to analyze whether that principle's been met, to look at gaps between the proposed model you've just heard about and their own needs and to think about the process as well. And to do this properly we're going to time each of our speakers to just six minutes. I'll run a timer here. And first up we have from the registries, that is to say Nominet, Nick Wenban-Smith. Nick?

NICK WENBAN-SMITH: Thank you, and good morning, everybody. I'd like to thank the business community and the Governmental Advisory Committee for inviting me to speak to -- this morning on this important cross-community session once again. As in the last cross community session, Abu Dhabi, I should make it clear I'm here as a representative of the registry stakeholder group but I'm not speaking on behalf of all registries. I'm here as a representative of Nominet. For those of you that don't know, in addition to being the ccTLD, the country code operator for the .UK, therefore part of the European Union at the moment and very familiar with the data protection regime that we have, we also do have some gTLDs. We provide other services to gTLDs, and so that's really where our interest lies here today. And thanks very much, J.J., for the overview of the interim model. I think I've got four words initially to say and those are, "thank you very much." I could take issue with the timing, it's a bit late in the

day, and obviously there's lots of important details that remain outstanding and to be worked out, but we believe that this proposed interim model as it stands now marks a positive step forwards. And in particular, it now starts to align the gTLD WHOIS model with globally accepted norms of privacy protection and prevents the blanket worldwide publication of registrant data, you know, without any sort of checks or filters and anybody in the world can check all that and a reform of that basic principle is long overdue. And it was the principle risk for the contracted registries when we look at the GDPR coming up.

So, I mean, we particularly like the opt-in nature of the model, the fact that registries can apply the same policies globally, regardless of the location of the registrant, and that it's not mandatory for us to distinguish between different types of registrant going forward. So those are important things for us. And these now look like a basis of a model which is implementable and compliant. So thank you.

In terms of the GAC analysis of what is yet to be worked out and what we need to see, from our registries the continued publication of the registrant organization field has a 60%, more than 60% overlap with the registrant name, and we know that less than 60% of our registrations are corporate registrations. So there is still a risk of leakage of personal data through the publication of the registrant org field. So that is a risk going

forwards which we would like to have a bit of consideration on before the final model is settled.

I have to say secondly, in relation to the email thing, I have to say that as the U.K. ccTLD registry for decades we have not published an email address in the WHOIS for U.K. domain names and this is not a problem. And we receive on the order of ten queries for data release under a release policy every month in relation to 12 million domains. So in essence, I don't think that this is something that is actually required to be put into the model going forwards. The interim model does propose a Web form or anonymized form of email address which is certainly better than publication of the registrant email address, but given the time left now to implement it, I think that that's possibly a bit of a distraction and personally I would drop that altogether.

It's not mentioned in the slide here, but the -- in the text of the interim model it speaks to inclusion of data processing agreements in place between ICANN and the contracted parties, including the registries. There are obviously many thousands of those worldwide, and it is an essential part of GDPR compliance. And given the time now left for implementation, the order of seven weeks, the number -- the notice periods that need to be given and the process of doing that, we need to see those proposed clauses for data processing to go in our agreements as

soon as possible, please. And when I say that, I mean not in the next fortnight but like yesterday.

Coming to my final point, and I know we're short of time and I wanted to make sort of specific points which are important to us and it's around the access system to the non-public WHOIS which is yet to be developed. We feel that there are some significant questions of principle around blanket access to classes of people and organizations to be decided. Regardless of whether you think in practice that that is a good idea as opposed to, for example, other alternatives like a responsible data release policy, which is what most of the European ccTLDs operate without any issues, we have yet to hear any sort of explanation as to how that sort of approach is compatible in legal terms with GDPR's purposed limitation points. And obviously the second point in terms of practicalities now, this is obviously not going to be in place for May. And I think we pretty much heard that admitted now.

So really my final, final point is that come May, in terms of data release, registries are slightly on their own and we're going to have to develop our own policies for data release in the absence of anything concrete as yet. And in a vacuum we're going to have to do what we need to do to give legitimate parties access to data, as we always have done and as we fully intend to going forwards, because obviously trust and cooperation with law

enforcement and rights protection is a high priority for us. We will continue to do that. But I am very concerned about the fragmentation of those sort of policies going forward. That's it. Thank you.

STEVE DelBIANCO: To echo the words that Nick had for ICANN, thank you very much. And we're next going to Thomas Rickert. And as you know, Thomas knows far more than most of us about GDPR, but to quote another famous German, Albert Einstein, imagination is more important than knowledge, as in I can only imagine how Thomas can limit himself to six minutes but we shall see. Go ahead, Thomas.

THOMAS RICKERT: Steve, first of all, I'm flattered by you mentioning Einstein and myself in the same sentence. That's so inappropriate. Let me applaud ICANN for publishing the cookbook. ICANN has managed to find the second best name you can have for a data model after the playbook name was already taken, right? No, on a more serious note, thanks, ICANN, for the interim model. Thanks for the cookbook that has recently been published which has an awful lot of improvements that we would really like to applaud ICANN for. So we finally saw ICANN engaging with the community far more actively than in the previous months, and

although there will be some duplication with what Nick has said, it's worthwhile reemphasizing some of the positive aspects of the cookbook and the interim model.

First of all, the possibility for contracted parties to apply this model at the global level in order to avoid fragmentation in the marketplace. Then the -- that no distinction needs to be made between natural and legal persons because as many of you well know, but probably most of you will not know, the names of legal entities, which you might think is corporate data and therefore not personal data, can be personal data if they allow for the identification of an individual. And if you're dealing with sole traders or small- and medium-sized companies, in many, many cases the names of the founders or shareholders are in the company's name. And therefore, not being forced to make a distinction between the two bears a huge risk of publicizing personal data. So that's great news.

Then the limited publication of registrant address details is great. Further, the fact that the publication of the email address, phone number, fax number is no longer required but that this is to be replaced by contactability means by virtue of an anonymized email address or Web form, that is great. We've discussed this with the contracted parties and the contracted parties volunteered to take ownership of this when it comes to operationalizing the possibility to contact the registrant. So

they will come up with proposals on how to make this possible from an operational point of view.

Also, we would like to applaud ICANN for acknowledging issues with the self-accreditation based system for gated access. Because we do not see any possibility to make that work in a compliant fashion.

Having said that, there are many areas in the cookbook where we are waiting for additional information and which need more discussion. So, for example, the collection of full thick WHOIS data is assumed to be required without any further legal rationale or explanation. So we're not saying that this is per se impossible because of the principle of data minimization but we need more information as to why ICANN thinks that the collection of these data elements is required. So we're looking for guidance and legal grounds on that aspect.

Same would apply for the transfer of data from the registrar to the registry, where we are waiting for a robust legal rationale as to why this can take place. With respect to the retention period of the duration of the registration plus two years, this is something that can be discussed. But again, there is no rationale in the cookbook as to why this is required and we're waiting for information on that.

I guess the most important point, though, is the gated access system that ICANN is proposing and the role of the Governmental Advisory Committee. And we do have concerns that asking the Governmental Advisory Committee and governments to help operationalizing this system will redefine the role of the GAC, which, according to our bylaws, is merely advisory role. As many of you will know, the GAC as well as the European Commission have sent letters to ICANN asking for the gated WHOIS access system to be as open as possible. There have been requests by the GAC not to deny access to an accreditation system based on the origin of the requestor, yet there have been requests both by the GAC as well as the commission to be fully in compliance with applicable national laws when it comes to disclosing data. So I think it's perfectly appropriate to ask the governments and the GAC to offer legal advice as to how this can be made to work legally. But operationalizing a gated access system is something that needs to be done by ICANN and its community.

So I think I should end my little intervention here. I think I'm even a little early, Steve. So I hope that we will have more time for discussion subsequently.

So in essence, we're waiting for more information that -- information that allows the contracted parties to legally assess the proposals made by ICANN.

STEVE DelBIANCO: Thank you very much, Thomas. And we're next going to hear from Cathrin Bauer-Bulst of the European Commission. But first, I did want to remind you all that the questions that both Thomas and others have raised are partially reflected in this cookbook that ICANN published last weekend. Approximately half the pages of the cookbook, all of section 5, that is, actually recounts the discussion in the community, the comments that were received, does a decent job of showing both sides of the argument, and I think tees up so many of the key questions that we are hoping that DPAs will be able to respond to. So with that, I'd like to turn it over to Cathrin.

CATHRIN BAUER-BULST: Thank you very much. And thank you to Thomas for already emphasizing some of the points on the GAC's role in this. I'm going to expound on this a little bit more. But first, I just wanted to take one minute to explain why this matters so much to the GAC and to all of us. It basically comes down to one basic principle, people expect the Internet to be a safe and secure place and ensuring that safety and that security requires a very minimum of accountability. And as you all know, the WHOIS plays a key role in this.

Now, this is why the GAC has strong views on these issues, as does the European Union. And just to clarify the position that was submitted by the European Commission actually reflects the position of the still 28 EU member states and the European Commission jointly, so it's the Union position. And both the Union and the GAC have insisted that ICANN preserve the WHOIS to the extent possible in line with its commitment and in line with compliance to the law.

Now we do appreciate the challenge inherent in this exercise. And we welcome ICANN's efforts very much in providing the cookbook and the calzone that was cooked on the basis of this cookbook.

Now, as you all know, the Internet is a public resource governed by a set of private arrangements that replace a system that is otherwise in similar spaces created by international and international laws. Because the contracted parties administer a public resource, there's responsibilities that come with that and they have to serve a number of public policy interests.

Now, ICANN's mandate goes beyond the mere technical function of mapping names to numbers. Now we have the odd situation where there's a set of contracts between private parties that serve the interests of those parties but at the same time also have to serve a number of public policy interests. And one of

those public policy interests is that there needs to be a minimum of accountability online.

Now, this does not call into question compliance with the law. The GDPR provides a number of mechanisms for this as set out in the European Union position, which outlines in a lot of detail how the various public and legitimate private interests can be taken into account using the mechanisms provided by the GDPR. Goran has already recited this. And is also set out in the unique position that the GDPR does not prohibit the publication of all personal data. Publication has to be proportionate, serve a specific purpose, and you need a legal ground.

Now, the GAC has identified a number of positive aspects in the proposed interim model. It has a clear objective to identify clear purposes for the processing of WHOIS data, which is an essential element. It has a commitment to continue full data collection and recognizes the key role that the GAC has to play in the accreditation mechanism.

Now, I just want to flag two points where the interim model does not yet seem to meet the requirements set out by the GAC. And I invite you all to consult the comprehensive comments the GAC has made all throughout this process for further points. First of all, as Thomas has already highlighted, there's still some of the rationale missing for the publication or non-publication of

various data elements including registrant name and email address.

While the cookbook has a summary of the input that the community has provided and the recognition that not everything can be made public, there is no clear explanation of why precisely the choices were made that ICANN has made here.

And that requires a lot more detail, because there needs to be an assessment of the necessity and of the proportionality of the data processing in light of the legitimate purposes pursued. And that's also a basic element for any conversation with the European DPAs.

My second point is on the accreditation model itself.

Now, this is a key element because it will determine how everybody will access the non-public part of the WHOIS data, those actors that have a legitimate purpose for accessing it.

Unfortunately, it remains the least clear part of the picture. There's two aspects to this. First of all, we will need a solution for the short-term. Because it's clear to everybody in this room that we're not going to have a fully fledged accreditation system in time for the end of May.

So in the short-term, we need a temporary solution because otherwise we cannot go live with tiered access and, by

extension, with not publicly disclosing certain data elements. So there needs to be harmonized mandatory procedure based on the pursuit of legitimate purposes.

In the long term, we will need to design the full accreditation system. And the fact that the GAC has to play a key role here has been recognized.

However, as Thomas has already highlighted, the GAC is an advisory body and cannot assume an operational role. So the GAC welcomes the opportunity to provide guidance on the accreditation mechanism and on codes of conduct, if those should be chosen. But it cannot relieve the joint controllers of their responsibility.

Now, the GAC will continue to discuss its role in this possible process in the coming days. And I invite you all to join us over in Ballroom 2 for those discussions.

So, to summarize, I think we've made a number of very important steps forward. But there's a large number of key areas where the interim model and its implementation will require further work. The GAC has provided detailed guidance and stands ready to continue the constructive cooperation.

Thank you again to ICANN for the efforts it has made at accommodating the various viewpoints that the GAC has already

put forward. And we look forward to working on the model together to try and accommodate them. Thank you.

STEVE DELBIANCO: Cathrin, thank you for that perspective from the GAC's public safety working group. I'll note that the two gaps which you identified -- one gap was a lack of a rationale to hide the registrant's email from the public and public display. And the second was a lack of an adequate exploration of what to do while we wait for an accreditation model for gated access. I appreciate that.

And it tees up well for the next two speakers, who are business users of WHOIS for purposes of cyber security, consumer protection, and brand protection.

We'll hear first from Patrick Charnley with the Coalition for Online Accountability and the intellectual property constituency at ICANN. Patrick.

PATRICK CHARNLEY: Thanks, Steve.

Yes. So we're going to talk a little bit about why access to some public WHOIS data is, in fact, very important and explain that through some actual uses of this data. And then I'm going to

talk briefly about elements of the ICANN interim model and how we see things going from here.

I work at IFPI, the International Federation of Phonographic Industry, which is the recording industry. We have a 24/7 operation that monitors the web for infringing content and takes it down on behalf of our members and their national groups.

We found in 2016 some 19.2 million infringing URLs of our members' content. And it's a big operation to prevent serious commercial harm as a result of those infringements. One of the most important data points for us is the registrant's email address.

We use that, one, for contactability. So many of you will be aware of the DMCA and equivalent legislation around the world which requires us to send notices to certain infringing sites to take down content.

We need to be able to send that notice directly so that we can have a delivery receipt and a "read" receipt in order to evidence the fact that the site does have knowledge of the infringement. It was mentioned earlier that perhaps a relay system wouldn't even be necessary in the existing model, which raises the question how are we supposed to ever protect our members' rights if we can't contact these people? And relay is simply inadequate.

Also, for investigations, because what we often find is that one operator of an infringing site will be running other sites or other criminal activity. And we're able to investigate through the email address, which happens to be normally the only piece of accurate WHOIS data -- we're able to investigate and establish patterns of criminal activity and, therefore, to take action. So the email address is, in fact, absolutely essential. And, when it comes to establishing who is leaking, for example, prerelease music where a recording has been leaked before it's been commercially released and causes enormous damage to the artist and record companies involved, the email address is absolutely vital.

But this is broader than just IP infringement. It goes to consumer safety. Tim is going to talk about that in a bit. But from our own experience of that, IP infringement is used to steal consumers' identities. And we know the City of London police, for example, with whom we and other right holders have worked, has noticed an increase in the use of stolen identities where a person's email address is stolen in the process of them accessing infringing intellectual property. And then that email address is used to register domains and to serve malware, phishing, and other content that harms the public interest more broadly.

So that is why having some information publicly available is absolutely essential for our constituency. And IFPI is but one member of the IPC. And these activities are carried out by all of our members and by organizations across the world.

We would urge you to look at the email sent by a coalition of some 60+ child protection and intellectual property protection and other organizations to the DPAs and to governments which explains these points in some more detail.

So, in terms of the model itself, some of our concerns are, firstly, that ICANN has repeatedly stated an intention to stick as closely as possible to the existing WHOIS system. And yet what we see is a model that does not achieve that. It seems to us to be a very blunt tool in which -- which overreaches in terms of seeking to comply with the GDPR.

That is shown, for example, by the paucity of public information that would be in WHOIS by the application to both legal and natural persons despite the GDPR being very clear that that is not required and by the option of applying this globally when it's not a global piece of legislation. What concerns us most, probably, is that we do not see evidence of adequate consideration having been given to the very important public interest uses, including the ones I just outlined. We don't see that evidence in the documents supporting the ICANN proposal.

So it's not at all clear to us that the correct proportionality analysis has been conducted in order to reach a conclusion that it is not possible to publish the registrant's email address in the public WHOIS.

This is despite the Article 29 working group having -- working party having highlighted that there is no prohibition on publication data but that the analysis needs to be conducted correctly. We simply do not see evidence of that having happened.

And we do believe firmly -- having considered this point very carefully ourselves, we are well aware of the importance of protecting people's fundamental rights to their personal data. We are well aware of that.

And we have taken that into account when considering where we think the correct proportionality analysis comes down. And we do believe that having an access point of the publication of email address in view of the numerous public interests associated with that is where the correct analysis comes down.

Then I think, finally, where do we stand on the next steps? So we understand that an accreditation process is to be designed. But we do not understand when and by whom. We know that the GAC has been asked to be involved in it, but it's not clear whether they've accepted this challenge.

So we ask ourselves -- and Cathrin alluded to this -- where are we going to be when the model is implemented? Are we going to risk a blackout situation, because there is no mode for access in the interim period?

And, if we do, do people fully understand the serious harm that that will cause to the public interest?

And Tim will come on to that in more detail. So we ask ourselves, would self-certification be acceptable in the interim period? And, if not, then we need an accreditation system very quickly.

And I would just finally sum up by saying that members of the IPC and the business constituency are working very quickly on an accreditation model now which we hope to be able to communicate to the community very soon. And we would really hope that our views on how accreditation would work could be taken into account in a serious fashion and way that we are not convinced has happened so far in terms of the importance of updating WHOIS. Thank you very much.

STEVE DELBIANCO: Thank you, Patrick.

Patrick, I'll note that, when Goran told us earlier that the proposed interim model has been sent to the DPAs, I think it's

clear that the hope is that the DPAs would give an indication as to whether they believe that the proposed interim model would be compliant.

But what I think you've raised, which is slightly is different, Patrick, is we would welcome guidance from DPAs about whether they went further than they needed to in terms of pulling, for instance, an registrant email address out and making the other recommendations that are in this model. So I think we all would share the hope that the DPAs would be as clear as possible about the adequacy and potentially whether we over-complied in ways that they can help us understand.

Now we'll next go to the CEO of Domain Tools and a member of the business constituency, Tim Chen.

TIM CHEN: Thanks, Steve. And thank you for inviting me to share my views on this panel.

It's an esteemed panel. I look down on this row of people, and I'm reminded of what Elizabeth Taylor's 8th husband said on his wedding night, which is, "I know what I have to do. I just don't know how to make it interesting."

I'll do my best. This is an extremely serious topic and one we spent a lot of time on.

Just in terms of context, Domain Tools has been building research tools on top of research data and significantly WHOIS data for nearly 20 years.

And we count among our customers over 500 organizations worldwide, many of the largest and most sophisticated computer emergency response teams in governments and over 100 customers in the EU alone.

I will do my best to represent their interests as well as the interests of the BC here on the panel here today.

One of the items that Patrick mentioned that I do want to speak briefly to is consumer protection. I don't think you naturally think about that when you think about some of the enterprise and network security use cases for WHOIS data. But, ultimately, WHOIS data is used every day. And it's built into the fabric of the security that happens at the margin or at the last mile of the Internet.

This is in the form of domain reputation systems that are used to enable or block email traffic, enable or block web traffic, or other DNS traffic. This is the kind of work that protects people like you and me, all of you out there in the audience, all of us up here, everybody we work with, our families. The work that security practitioners do in their day-to-day work has an effect in the last mile for all individuals who are connected to the

Internet. And they're a constituency that I hope is duly represented here as well.

I also want to add that, as a member of the BC, we take the privacy of individuals worldwide very seriously and support the spirit of the GDPR and what it's trying to accomplish.

What I think I'm trying to do is make sure that, you know, we know that all issues at this level of policy really are trying to achieve a balance of the equities that are at stake. Goran has talked about this. And trying to find a balance of the equities that are at stake here. And, like Patrick said, we believe that the voice of the business users and of the security practitioners in my personal case need a voice here as well.

I encourage everyone out there to get involved in the conversation while there's still time to comment on this model.

Specifically, to move to the model itself, which is what I was asked to talk about, Patrick has talked in detail about the email address. So I don't want to belabor that point.

There was a submission by Microsoft that talks about the use of email address and why it's so important. What I can say is that we studied our user base. We did a poll of what data fields in WHOIS is most useful for the most important security use cases

and work flows that you operationalize inside your SOC every day.

And, by far and away, the registrant email address in the WHOIS record was number one. So, when we think about trying to come to the table in the spirit of compromise and finding an outcome here that's palatable to all parties, that is a data field that I hope gets reconsidered for inclusion. Because it's unique. And being unique -- it's so important in security to be able to have a unique identifier of some kind associated to DNS resources like domain names. It is validated by the registrars at the time of the domain registration. It's certainly required to do the registration, and it's available now.

So, if there's one field that our constituency would like to see, as Patrick has talked about, the email address is critically, critically important. And, if you read the submission by Microsoft, that gives you detail why that is from a security use case context.

The second point I'd like to make is really to make sure that the security practitioners are included as a constituency for the gated access system that a number of people here have talked about.

And so something we can definitely agree on is there needs to be much more detail in what the accreditation process is going to look like and how anyone, really, besides law enforcement is

going to get the support of the community and support of the model to get access. Really, any interruption, even a day's interruption of access to key pieces of data that security practitioners use every day to help protect their networks, which is their employees and customers and their IP and all Internet users as I talked about, is a significant disservice to all of us. And, absent some rapid progress on accreditation model, I'm concerned that there is no solution to validate people that have legitimate interest in this data for what I believe are all the right reasons. Again, to refer to publications that are done by very thoughtful people who are doing this work, there was one two days ago by the folks at the mobile messaging and malware anti-abuse working group, known as MAAWG. It's one of the most long-standing membership organizations of security practitioners involved in email -- originally, email traffic and now web traffic as well.

And they have a short statement on the importance of this for the security community. The reason that I draw your attention to that is it's one of the first times that the security community together through one of its organizations has made a comment specifically on this process.

And it's much better for you to read it from that organization than to hear from me as a representative. So I encourage people

to read that. I think it's a very thoughtful and balanced approach published on the ICANN Web site.

The last topic that I'd like to introduce, which is really just introducing a topic for community discussion, is a topic that I don't think has been surfaced in a clear way so far in this process. The -- excuse me. The -- one of the most important security use cases for WHOIS data is ability to search across the dataset to correlate that domains relate to other domains. I won't get into the detail there, but it's extremely important. It's used by nearly all of our customers every day to do really important security work, both individual investigations, live investigations of malicious activity on network as well as proactive scoring and blocking of traffic that happens to scale by machines on networks worldwide. And the only reason that there is any database, if you will, a searchable -- ability to search across DNS-wide WHOIS records is because we built it. There is no mechanism within ICANN to do that. And absent individual searchable WHOIS that exists in a limited number of TLDs like Nominet, for example, only on the datasets that they make public, it doesn't exist, individual registrars with TLDs. There's a fundamental question at stake here which is whether or not that critically important secure use case is going to be enabled or disabled through this process. The way that the model is written right now, it reads as if it's disabled. A limited amount of data

available in the public dataset which hopefully still has port 43 available for a higher volume access to the data, and then no discussion of what happens behind the gate. If the outcome is there is no access to the data at scale behind the gate, basically that function goes away. And it's my hope that if it's not us, either the registrars themselves somehow through ICANN, there's still the ability for people who are practicing security for all of our best interests have the ability to do that research, have access to data they need to do that research, because it's critically important. Thank you.

STEVE DelBIANCO: Thank you, Tim.

[Applause]

Yeah, and I'll note that the two business users had a very different perspective. I think that Tim Chen's company has far more programmers and data scientists than it does lawyers. And these programmers and data scientists are using port 43 access, single specific queries, to build the data that they use for a lot of other purposes. Purposes that Patrick and Cathrin and others have used. And that is why we put port 43 in italics in the dead center on the slide in front of you which is to try to seek some clarification as to whether that will be maintained in the

post-interim model world. Maintained both to the public side of the data as well as the gated access side.

All right. Next up we have Stephanie Perrin representing the non-commercial stakeholders group of the GNSO. Stephanie.

STEPHANIE PERRIN: Thanks very much for inviting me to this panel. The non-commercial stakeholders group represents the end user. We have published a preliminary response to the cookbook yesterday, and you will find it on our Web site and wiki. I'd be happy to provide further detail.

I feel honored to be on this panel, but also a little guilty because there really ought to be an independent data commissioner sitting on this panel, and you'll forgive me if I channel my -- my former employer, the office of the privacy commissioner of Canada, because I feel some of those perspectives need to be ventilated here at ICANN. I'm looking at Kathy Kleiman of NCUC in the front row who invited me to speak when I was in that office in 2005 at the privacy meeting. The facts and the legal interpretation have not really changed, folks. What we have now is 4% fine.

In terms of getting advice on how the data commissioners feel on this matter, the international working group on data

protection and telecommunications released a paper on Friday that goes into great detail on how the global data commissioners feel. I think it would be cynical indeed if ICANN encouraged only compliance with the GDPR and left it as optional for other citizens to not have their rights respected. There should be compliance with law, which is one of our bylaws.

In any case, there's -- there's a view, a commonly held view, I would say, that the non-commercial stakeholders group does nothing but take pot shots. Not true at all. We're busy working on solutions here. And in terms of tiered access, I'm going to focus on tiered access, because quite frankly, Thomas and I agree on most things. I commend you to read the eco workbook. It's the best legal analysis I've seen since I've been volunteering at ICANN. And everything he said was great. I more or less agree with. So I'm going to skip to the things that we don't think are great, but that doesn't mean we aren't supportive of so many of the good things that he signaled.

Tiered access is a very difficult task. We do not believe that self-accreditation is a reasonable model, and I'll leave it to your lawyers to tell you why you'd be crazy to depend on self-accreditation. We have -- some of us are working on the concept of international standards, possibly an ISO standard, but we're open to all kinds of different approaches and we'd like to have a

workshop in Barcelona to discuss these things there are already ISO standards to accredit those who, for instance, give certifications for Web sites. This is not rocket science. It will take time because standards efforts always do, but that's really what ICANN in its accountability model ought to be aiming for.

I talked about this at Abu. I'm now on to a new project which I haven't necessarily talked people into but that would be COSO standards of accountability for ICANN and its processes. And I would go down from tiered access to the need to make the actual human rights bylaw real here and apply a human rights standard to this effort. Well, let's give it a whirl. Let's try a human rights impact assessment on this, because in the non-commercial group we care about free speech. We care about protection of people who are free speakers, who are political dissidents, and this is what exposure in the WHOIS means to us. It's not just the data protection issue of protecting name, address, and phone number. It's exposing people to violence, which is what happens, and we have the data on this, should you question this. So it's really important that human rights becomes real and implemented. That's the kind of thing that COSO measures, and I would encourage the ICANN administration to get with the program and think about a maturity model and what these metrics might be. So we are quite concerned about this.

I'm going to just skip down to a couple of other elements. We do not actually agree that continuing to -- to gather the thick data is necessary and proportionate. We should be focusing on data limitation. And this is well recognized around the world globally as a key principle. I would also point you to the Council of Europe's guidebook that they published in the context of the Convention 108. They took the time to focus on ICANN's procedures and policies here. Please, we should have some respect to this effort that has gone on in the data protection community.

Moving along, we certainly endorse the anonymous email mechanisms. And while I take the point that our cybercrime fighters in the private sector need some of this data, so do health researchers and they've been getting along with a lot of good data analytics on anonymous data. There are ways to allow you the kind of recognition -- the kind of tracking that you need without having the actual email address public and in any case, if you are actually going to take these -- these sites down, as opposed to just blacklist them, you can certainly get accredited under the ISO standards. We don't, you know -- we're all for respect for privacy, but we also like law enforcement and we like cybercrime to be stopped. It is not true that we are promoting these -- these nefarious activities. We're just trying to make sure that the end users are not put out there

at risk in order to facilitate cheap and easy access. And it's our position that this is what has gone on for the past 20 years, and it's certainly time that it stopped.

One further thing, and I'm -- I'm watching Alan because he's timing me and I must be over time already here.

STEVE DelBIANCO: Yeah, just last point.

STEPHANIE PERRIN: Last point would be the purpose of processing. You cannot, in the terms of data protection, consider a purpose of processing to be in the public interest. You cannot start with every third party access to data as a bunch of use cases and say that's the purpose of processing, particularly when those have been -- and the data commissioners have pointed this out -- they've been against the law for many years. So we would like to keep it to the narrow remit of ICANN and consider the purpose of processing to be tightly limited to ICANN's purpose. Thank you.

STEVE DelBIANCO: Thank you, Stephanie.

[Applause]

And I note that Stephanie's point about anonymized emails would work only if the anonymized emails were consistent across registrant. The very same registrant would have the same anonymized email and every TLD and every registrar or registry, well then correlations would be possible. But if it was anonymized to each registrar, you can't do any of that correlation that Tim talked about. So there's a key point to bring up.

Finally, we have Alan Greenberg, chair of the At-Large Internet users, the At-Large Advisory Committee. Alan, over to you.

ALAN GREENBERG: Thank you very much. And in fairness to Stephanie, I was timing everyone, not just Stephanie. I wear a mult -- a number of different hats. I am chair of the At-Large Advisory Committee. I'm also chair of the RDS WHOIS2 review team, and I am not speaking on behalf of either of them here. The review team, because we are just in the midst of starting our work, and at the ALAC because although we have had some discussions regarding this, we have certainly not come to closure on a position. So although I will reflect in a moment some of the principles the ALAC will be working with, not necessarily -- certainly not the outcomes.

The ALAC, the At-Large Advisory Committee, represents the interests of Internet users within ICANN, and at last count there -- it's questionable, it's some debate, but the number seems to be around 4 billion now. We consider registrants, individual registrants, as users. Obviously a much smaller number than the 4 billion. And we, a long time ago, faced the issue of how do we balance the issue -- the interests of the users and registrants where they differ, and occasionally they do. And we took the position at that point, and I will -- I would be surprised if we change it today, to say if we have to balance 4 billion versus 100 million, or whatever the number is, we come out on the side of the 4 billion, if indeed there is a difference between the two. And here there clearly is potentially a difference.

When the current interim model was announced, I think the single word that describes how I felt is "relief," compared to some of the possibilities I thought it might be. That doesn't necessarily indicate satisfaction, but certainly it was more balanced than some people were predicting it was going to be.

And now I am talking not on behalf of the review team or on behalf of ALAC but my own personal positions. Privacy is important. But ensuring that we have the tools to combat cyber abuse, cybercrime is equally important. And I'm not going to go into the details of email addresses or other things, but ultimately, as has been pointed out, if we end up in a position

where we're going to black out all of WHOIS for both law enforcement on the short term and the non-law enforcement people who are fighting cyber abuse, even for a short period of time, it's not going to be a nice situation. The people that are working -- you know, the malware people, the abuse people, are rather innovative. We saw the largest distributed denial of service attack last -- about a week ago and not only was it the largest but it was also using a different technique. And, you know, the world is changing as we move forward, and we really need the tools to fix that.

In terms of the specific model, I was a bit disappointed that there wasn't at least an attempt to recognize legal versus natural persons. I understand that if my company name is alangreenberg.com, that's personal information. I understand that even if I'm, you know, some big corporation and I choose to have the person responsible for my domain names use a personal name in their email address, as ICANN does, for instance, that is release of personal information. But I believe that's an issue for that company to consider. So if I as a -- as a legal person provide personal information as part of my contact or part of my company name, I think that's a GDPR or other privacy issue for that company and not for ICANN. Unfortunately, ICANN has never distinguished or asked registrants to distinguish between whether they're a legal

person or a natural person. So we have a really big problem in the established database. And yes, we have an organization name, but that's used -- my registrars tell me it's used very flexibly in interesting ways. So we have some real problems.

And lastly, the issue of the accreditation system -- sorry, one more issue. Very few real users look up names in WHOIS. Okay. But as has been pointed out, WHOIS is widely used in the domain reputation business and, you know, if you use any standard browser, it's using the information that's been gleaned by WHOIS to say, do we trust this domain or not. And your browser automatically will flash up a message saying, you know, are you sure you really want to go there. So you may not use WHOIS for consumer trust issues, but the infrastructure behind you does.

And lastly, I also have concerns about the interim, interim accreditation system. You know, what happens when this goes into place. I'm hoping the answers that come back from data commissioners are, you know, we'll have some flexibility. But if we don't, you know, how do we stop things from being blacked out for the people who are trying to help us. Anyway, and that's all I have to say. And I'm at six minutes.

STEVE DelBIANCO: Outstanding the way each of the panelists stuck to the six minutes. And we're going to have plenty of time then for audience Q&A. But before we do, indulge me for just four minutes to remind everybody that it doesn't stop here with the interim policy. I want to try to remember that the ICANN process is about bottom-up development of consensus policies. And the way ICANN's contracts work with registries and registrars and if we do our job, the policies that we develop in the RDS PDP policy development process replace the interim model. At every stage of this debate, whatever ICANN has published, proposed interim and drafts, they've included an acknowledgment of what interim means, because it means temporary. ICANN acknowledges that the interim model we've been discussing will not replace the multistakeholder policy development activities and they named three of them in particular, the privacy proxy services which are used by about a quarter of gTLD registrants today. There are updates to ICANN's procedure for trying to resolve WHOIS conflicts with local laws, nationally privacy laws. And finally, what I mentioned earlier was the development of a new policy framework, the RDS PDP, the next gen RDS that Stephanie spoke of earlier. That is our responsibility. And as this diagram shows, the ICANN community, that's at the top, that's us. It is our job to deliver those bottom-up policies. We've struggled for years, but perhaps this will be a renewed sense of urgency because once we deliver it, you'll see that the new RDS

implementation replaces the interim compliance model. I don't know what date that is, there's a question mark next to May 2019. The bottom row of this is the Data Protection Authorities themselves. In May they undergo a magnificence transformation and become the European Data Protection Board and as such there's hope that more specific guidelines would be issued. There's even hope that we'd see binding opinions on the new RDS implementation that we eventually come up with as a community.

So with that, I'll go back to the key point in front of us which is this diagram. I wanted to first give our panelists an opportunity to respond to what each of the others have said and then we're going to immediately go to audience and Adobe Q&A. So anyone on the panel. Goran first and then Thomas.

GORAN MARBY: Thank you. Something that occurred to me during this presentation is that the model we've actually ended up proposing seems to be nobody likes, but for totally different reasons. So we seem to me to be very good at distributing misery evenly. Yeah. Anyone want my job?

There's just a couple of things I want to point out. I'm really -- I'm really help -- I'm really happy about the fact that on this panel here we all say the same thing when it comes to we need

firm guidance from the DPAs because we don't know. We have some guidance from the DPAs, we have a very good relationship with them, but if this is really going to pass over to the -- after the law is enacted, we need that firm. Otherwise, there is a big risk that the WHOIS will be fragmented.

Because we will not be able to enforce our contracts, the ability for us to diminish, I think Jamie has told me to say. There's one thing several of us has talked about.

We never asked the GAC to be operational. Give me a second to explain that extra.

When it came to police forces -- and, remember, the alternative for having an accreditation system is probably due process. If we sort of -- forget the old WHOIS. In the GDPR world we have to do something different. So think about this on the line how to get for good reasons access to the information which is sort of behind the firewall. One starting point in that is due process. You need to have a court order to get access to it. That's one starting point. As I've said, I have to figure out a way of being in between the policy set by the community and what we believe is what the law says. So we started by looking into self-accreditation (indiscernible) system.

And anyone that can come up with proposals for systems, please provide them. So far we haven't seen so many. I heard there

were a couple here and a couple there. And I genuinely ask. Because what we heard so far or what we understood is that governments like government involvement. We're not talking about the GAC.

So, first of all, police forces. We just happen to have the GAC here as an assembly of governments. So the first thing we proposed was that police forces around the world get through their -- it's the country itself that decides that, sends that through the GAC to us.

So it's a mechanism to show -- to give it to us. Because they talk to each other. They are governments.

The second one, then, which I truly understand from some of the -- it was mentioned that we are doing a lot of work with our OCTO team, Office of the CTO, for instance, to start calculating how we can better -- I think there are presentations about that here during this meeting as well where we try to look into how the market actually behaves. What we call the bad domainers.

We don't get access to that data either if we can't have an accreditation model that works. So we don't sit on a gigantic database, as you all know. We will, actually, have an effect on our ability to work as well. With that said, the other side -- and we have intellectual property as an example. Our intention was that the governments would -- through GAC come together and

do a code of conduct, how to behave. This is primarily also to give the contracted parties a sort of protection around what they then are going to do.

Because -- and then we should use something like WIPO to actually operate. You can see this in the paper. You may not agree with it or disagree with it. But it's a proposal that is based on the current knowledge we have.

If the DPAs comes back and says, "That's too much. You don't need that. We can do self-accreditation." We don't have. We will not say yes or no. If they say it has to be due process, we will accept that as well.

But it's always a good thing actually how to give a proposal how to do it.

There's one more thing I'd like to say, and this is important. Let's say we have now a system for, for instance, the causes of Internet security. And those people download data. There has to be an agreement between contracted parties and the companies who get access to that data. Because it has to be a limited purpose for actually accessing the data. So what happens probably -- and this is something we need to look into, actually. They have to look into. When you transfer that data into another database which is outside the WHOIS database for, for instance, the purpose of looking into abuse, you probably are

applicable through the GDPR as well, which means that you have to have the safeguards as well.

I would not say -- because my lawyers and my communication manager would say that I'm not allowed to say this. But in some extent GDPR is a virus. I didn't say that.

UNKNOWN SPEAKER: I didn't hear it.

GORAN MARBY: Thank you. And it's not on record.

STEVE DELBIANCO: Thank you, Goran. So I'll note that on the right-hand side of this diagram, that is exactly what it represents. The ICANN proposal that the individual governments pass lists to ICANN via the GAC. The GAC, in that respect, is simply a conduit.

In the bottom right-hand corner, a certification program or code of conduct would be developed by individual governments. And I believe the GAC would, therefore, be a coordinating body and simply pass through the entities that are certified to fit the code of conduct. So I don't think GAC has as large a role as some have feared.

Now we'll go to Thomas Rickert.

THOMAS RICKERT: Thanks very much, Steve.

Some on this panel have called the plan not to publish the registrant's email address as over-compliant. While I understand that email addresses can be a valuable source for investigations and other activities, let me read out to you two sentences of a letter that has been written by the chairman of the Article 29 group back in 2006.

In the light of the proportionality principle, it is necessary to look for less intrusive methods that would still serve the purpose of the WHOIS directories without having all data directly available online to everybody.

The original purposes of the WHOIS data directories can be equally served by using a layered approach as details of the person are known to the ISP which would be the registrar in this case that can, in case of province related to the site or the domain name, contact the individual or transmit the information to an enforcement authority entitled to -- entitled by law to access this information. So that's been out there for many, many years. The first correspondence dates back to 2003. So I don't see any way on how you can publish the email address in a compliant fashion.

Second, many on this panel have highlighted the importance of the WHOIS database. And we appreciate that. It is a great source.

The only problem is that it has been provided illegally for many, many years. And this can't be perpetuated. So we need to find ways to make data accessible as easily as possible to those that have a right to get access to the data.

And the question is: How can that be done? So let me try to demystify a little bit what this notion of legitimate interest means. That is enshrined in Article 6(1)(f) GDPR for those who want to read it. So you can have a legitimate interest of the controller, which would be the registrar or the registry, or a third party, which could be ICANN or law enforcement authorities or trademark owners for that matter.

But in that case where you claim to do data processing -- and revealing data would be a processing activity -- you need to balance the right of the data subject against the legitimate interests of those who are claiming it. And making WHOIS data available, in gated access or otherwise, in the above fashion to all requesters would mean that we think that those legitimate interests outweigh the rights of the data subjects in the WHOIS database for all the data subjects in the WHOIS database.

And that is not easily done. We don't say it's not possible. But you need to write up a robust line of argumentation why you think this is feasible. And this is where we need the government's help in order to make that possible in a compliant fashion.

Last quick remark, Steve, you were spot on saying that this is an interim activity. It is the compliance activity we're discussing now. And we really need to dive into the community process in parallel or afterwards because ICANN takes its legitimacy from community-driven consensus policies. And these need to be adjusted to the new legal environment as we move on.

STEVE DELBIANCO: We have one more panelist reaction from Patrick. And we'll make it quick. We'll look to the room. We have five mics distributed in the room. And I know that we have a number of questions that Rita and Jeanette have accumulated from the Adobe chat. So, Patrick, before I turn to you, I did want to try to correct the vocabulary a bit. The cookbook calls for bulk data transfer only to ICANN. Those are the blue arrows in the lower left-hand side of the diagram. Those are bulk transfer. There is no bulk access other than data escrow at ICANN. There is automated access through port 43, single specific queries that, once queries have been obtained, they can be stored and

analyzed. There is no anticipation of bulk transfers of data en masse to anyone outside of ICANN or the escrow providers.

Patrick.

PATRICK CHARNLEY: Thanks. Very briefly. Thomas, you raised some interesting points there in terms of how you actually carry out this analysis.

Looking back to a statement made in 2006, I'm afraid I don't think takes us anywhere. Because what we don't know, A, is what was taken into account when that statement was made. What we do know is that, in the 12 years since that statement, cyber crime, intellectual property, the nature of the Internet itself has changed vastly.

And one of our concerns is making the correct assessment now, doing the balancing act between legitimate interests and -- which, by the way, intellectual property is a fundamental right in the European Union -- and the rights of the data subjects themselves, do they have access to all the relevant evidence to carry out that analysis?

And one of our concerns is that we do not know what the DPAs have been presented with when they've been asked to make this assessment. Thank you.

STEVE DELBIANCO: Microphone number 2 is first. Please go ahead. Erika.

ERIKA MANN: Thank you so much. I have two comments. I wonder, listening to Goran and to J.J. at the beginning, I think both of you pointed to the fact that you somehow like to globalize the European and EU-specific GDPR system.

I wonder if you plan to do this in all relevant other legal cases which might pop up around the globe in the future as well. And my second point to the request with regard to access for legitimate cases to the WHOIS, are you planning maybe to look at existing systems which are already in place either by telecom operators or Internet companies? Because I'm not sure if you really need to invent a new system.

STEVE DELBIANCO: Goran.

JOHN JEFFREY: So on the first question regarding the applicability, how would the model apply, at least in the interim model -- and I think there's policy development work to see how that goes as it becomes a policy.

But at least on the interim model, what we're trying to do is allow it -- obviously, it needs to be applied to European economic area.

But what we're hearing from some of the contracted parties is they're going to have a very difficult time distinguishing between from those registrants that are in the European economic area and those that are outside. And with the fact that they'll be violating the law if they get that wrong and ICANN's interest in it as a data controller as well, we think it's important that some of them will be able to provide that on a global basis, apply that policy globally if, in fact, that's what they choose to do. If there are unique cases where they're only dealing outside of the European economic area, they don't have registrants, then they would have an option available to them to not apply this model but to comply with the existing WHOIS system.

STEVE DELBIANCO: Thank you, J.J.

We're going to go to microphone 4. That always makes me nervous when a questioner has a computer in front of them. Because this is not a great time to read statements.

It's a great time to interrogate a panel, including the CEO and general counsel, since written statements are supposed to be

submitted all through this process and can still go in to GDPR@icann.org. Number 4.

BRIAN WINTERFELDT: Thank you so much, Steve. I'm sorry my laptop makes you so nervous. Good morning, everyone. Thank you so much. I'm Brian Winterfeldt. I'm the current IPC president.

I just want to support and briefly add to the points that were well made on the panel this morning by Cathrin, Patrick, and Tim.

IPC has made written statements, and they have been submitted. And I encourage folks to take a look at those.

We do continue to have some serious concerns about the interim model and its potential threat to the ability for us to access important information for the IPC and other folks in the community, including consumer protection, cyber security, and law enforcement to do their work.

I won't go through all the individual points that we support because, again, they were well-made by Cathrin, Patrick, and Tim. But we do continue to have serious concerns about access to critical public data, the global scope of application and, for example, the lack of distinction drawn between a legal entity

and natural person. And continued bulk access is something that's already been mentioned that's very important.

The ability of the proposed model to ensure datiocracy (phonetic) of the development of a fair, quick, and easily implemental accreditation system. Those are all things that we think are incredibly important.

My question really evolves around the accreditation approach in general. I know we've talked a little bit about that on the panel this morning. I think our serious concern is, as we see with the interim model that's proposed, the vast majority of data is going to go behind a wall and not be publicly accessible.

What is ICANN going to do to assure that the interim model is not rolled out in a way that does not have a proper accreditation system in place and will leave not only intellectual property folks but cyber security, business and other individuals who need access to that date to do their jobs?

STEVE DELBIANCO: Thank you, Brian. Goran and J.J.

GORAN MARBY: Thank you, Brian. Again, it shows that we came up in a good place. Nobody agrees with anything.

The funny thing is that there's one point I want to make. There is a negotiation trying to assemble the information and also trying to make -- we also present -- most of the things that Brian just wrote up, we actually put in the paper to the DPAs as well. Because we don't have the answer to it. No one does have the answer to it until the DPAs have said what they want.

I think that's very, very important to recognize that we now -- we reached a point where the European government, through the DPAs, have to give us firm guidance. Because I want to repeat this. And I'm going to repeat it every meeting I have. I see a big fear -- if we can't get firm -- very firm guidance that it's legally acceptable by the contracted parties when this law is enacted, that we will have a very fragmented WHOIS. And that's according to our bylaws, and that's how we commonly do things.

That's where we are. ICANN org doesn't have the mechanism to enforce if we don't know what the law is. That is important to remember. Thank you.

STEVE DELBIANCO: J.J.

JOHN JEFFREY: Just to implement, if you pull up the interim model that's been published, you'll see that there's five specific points where we're asking questions to the DPAs. And we're showing that there's divergent paths within the community. We really are concerned. Many of the things that Brian mentioned are right in the middle of those. I think there was one that isn't that's become part of the topic this week that we'll make sure is also addressed.

STEVE DELBIANCO: Thank you both. There are four minutes left, I'm told, before we have to vacate the room. That is going to abbreviate the number of questions that can be taken. I believe that Goran and J.J. will commit to do a public discussion to take additional questions while we're here this week in Puerto Rico.

Can I get a confirmation on that? I appreciate that you've been here for 90 minutes. But I hope that you would find another 60-90 minutes sometime later this week. And we'll watch for the ICANN email newsletter to know when and where it will be on the schedule.

Let me go to the Adobe room for one question. We have three minutes left.

From Steve Metalitz for CLA: "J.J., it is disappointing that you continue to state that the CLA model provides for anonymized email access. As stated in an email to you on February 22nd after you made the same assertion in a webinar session, 'We have never advocated for the solution,' and indeed in the letter sent to you and other ICANN senior executives six days ago explained -- and other ICANN senior executives six days ago explained in some detail why we thought this proposed substitution was both unwise and unnecessary."

He provides a link where the letter is posted.

"While we asked that our February 22nd email correcting the record be posted, this has not been done. So I wanted to take the opportunity to correct the record yet again." Thanks.

STEVE DELBIANCO: The record has been corrected.

That means microphone number 3, please.

FABRICIO VAYRA: Thank you so much. Fabricio Vayra. I think many of you know me either as having done enforcement for private companies for 11 years or now in the private practice representing some of those companies. So I think what that gives me is a pretty

interesting perspective for the past 18 years of how much resource goes into both brand protection, consumer protection, et cetera. And I'm sorry that Alan left the room, because I share his fear when he says that things are going to go dark.

I recently wrote an article that was entitled, "GDPR: What comes next? The parade of horribles."

In addition to being able to use a phrase from law school that I couldn't use in professional context, I firmly believe we have a big issue. Go dark. That's a big issue if people can't enforce and protect us. So my question really is for Goran.

What seems to be critical in this whole thing is accreditation. And, to avoid that parade of horribles, what do you need from us to get an accreditation model on the table today to make sure that we don't walk out from this week leading down a parade of horribles? Because I think everyone in this room would agree both from a brand protection standpoint, a consumer protection standpoint, and from all the contracted parties' perspective that what they don't want is the parade of horribles. The mass litigations, the mass subpoenas, and everything else that comes with not having data.

GORAN MARBY: Thank you. Accreditation is important, but is not the important. If you don't want to have a fragmented WHOIS at the end of May, we have to work together with the European member states and their DPAs to get firm answers. Without increased legal certainty, whatever we discuss in this room will not have a possibility for us to enforce that on the contracted parties. So I humbly ask you -- any European member here -- and it doesn't matter to me which side you're on.

Go and hug your GAC representative and ask them humbly, "How can I help you to engage with the DPAs," so we get a firm answer. And one of the answers we need to have is how the accreditation model should work.

Because in a slightly later letter than 2006, the DPAs of Europe pointed at a tiered access model. And that's important to remember.

We have had open conversations with them. To end that, we're also continuing the discussions with the DPAs going forward as well. We have a very good relationship which we may not have had before. And that relationship we're trying to strengthen, and I do think they're doing a very good job. So it's not about that.

It's just that now we need the multistakeholder model -- we need the help of GAC members to get this out. So hug your GAC members when you see them.

JOHN JEFFREY: I'd like to add, I think it's very important to realize that you have to provide the information to the DPAs about the timing as well. One of the questions that we have in front of them is what can be published in the public WHOIS on the date of GDPR effective date, if, in fact, we don't have an accreditation model in place that's fully capable of being implemented. This is a critical point. And it's one that with the registries and registrars saying they may not be able to implement the accreditation model in the 10 weeks that are left. It's very important that we have clear guidance on what can continue to be published. Is it the full WHOIS? Is it some subset? What is that?

STEVE DELBIANCO: I find it hard to believe that any DPAs in the short-term are going to provide us with specific guidance on an accreditation program.

I think what is more likely is that, as Fabricio asked, if we tried the approach as we did the proposed interim model which is is to run something up the flag pole and get a reaction, that may

call on the community to develop some accreditation schemes and run them up the flag pole if we can't get specific guidance back from the DPAs. With that, we're concluding this session and looking forward to another one later this week. Let me first thank the GAC for assisting with organizing it, our staff, our panelists, and of course our hosts here in Puerto Rico for getting the audience all fired up with the dancing and music this morning. Thank you, all.

[Applause]

[END OF TRANSCRIPTION]