STEVE DELBIANCO: Thank you. This meeting is now being recorded. We'll run from 9:00 to 12:00 today. If you don't have a copy of the agenda, we'll be sure that you receive one. Brian circulated them this morning. Along with just a dozen or so slides. It's really a discussion opportunity. It could not come at a better time. We are going to dispense with introductions of a long list of guests since the Adobe Connect basically records the names of all those who joined in Adobe.

However, this is a great opportunity for those of you who are not on Adobe to read your name out. Those of you who are dialing, for instance, and not on Adobe. We would like to have a great appreciation for those who are present but not recorded in Adobe. So, we'll start with this room here in Washington, DC. Would any of you who are not in Adobe please give your name and affiliation. We'll start on the front row here.

SUSAN ANTHONY: Good morning. Susan Anthony. United States Patent and Trademark Office.

STEVE DELBIANCO: Hit the green button to turn your mics on before you speak. Thank you.

JAMES BLADEL: Sorry. James Bladel from GoDaddy registrar. Thanks.

JUSTIN PHILIPS: Justin Philips, ICANN Wiki.

MATTHEW RUBEN: Matthew Ruben [inaudible] Global.

TRAVIS JOHNSON: Travis Johnson, IACC.

TIMOTH CHEN: Tim Chen with Domain Tools.

DEBBIE COHN: Debbie Cohn, International Trademark Association.

STEVE METALITZ: Steve Metalitz on behalf of the Coalition for Online Accountability.

LAUREEN KAPIN: Laureen Kapin, Federal Trade Commission.

UNIDENTIFIED MALE: [inaudible], FBI.

ASHLEY HEINEMAN: Ashley Heineman, NTIA.

JOHN RODRIGUEZ: John Rodriguez, US Patent Trademark Office.

BECKY BURR: Becky Burr, Neustar.

JONATHAN ZUCK: Jonathan Zuck from ALAC.

JIM PRENDERGAST: Jim Prendergast at Galway Strategy Group.

MARGIE MILAM: Margie Milam with Facebook.

FABRICIO VAYRA: Fabricio Vayra, Perkins Coie.

LORI SHULMAN: Lori Shulman, International Trademark Association.

MELINDA KERN: [Melinda Kern] [inaudible].

CHRISTINA MITROPOULOS: Christina Mitropoulos, American Apparel and Footwear Association.

SARAH DEUTSCH: Sarah Deutsch, ICANN board.

UNIDENTIFIED MALE: [inaudible] Winterfeldt IP Group.

STEVE DELBIANCO: That's great. Thank you to the room in Washington, DC. Those who were not on Adobe introduced themselves. Are there any others in Brussels or on the phone who would like to introduce yourself because you're not in Adobe?

JONATHAN COHEN: Jonathan Cohen, Intellectual Property Constituency.

UNIDENTIFIED FEMALE: Here in Brussels, [inaudible] [AT&T BC].

UNIDENTIFIED MALE: [inaudible] Patel with [inaudible].

UNIDENTIFIED FEMALE: [inaudible] as well.

UNIDENTIFIED MALE: [Carlos Garcia] from [inaudible].

UNIDENTIFIED FEMALE: [inaudible] European Commission.

UNIDENTIFIED MALE: [inaudible].

UNIDENTIFIED MALE: [inaudible] German Federal Ministry of Interior [inaudible] Berlin.

STEVE DELBIANCO: Any others? Alright, great. Thank you very much. We're going to wrap up quickly with a brief setup. Then, I'm going to turn it over to Brian Winterfeldt who will work through the agenda aspect of an overview of what we I guess have come to call the ICANN Convergence Model. Again, this is Steve DelBianco speaking, but I wanted to remind everyone about one important element of context.

The ICANN interim model is not and was never proclaimed to be an ICANN bottom-up multi-stakeholder process. It is a top-down unilateral decision by ICANN when faced with what they believed was a credible threat of legal liability for their WHOIS policy and the requirement of that WHOIS policy on contract parties in the face of the GDPR coming into effect in May.

So, ICANN does not seem to take well to critique that this process didn't use the multi-stakeholder model because that's not what it is. It's ICANN legal and executive management team doing a consultation with the community, and many of you have been part of those consultations. Some have been formal with public comment. Others have been done through meetings and seminars and webinars, like the one the BC and the IPC conducted on the 24th of January. So, we're gratified to believe that some of that consultation has affected ICANN's selection of the model. But, let's be clear. This is not the multi-stakeholder process. We'll do our best, though, to reengage the multi-stakeholder process.

But, for the time being, what ICANN is doing is being sure that it is protected. That seems to be its first and foremost goal. The second goal is to try to accommodate the concerns of the users of WHOIS as well as those who operate the system, registrars and registries.

With respect to registrars and registries, we have many of them involved in today's webinar and I'll be happy to have their specific input throughout the day, but I would summarize their top three priorities.

The first is to ensure that whatever model that they adopt, let alone what ICANN does, that they will want to avoid to the greatest extent possible the liability, including fines, of being held in violation of GDPR. And we would all do the same thing were we in the shoes of a registrar and registry. In other words, regardless of ICANN's model, if ICANN's not indemnifying contract parties, the contract parties still have to be sure that they won't be in violation.

Second, I guess as a former programmer, I can tell you that I empathize this, but the registrars and registries want to treat legal and natural persons the same and not have to make some artificially intelligent distinction between the two. I think we'll see that in the convergence model that's coming forth.

The third is this notion that it be globally applicable and not just applicable to those that are resident in the European Union zone. Again, something that would require a significant amount of artificial intelligence to determine whether somebody was subject to the GDPR or not.

So, those would be three contract party priorities and the priorities for the IPC, BC, and other users of WHOIS for the purpose of protecting consumers and thwarting cybersecurity threats and protecting the brands that serve those consumers, the priorities are always to try to maintain as close to possible to the current WHOIS in a more accurate form that we have today, in a form that allows reverse WHOIS lookups.

In other words, there's a whole [inaudible] of ways in which we use it to protect consumers and stop cybersecurity threats that we've gone over many, many times before. But, we will try today to do a gap analysis so it's clear where the missions we need to accomplish with the use of WHOIS where they are met and not met by the convergence model.

Finally, I'll just conclude by reminding everyone that the process doesn't stop here. The community itself may replace whatever this interim model is by virtue of power of developing consensus policies. In other words, PDP on the registration directory services, the RDS PDP while [stalls] today would potentially be restarted, reinvigorated, and with the full attention of developing a bottom-up community-driven process. Because if one comes forward from the RDS PDP, it replaces the interim model. There is no doubt about that. It's in ICANN's declarations and they've confirmed many times the word interim in interim model is there because it's replaced by the community should we act.

With that, I think I will turn it over to Brian Winterfeldt to walk through the second element here on the agenda, and an overview of ICANN's convergence model.

BRIAN WINTERFELDT: Thanks so much, Steve. Good morning, good afternoon, and good evening everybody. Thanks so much for joining us here today about this important discussion. We are really happy that you all were able to join us. We put this together fairly quickly just because, frankly, everything is moving very quickly in the space and we are working hard to stay up to date and keep you up to date with everything that's happening.

Right now, ICANN has put forward what I believe they're calling the convergence model. It is the latest proposal of what they're going to adopt as the interim model for compliance with GDPR while, as Steve mentioned, the community continues its work and is able to develop an alternative through the PDP, which we all know can take quite a bit of time. So, we're incredibly focused on making sure that the interim model that gets selected is adequate and really is compliant with GDPR, but not over-compliant and also really takes into account all the uses of WHOIS that's really important to protect users of the Internet and to protect users of the various platforms and businesses that use the Internet.

I wanted to walk through. The convergence model may really be new to people. It is actually not officially published and that's something that I think has confused a lot of people. Even one of our speakers was looking for the published model. So, we're talking about a model that has not been published, but ICANN has gone out and has been speaking with community leaders to walk through what the model looks like. So, we thought it was important to take a couple minutes to talk about what we're kind of looking at today.

ICANN previously put out three different models, proposals. And I guess it was sort of four because it was model one, model two that had version A and version B, and model three. But, they're saying they've looked at the different community models that were put forward. They've looked at the comments and the feedback on their models that they've put out and this is what they're starting to home in on.

I wanted to walk through briefly the elements of that model because it may be new to some people who are joining us today.

There are still many questions and concerns that we have about the convergence model that's being put forward and we are going to be talking in more detail about those, but I wanted to cover those very briefly. The first is data collection.

The convergence model will continue to mandate that registrars collect all thick registration data. Thick data includes registrant administrative and technical contact information. This is something that we support. Data sharing. The model continues to mandate that registrars provide all collected thick data to registry operator and data escrow providers. This is also something that we support. Data retention. The model currently stipulates the life of the registration plus two years. A full assessment of data retention obligations will ultimately be a matter for the next generation registration directory services PDP working group.

Because of the work involved in surveying legal requirements across the jurisdictions. We want to note that the GAC called for a five-year period beyond the life of the registration and WIPO actually suggested a seven-year period in their public comment. We think that's an area where ICANN should consider whether they want to have a longer period of time and we believe there would be legal support for that.

The scope of territoriality. Fabricio Vayra I believe recently published a blog post on this topic that I think is very helpful with [Circle ID]. This is one of the major hot button issues in the community. The model must be applied to all contracted parties and registrants within the European economic area, or the EEA. It may also be applied globally by individual registrars and registries but only subject to a controller agreement that specifies additional implementation parameters.

We are aware of potential problems with this approach with regard to over-application of the GDPR requirements for the sake of registrar expediency. So, this is something that we're going to continue to talk about and something that we will talk about later today.

Finally, this is something Steve noted also was the natural versus legal person scope. The model makes no distinction between data of natural persons and legal persons. This was also something, again, that we think is going to be hugely debated and it's something that we do have concerns about and there are obviously some implementation issues and challenges with figuring out the distinction between the two, but that's something that we will be talking about more and thinking about.

There are a number of other gaps as well, which I think we'll be exploring later today. There are public WHOIS data elements that will be included. There's some discussion about what's not included. Right now, the model includes registrant organization, registrant state, province, and registrant country. So, there are elements that are collected but will not be published that include the registrant name, street address, city, postal code, registrant e-mail, registrant phone number, and administrative technical contact information.

We believe that some of these elements may be things that could actually be included in the public data. An earlier version of the convergence model, for example, did include the city – at least that was gone over. But, when it was reviewed with members of the Intellectual Property Constituency, it was deleted. So, we're thinking that there may be some changes there that might be helpful in the work that's done in the IP and security space and to assist law enforcement as well. So, we may be looking at that and talking about what might need to be included.

STEVE DELBIANCO: I would add, Brian, that the nonpublic WHOIS fails to disclose the administrative or technical contact e-mail address. I believe the model 2b is published by ICANN, probably a month ago. Those were a part of the public WHOIS element. So, there's been movement, as you said, away from anything that ICANN had published to where what ICANN is now socializing, and socializing it with multiple groups over the period of the last two weeks. But, over time, there have been modifications and tweaks in what they've been discussing.

So, we don’t know for sure whether ICANN will announce its official convergence model today, tomorrow, or in the next few days. That’s been forecast by [Cyrus] and the members of GDD.

But, there is still an opportunity to show that if the gap analysis reveals critical elements that we need that this would be the time to make the best possible case for those critical elements to become part of the convergence model.

BRIAN WINTERFELDT: I think that’s exactly right and that’s part of why we’re here today is because the model is not published. ICANN has assured that they will not publish the model any earlier than next week. So, we still have a chance to give our feedback and to push on these areas that we’re going to be discussing today where we feel like the model could be made stronger and be better.

You’re right. There has been an evolution from what ICANN originally published and there even seems to have been evolution as we noted throughout the discussions with the community. So, I think it’s really important from a BC and IPC perspective that we really push hard on the areas that we feel are able to be improved prior to the actual publication of the model next week and really make that very clear to ICANN about not only what we would like to change with what’s there, but also what we think is missing and really needs to be addressed, and this is sort of our last window of time.

Again, we really appreciate everyone joining today very quickly and becoming part of this conversation. Our hope is to go back to ICANN at the end of today with very strong feedback for them about how they can improve the model and what's missing and how it could be put back in, and our goal is to do that with justifications and support that we have from the EU Commission, from the GAC, from WIPO and from our work within the BC and the IPC to really show what the needs are of IP owners and businesses and security folks.

So, I think that is a good, quick overview of where we're at. Do you want to go over accreditation?

STEVE DELBIANCO: It's part of the convergence model overview.

BRIAN WINTERFELDT: Yes. We're going to actually be going over that I think later today. I think just for time purposes, I want to keep us on schedule. So, that was a brief overview. We did not cover every single point, but the points that we didn't cover in the overview are actually going to be discussed in more detail through our panels later today. But, I would like to try and keep us on schedule. So, I would suggest that we go ahead and move to our first panel, which is the latest updates on EU level discussions. I'm going to be turning the presentation over to Cathrin Bauer-Bulst, Christian D'Cunha, and Paolo Grassia who have joined us today and we're very grateful and I would like to turn this presentation over to them now.

CATHRIN BAUER-BULST: Yes. Hi, Brian. Hi, Steve. Hi, everyone. This is Cathrin Bauer-Bulst from the European Commission. Thanks very much for inviting me to present the European Commission [inaudible]. I hope you can all hear me.

I have to start with a disclaimer, being a lawyer. Just like Christian from the [ETF] will also have to tell you in a minute. We are not the regulators of the GDPR, so we can provide input and expertise, but it will ultimately be up to the national DPAs to take a judgment on whether something is data protection [confined] or not.

Now, that being said, I want to take you through just a couple of the main comments, main highlights, of the comments that were submitted by the European Commission and by the European Union.

So, there was first a letter from three commissioners. Then you may have also seen the technical comments on the models, which build on one another. I think the important messages can be summarized as follows. I'm happy to enter into more details if there are specific questions.

First of all, the Union does recognize the important roles with WHOIS and the very important role it has played for a number of users, and it tries to clarify in its position that the GDPR is not a step change. In fact, it is a reiteration of a number of principles that have been around for a long time and the Union position sets out these main principles once again.

I think one key message to take away from that is that the Devil is in the details. So, the data protection rules do not per se prohibit any form of processing as such, but rather they require you to think about why you are processing that data, define clear purposes, and then to assess the proportionality of the processing in relation to these purposes and make sure you have a legal basis to do so. So, a lot of the principles actually turn on accountability, transparency, and proportionality.

Moving on from that, the key messages that are contained in the Union position are, first of all, that in line with what I just said, you need to clearly define the purposes for which you are doing data processing and you have to transparently inform the registrant about it.

There, of course, the models are a helpful step forward because they help us see a bit more of the details around what is happening there. As we also said in the Union [position], a lot more detail is required to really be able to assess whether the purposes are [inaudible] whether specifically the [inaudible] and whether the processing would be proportionate.

The Union also set out some considerations about the scope of application, which Brian and Steve already alluded to. So, not everything is personal data and the GDPR is a specific territorial scope. And I'm not quite sure with the territorial scope is now set out in the convergence model really matches the criteria of the GDPR, but I will Christian to speak to that because he's the expert.

The Union provision also states – and this is an important message – that we can pursue public interest and private contracts. Because here, we are working in a special system. We don't have a law governing how the WHOIS is run or how ICANN is run. We are operating in a [maze] of bylaws and contracts that set out obligations for the contracted parties and for ICANN, some of which are not in the [inaudible] interest of those contracted parties, nor in that of ICANN, but the benefit of public interest purpose. So, I think this recognition that such public interest can be recognized in private law frameworks is very important.

The Union has also set out where that legitimate interest, as laid out in Union law, can also apply for the benefit of actors outside the Union, which is an important thing to remember in this context.

The Union has also said that there is a clear need to improve the data quality, which clearly is not really very high at the moment and that one of the requirements under the GDPR is to ensure high data quality in relation to the purposes for which the data is processed.

The Union has also stated that there are some practical needs of law enforcement that should be taken into account, and I will just a list a couple for the sake of example, such as the access volume. There is still a possibility to have the kind of access that they require for the purposes of their investigation. And also very importantly, that there be a mechanism to enable maintaining the confidentiality of law enforcement investigations. Again, here, we come back to the details of the implementation, but those are important ones.

I also want to clarify because I heard that the Union position has been misread as not endorsing the needs for other user groups to access the WHOIS. That is not what the Union position set out to do. But, rather, again, the Union position explicitly recognizes the GAC principles of 2007 which are quite eloquent also on other user groups. Here, it is just important to again assess which user groups are given access for which purposes to which data categories and to [inaudible] proportionate.

That is really the main message that the Union position tries to pass. It is not about whether you choose a layered access system. It is just one way of addressing some data protection concerns and it can be a way of implementing that proportionality requirement. But, in and of itself, such a layered access system does not yet justify the processing of the data for the purposes of the GDPR. we will have to look carefully and specifically at the needs of each of the user groups and the [inaudible] purposes that arise on the basis of these needs.

Now, the most urgent question is: how will this work? Here, I come back to a point that Steve made earlier about the need for community participation. That's also in the Union position quite explicit. The modules are still at a very abstract level and really we can only move to a true assessment of what is compatible with data protection rules and what meets user requirements once we start specifying further. And that is both a challenge and an opportunity because of course as users of the WHOIS, as stakeholders in the WHOIS, as registrants, registrars, registries, and ICANN we can now participate in the elaboration of these models. And in that context, we welcome ICANN's efforts of reaching out to the DPAs and attempting to further flush out these models in an effort to meet the different needs, which is of course far from easy.

I just want to make it very clear also from the Union position that the question of whether data is public or non-public is not per se required by the GDPR. The GDPR does not exclude and neither does the Article 29 Working Party that certain data elements which could extend also to the registrant name and e-mail address could be made public. It just requires that there be a purpose – a legitimate purpose – and a legal basis that requires such data be made publicly available. It is to clean up any misconceptions there.

With this, I will stop in the interest of allowing some time also to the others, but I'm happy to respond to questions now or at a later stage. Thank you.

STEVE DELBIANCO: Cathrin, before we move onto the next presenter, this is Steve DelBianco with a quick question for you. You noted that ICANN's models are abstract, but for purposes of discussion today, to move things down the road, it would be helpful if while the other speakers are filling in, if you were to look at the convergence model as Brian described it earlier, give us your opinion or assessment about the degree to which that would be compliant with GDPR when we come back around to you on this panel. Thank you.

CATHRIN BAUER-BULST: Sure. Happy to. So, should I turn it over to Christian [inaudible] me?

BRIAN WINTERFELDT: Yes, Cathrin. Please go ahead and turn it over to Christian. Thank you so much.

CHRISTIAN D'CUNHA: Hello. Good morning, good afternoon. This is Christian D'Cunha. I work for the European Data Protection Supervisor. Thanks for the invitation. It's disclaimer time as well for me. I don't represent Article 29 Working Party. I work for the EDPS, which is a member of the Article 29 Working Party. We're not even the rapporteur, but the lead data protection authority on this important question within the working group. We don't have any mandate to speak on behalf of the group.

Having said all of that, it's very good to keep this conversation going. The working party is being focused talking about this for many years. I know that we've had discussions with representatives of ICANN on many occasions in recent years, and I think ICANN have been in touch with different DPAs as well for one-to-one discussions.

I think the first discussions open with the working party back in 2003, there's been [letters] in 2006, 2014. The latest one was in December 2017. We know that there is a lot of work going on at the moment.

But, having said all of that, I'm coming at this discussion rather blind because I don't know what these options are which are on the table. I got these slides just before I left late for this meeting, so I've had a chance to glance at them. Hopefully, this is the first opportunity of many to explore how they might interact with the GDPR.

The working party holds very firmly to having a [inaudible] approach on this. It's on the agenda almost every time they have a plenary meeting. The last one was a few weeks ago. So, they're very much speaking with one voice on this. I'm not aware whether or not they've seen the options themselves by different DPAs there. I don't think we have any DPS. But, we want to take care.

The position that we would take I suppose as EDPS in general terms is obviously what we're talking about here is something which goes to the constitution of the European Union. So, the right to data protection, the right to privacy. These are fundamental rights, so we take them very seriously. The Internet, as well, is an organ for the fundamental right to freedom of expression and it can help underpin democracy as well. We don't see any, in principle, conflict between data flows and protecting individuals who might be affected by the misuse of data or the unnecessary collection of data.

But, in relation to data of registered domain names, we're conscious that we haven't found a satisfactory solution yet. From next year – well, for May this year it will be clear because of the GDPR, although you could argue that it always has been clear, as Cathrin said. There is no great step change in the law through the GDPR. But, it does make it clearer than ever in the GDPR that registrars offering services to people in the EU will be subject to the rules of the EU, and therefore they could be subject to enforcement by supervisory authorities in the EU if there is no ways found to protect the data in the domain name registration systems.

Where does that leave us? You've probably seen the letter that the DPAs wrote in September. There's this other question mark over understanding what the concept is on the GDPR, on the EU law, on what personal data is. I noted your slide on the types of data that would be kept public or kept on the non-public … Be non-public and be publicly available.

The basic principle and the way that the law is evolving in the EU with case law and through the courts is that any sort of unlimited, indiscriminate disclosure of personal information is generally regarded to be disproportionate, and therefore not compatible with EU law. So, any proposal to publish, in a limited sense, individual domain name holders would raise serious concerns.

You'd need to demonstrate, as Cathrin said, that there is a legitimate purpose and a legal ground for doing it. It's two separate tests. One key thing, one key innovation, we would say in the GDPR is the notion of accountability. What this means is that everything, the whole ecosystem, the architecture, of the new regulation revolves around the notion of the controller and the controller's responsibilities. And that, I think, has been one of the most difficult things in our discussions with ICANN to really nail down.

But, you'll see from the letter that was written in December from the working party that it seemed to us that ICANN and the registries jointly determined the purposes and means of data processing for the WHOIS directories, therefore that they would be deemed to be joint controllers. That was a [supervisional] view.

If, starting from that basis, you would then need to consider what would be the legal basis for them, for publication of this information – publication being a form of data processing, which would have a big impact of the individual who is concerned by the data, and they have a different legal bases to consider. But, consent seems to be the most obvious one, but there are some very strict rules about how consent is to be interpreted. So, if it's not freely given, then it's not deemed to be consent under the GDPR. That could be a challenge.

The last couple of points. We've recommended having layered access to the data which is held in the directories from your slide, again – we've just seen them, but it looks as though it's the sort of thing that you're looking into. We don't dispute the fact that law enforcement or other authorities might need to have access to this, but the question is under what terms and to what extent and what the controls and safeguards in place are.

The last point is, the last point about the kind of enforcement regime which will come in for May this year, if ICANN were to be considered a joint controller, that would mean that they would be subject to the general data protection regulation. They would need to indicate one or more establishments in the EU. If it was outside the EU, they'd need to appoint a representative in the EU and that it would be … The one-stop-shop could be in [vote], which means that the data protection authorities would gather together and decide which authority should be in the lead if you indicate that ICANN has establishment in more than one [inaudible] state.

So, that's really all I can say at this point. I'm sorry if it's what you've heard already before. My boss is very keen for me to come here, mainly to be in listening mode, and find out how you're getting on with these difficult discussions.

BRIAN WINTERFELDT: That's great. Thank you so much for joining us. We really appreciate your perspective and we appreciate your time. That was incredibly helpful. Now I'd like to turn it over to Paolo Grassia.

PAOLO GRASSIA. Hi. Thank you very much. I will be very short. Thank you very much for inviting ETNO to contribute as part of the ISP constituency. We at the Association of Network Operators represent telecom operators – the European telecom operators – that have been data privacy directive compliant, would be GDPR compliant going forward. But, we have a keen interest of having ICANN as compliant as possible because we take the view of users, of course, of the WHOIS and the way we interact with the registers is really important for us.

I'd really like to draw on a couple of points that were raised right now from previous speaker. Indeed, I looked with a lot of interest at the letter from the Working Party 29 of the letter in December. That gives a good analysis. A good analysis is based on the current model, not from the new model. So, if you see, the big key point is what did legal grounds for processing a full publication of WHOIS data by ICANN. It seems that there's [inaudible] Working Party 29 [inaudible] is discarding most [of these] legal grounds because, as it was already said, the consent seems to not be freely given because the access of consent would result in denial of the service. Performance of [inaudible] is a legal ground that couldn't be pursued because the domain name holder is not a party of the [inaudible] and this doesn't seem bound to change under the convergence model.

At the same time, I think that the legitimate interest concept is really interested in view of your converged model you're moving towards because the reason why Working Party 29 says that legitimate interest is not acceptable under the current model is because it's not proportionate and you can't be [granted] legitimate interest for an unlimited publication of all data over the Internet.

Of course, it's not for me and not for anyone in this room to judge whether legitimate interest would be a good way to go under the convergence model, but it seems from your preliminary presentation that there is some improvement because the convergence model [wouldn't] imply [inaudible] publication of data, so you have public and non-public WHOIS data and the set of public data, as I read them, of course [inaudible] identification of the [inaudible].

As you know, as raised by thee European Commission in the letter, they point out the new definition, the new concept of personal data which is very, very broad and it involves personally identifiable information, but also information that could lead to identification of the data subject. I think there may be chances that this separation of public and non-public data under this criteria and these two different data sets may lead to a more lenient approach from the DPAs.

This is, as an observer, an opening that I see. But, of course what I wanted to stress also, a strong [inaudible] experience of our members is that prior consultation with the DPAs is of essence here.

In fact, under the GDPR, the data controller is required to run a [brief] assessment and needs to be processing – [inaudible] processing operation it wants to pursue may need [inaudible] for the data subject. The controller should involve and consult the DPA before finalizing this processing operation. But, in fact, what we assume from [interruption].

So, I think that indeed before ICANN completes this convergence model, I would just suggest—

UNIDENTIFIED FEMALE: We're not hearing you. Sorry. Can you hear us?

BRIAN WINTERFELDT: Yes, we can.

UNIDENTIFIED FEMALE: We've got the host in the room. Are you guys all here now? My apologies for that. That was the only way I could get it to stop. We should be able to carry on. I'm sorry about that. Thank you for your patience, everyone.

PAOLO GRASSIA: No problem. Things happen. I will just conclude also stressing in the DPAs letter [inaudible] before the model is finalized is of essence because I think it's something that [inaudible] complete model and complete [inaudible] processing to DPAs for approval before they have been consulted thoroughly. That's just my message.

STEVE DELBIANCO: Thank you, Paolo. Cathrin, have you had an opportunity to assess the first few pages of the slides that Brian circulated? Mainly with respect to what's described specifically in the ICANN convergence model. Give us your view on whether you believe it would be compliant with GDPR.

CATHRIN BAUER-BULST: Thank you, Steve, for putting me on the spot. I'm looking. I think whatever model [inaudible] could be in line with the GDPR. [inaudible] was saying – and I was trying also to convey – we need to look a lot further than this to determine whether it meets the GDPR's requirements, because really we can say we have a [inaudible] model, but then whether that is data protection compliant or not will depend on to whom you give access to the non-public [inaudible], which parts will be public and for which purposes on what legal basis, and how you [inaudible] a system that ensures the kind of accountability that Christian and I were referring to.

That's what I meant when I said we needed a bit more detail here, because I think there's a lot of options now for [taking it forward] and differentiated access is definitely a very good step in the right direction from the data protection perspective. I'm looking at Christian here who is not shaking his head, so I'm still on safe ground.

But, we need to look at how that will work in [inaudible] in order to be able to assess whether it meets, A, the needs of the users and, B, the requirements of the GDPR, both of which need to be met and reconciled. And the GDPR has a number of pretty solid mechanisms for this, and as soon as we start elaborating we can start exploring whether those mechanisms give us a green light. I was looking at Christian whether he wants to add anything because I'm not the only [inaudible].

CHRISTIAN D'CUNHA: Well, if you take a hold of that [inaudible], I might have more to say for thinking about it. But, I really can't say. You can't make a judgment on compliance on the basis of a few slides that have only just been seen. I appreciate … There's a lot of work obviously behind all of this, but there are a number of basic questions which have been repeatedly put by the working party. I think they would expect to see a more systematic engagement [inaudible] questions. There's not a big … The GDPR is a very important development, but things haven't really changed from the directive. The principles are still the same. There's still the need to have a legal basis and purpose limitation, a notion of who's ultimately responsible for the decisions that are being taken. Sorry I can't [inaudible] on that.

STEVE DELBIANCO: Quick question.

CHRISTIAN D'CUNHA: Yeah.

STEVE DELBIANCO: Thank you, Christian. Just a follow-up. I would wonder, though, to say nothing has changed ignores the stark reality that, come May, fines of

4% of gross global turnover can be imposed. That is certainly perceived as a step change, although from your perspective, you may not see a step change in regard to what the policy is. But, when the policy includes fines, I have to suggest that is perceived as a step change.

My question for you would be let's suppose that the model is published as ICANN suggested within the next several days and with far more specificity as to the criteria by which the non-public information could be revealed Cathrin's point.

Once that is published, can you say with the DPA – a lead DPA – prior to the formation of the data protection board, would a lead DPA be able to very quickly assess and give approval of ICANN's interim model soon enough that it can be relied upon for the programming and compliance activities that parties have to undertake?

CHRISTIAN D'CUNHA: Well, the first point you might find is an innovation in the GDPR and it's an important one. I don't want to downplay it at all. But, on the other hand, I wouldn't hold your breath before the first fine is applied because if you read the articles in question, there's some very complex criteria which needs to be satisfied before if that tall of enforcement is used collectively by the DPA.

I don't think people should be overly obsessed with fines. Fines are basically built into the system in order to create a realization that these things are very important and there is genuine harm that can take place to the individual if information about them is used in the wrong way, a disrespectful way.

On the second point, I don't know. it's a hypothetical question. I don't think the Article 29 Working Party [inaudible] Article 29 Working Party between now and May could certainly consider a model and the DPAs would be ready to work together to assess it and to give an opinion n it. I don't know how quickly they would do that. The last meeting of the working group is in April. after that, they will meet again as the European Data Protection Board.

There are 29 different authorities involved in the working party, so they'd need to work very quickly in order to get you a response and I can't guarantee that would be forthcoming before the 25th of May. But there's no harm in trying and I think they would appreciate the gesture.

You'll know that they've been a bit disappointed that there hasn't been more progress over the last 15 years. obviously now that there's three months to go before the GDPR, people are starting to have a sense of urgency.

Having said all of that, speaking on behalf of EDPS, I wouldn't expect [inaudible] to suddenly change overnight.

BRIAN WINTERFELDT: Christian, a quick follow-up question to that. We hear you that it make some additional time for feedback to be given on the model. There has been talk potentially about a forbearance in enforcement while we seek final approval and to give potentially parties time to actually implement. Is that something that you think is a possibility and you think may be considered?

CHRISTIAN D'CUNHA: Well, there's no provision in the for a kind of grace period. It's all about engagement with the DPAs and showing being productive, being sincere in your risk assessment. Those efforts get recognized. It's not the case that you can suddenly suspend your enforcement powers. It's more like trying to make sure that the best possible outcome is achieved. It's not as simple as that. Sorry. I think we need to hear some more music again.

BRIAN WINTERFELDT: Well, we're not asking you to make anything up. We do appreciate you answering the question to the best of your ability. Laureen Kapin has a question.

LAUREEN KAPIN: Thanks, Christian. Here, ba-da-bum-bum-bum-bum-bum. So, now you can answer my question which is since we know that ICANN has a major office in Brussels and the working party has the view that ICANN is a joint controller, I'm wondering if that weighs in favor or makes it more likely that the Brussels DPA might be the lead one-stop-shop for ICANN compliance issues.

CHRISTIAN D'CUNHA: Well, the letter was just a preliminary assessment that they could be joint controllers. Then it goes on to say that, at least under the GDPR, they'll need to indicate where the joint controllers are established, and if they're established in different places, then the group will decide who will take the lead.

If you were to say that ICANN, most of the big decisions are taken in Brussels, then there would be a strong case in saying the Belgian DPA will take the lead. This is all kind of speculation because there are all sorts of … There are some procedural steps that need to be taken under the GDPR to establishing the [inaudible] amongst the DPAs.

BRIAN WINTERFELDT: Great. Thank you so much. I have one quick question which could be, I guess, for Cathrin, Christian, or Paolo. We've had some discussions about the data accuracy requirements that are in the GDPR and what those mean potentially in terms of WHOIS. I'm wondering if any of you have any thoughts on that or interpretations because we know within our community, we've had some very different perspectives on what that could mean.

CATHRIN BAUR-BULST: Right. The principle of the GDPR is that personal data should be accurate and kept up-to-date, and inaccurate data should be raised or rectified without delay. And it has to be, with regard to the purposes for which they are processed. So, obviously, for a number of purposes, the data would need to be accurate. But, what that exactly would mean in terms of the obligations for the registrars and registries to verify data that has been inputted by the registrant I think is somewhat a more complicated question. I'm looking at Christian whether he has any additional input, but it's not something that … I mean, the requirement is clear, but to what extent the measures need to be taken, that would need to be further specified.

CHRISTIAN D'CUNHA: Yes. It all comes back to the controller again. They're responsible for the quality of the data and the person who's concerned by the data and the data subject. They have a right to, if they consider the quality of the data to be defective, then they can ask for it to be rectified.

BRIAN WINTERFELDT: Great. Thank you so much. We're going to ask any other questions be put into the chat and for follow-up later. We are running a bit behind schedule, so we want to move forward to our next panel. Thank you so much Cathrin, Christian, and Paolo. This was incredibly helpful and we really appreciate you sharing your thoughts with us and also answering our questions.

[ALEXANDER HEDRICK]: Brian, there is still a question from Brussels. For the record, this is Alexander [Hedrick] from the [PTO] Law Firm. As a new lawyer, for me there's something missing in this whole discussion which I haven't seen yet, or maybe I missed it so correct me if I'm wrong. As my previous speakers already iterated, the introduction of the GDPR is not a step change. It's still primary anonymization of existing laws which have been around for many years.

What I'm wondering is why are we not talking about the WHOIS policy of existing EU ccTLD registries or maybe [inaudible] ID as the main example. As it stands, it seems to me that their WHOIS policy, or

[EURID's] WHOIS policy is less strict that the convergence model shown here today.

For example, they do make a distinction between [legal] and natural persons and they publish the e-mail address and language of the registrant – the registrant who is a natural person. So, I'm not aware what steps are taken by the [inaudible] European registries to further comply with the GDPR, which has obviously stricter obligations.

But, it seems to me that this would be an important part of the discussion or should at least be discussed and I haven't heard this yet, so I don't know if there are any comments on this.

CATHRIN BAUER-BULST: If I may, this is Cathrin from the European Commission. We're in charge of the dot-eu and we have delegated this to [EURID] for implementation. I agree with you that [EURID] is exemplary in many ways because it has a very [inaudible] policy. It has a very solid anti-abuse policy. And it has some publicly available WHOIS data which [inaudible] most of the public access needs. So, they actually see a very low volume of WHOIS requests.

Also, because they keep their [inaudible] clean and I have to say [inaudible] that there's a clear link between the number of WHOIS lookups needed and the abuse [mitigation] measures that a registry takes.

So, while we think that from these perspectives, it's very useful, there would be a complication in scaling up this model which is that [EURID] currently has a practice of making you fill in the form for each WHOIS request, and if you have a larger volume of lookups, obviously needing to fill this form every time would create a certain obstacle for a number of users who need more access, and it works for [EURID] again because they don't have that many lookups. But, it's not a scalable model in terms of the way the self-certification process operates at the moment.

So, if that were to be adjusted of course, self-certification is one of the things under discussion. I'll stop here. Sorry, Steve, we're throwing you off the schedule.

BRIAN WINTERFELDT: No problem. Thank you so much, Cathrin, for answering that question. We really appreciate it [inaudible] perspective. We are going to need to move on to our next panel now. Again, I want to thank Cathrin, Christian, and Paolo for their time and for indulging all of our questions. We're going to move on from latest developments in the EU and we're going to turn over to Claudia Selli, chair of the BC to begin our … Sorry, yes. Please, Claudia, go ahead and get our discussion started on WHOIS user perspective on ICANN convergence model. Thank you so much.

CLAUDIA SELLI: Thank you very much first of all, Steve and Brian, for putting a lot of effort in organizing this webinar. As the previous one, I think it's very useful as we go towards the adoption of a final model of compliance to continue the discussion between exchange between communities and constituencies and ICANN because it helps really to clarify some questions, concerns, and also to hear the different interests at stake.

Secondly, thank you very much for giving me this opportunity to share the BC views concerning the convergence model. The BC has made clear in different [inaudible] that of course we would be in favor of model one, and we think that the convergence model [inaudible] still some missing elements.

One of the elements that we think should be considered is certainly the geographical scope application. In fact, the model of convergence would apply, as Brian also pointed before, globally regardless of whether the registrar and registry and also where the processing fails within the scope of the regulation that's [adding] some [inaudible] of course. Also, the limits or the requests of the GDPR would be felt in other regions and maybe also more critical areas and maybe where also users might need to have access to [inaudible] in a consistent way, it wouldn't be possible also in other regions globally.

I also think that this would go against the public policy and might lead to some conflicts of law in other jurisdictions.

Also, as it was pointed before, the convergence model would also apply to legal person, and as the Commission has pointed out in the letter of February, the GDPR only applies to natural persons [inaudible] really no need also to regulate the data of legal persons.

The other thing is that the model doesn't, from what I understand, distinguish between the data subjects and search party. It's currently not really clear. In fact, if the requester is the data subject, it shouldn't require to go through the same type of requirements as the third party, and in fact the data subject would be entitled to access the data and has the right to accuracy and to correct the data.

Moving to another aspect, in terms of access to non-public WHOIS data, of course it gives access to a defined set of third parties, certified under an accreditation certification program.

It's not really clear how the certification program will run and we are waiting of course for the details in order to give a judgment, or [also to have] an opinion, I would guess, that this would enable a one-time approval over a [inaudible] period. Although we would report the standardized accreditation process, we think as well that it requires a lot of work to put it in place.

So, in the interim solution, we would favor a robust self-certification process meanwhile. In fact, the robust self-certification process which is currently under model one, it would give quick access while being compliant with the GDPR requirements. In fact, as Cathrin has pointed out earlier, the Article 29 Working Party doesn't say it would allow to publish certain data if there is legitimate interest, of course, and if it's proportionate.

I wanted also to stress that for private actors, private sector companies, researchers, IP rights holders, it would be critical to maintain the access to WHOIS public data while respecting the GDPR.

In fact, the model, we would certainly support the fact that it allows the collection of thick data, but at the same time, I'm a bit concerned about the fact that it doesn't allow for publication of certain data such as mail or ID, and because it can have some consequences in the search – the way, for example, the reverse WHOIS function. In fact, the benefit of WHOIS is quite known and I think also institutions are recognizing that.

The other day, I participated to a round table on cybersecurity and commissioner [inaudible] responding to a question about how GDPR would impact some uses, some services. He precisely pointed to the benefits of WHOIS and importance of keeping it accurate, particularly for law enforcement, of course.

In fact, I wanted to highlight five, for example, uses of WHOIS, how WHOIS is beneficial to consumers and companies alike. First of all, you can identify malicious websites. A domain record is very handy in a preliminary point to figure whether a website is potentially harmful or maybe involved in cyber [threats]. And lots of factors can raise red flags. For example, if the registration, the recent data [inaudible] for a domain or a fairly close expiration date of the domain, or if the registrant comes from a high-risk country, or for example if the registrant and the company address are different in location.

So, with the reverse WHOIS, you are able in fact to also see other sites that are being registered by the same entity or by the same registrant. So, to find out also other possible [inaudible] sites.

The second use is to identify [fraudulent] entities. The third would be certainly to identify different associations for fraudulent activities, identity [inaudible] domain with DNS and credit card fraud. Fraudulent activities, of course, over the Internet can be also very dangerous because if you think about counterfeit pharma sales, it can be even deadly. Or if you think about counterfeit automotive parts that wouldn't function or counterfeit, for example, furniture. If you buy a crib for your son or daughter, for your baby, you don't want to put your baby in a counterfeit crib that can lead to injuries, for example. So, you wouldn't be able to discover whether the website would be fraudulent or not.

The last element that I wanted to bring into discussion is the interim model versus a long-term strategy. In fact, of course the community is quite worried about the final decision that ICANN will take and when because, of course, this wouldn't leave much time for registrar, registry to implement it. But, as the Commission suggested, we should have, and as Steve pointed out, a good discussion at the community level in order for all parties to be heard, all concerns to be heard, and maybe find a satisfactory solution.

And of course we can take this momentum where the model has been outlined to continue the discussion and also maybe it's a way to accelerate the PDP to where the policy framework, the compliance with the GDPR. So, we can certainly restart and continue the RDS PDP.

So, I think these are some questions that I wanted to throw on the table and I would like all of us to think about that and not to focus only on the interim model. I will stop here. Thank you.

BRIAN WINTERFELDT: Thank you so much, Claudia. I'm now going to turn the mic over to Lori Shulman, senior director of Internet policy at the International Trademark Association to discuss trademark, brand, and IP perspective.

TIMOTHY CHEN: Actually, we switched up the order on you, Brian, if that's okay. This is Timothy Chen with Domain Tools on behalf of the Business Constituency. Thank you, Claudia, for those comments. I will be very brief, and then I will be passing the mic to Lori.

First, I just want to say that we acknowledge the rights to privacy of everyone worldwide, not just European citizens and the importance of this process, the critical fundamental roles at the European DPAs, as well as ICANN [inaudible] in this process and the challenging situation that the contracted parties are in.

Our hope in all of this is to try and come to a workable solution, because for us individually, the security and stability of the Internet and the safety of individuals and employees of the businesses that we represent are our primary importance.

I'm going to touch on just to meta points and then pass the mic to Lori. I will also say that the use cases, which is one of the topics here, this documentation, the EWG – the very good EWG work – as well as in the RDS work that people can refer to for specific examples of use cases that Claudia was talking about.

The first point that I want to make is that DNS is, by its definition, an open trust-based network. The function of DNS, and of the Internet, and the continuing function of the Internet and the security and stability of the Internet for which ICANN is responsible is dependent on protecting that trust.

Another way of looking at trust, if you flip it on its head, is risk. What folks in security and brand protection are doing on a daily basis is trying to do a risk assessment, either individually, in understanding who is on the other end of a DNS transaction for which we believe they have a right to know, as well as at scale for some of the more forward-looking security use cases for the data which we can talk about another time.

So, fundamentally, it's important to protect that trust and if you look at DNS, it's really a many-to-many network. The challenge with a gating process is that the information becomes a many-to-few paradigm. In those cases, when you think about that, you think about the fact that while people think about security being done by large organizations or a couple very smart people inside these big security operation centers worldwide, it's actually done every day tens and millions of times at the edge of the network, individuals – people like you and me, our families, our employees making decisions on where they go and why they go there on the Internet. And enforcing security of that level is fundamentally almost where it's the most important and the remit of the Business Constituency extends security to individual Internet users because they are our customers. So, if they are making decisions on whether or not the website they are going to is actually the website of the business or not is just one use case.

So, we think about this. We think about the Business Constituency and the ITC, we're also thinking about Internet users worldwide by definition. So, when I think about those two things, the fact that security is done at the edge of the network and the fact that a gating process creates a many-to-few information flow, it becomes of primary importance what sits outside of that gate and what people of scale are allowed to do because I don't believe that the credentialing process is going to allow credentialing for Internet users worldwide at any scale or functionality.

Then, separately, of course, what happens inside that gate is also of primary importance. Lori will be talking about one example of that with the e-mail address. [inaudible] has talked about all of the use cases. I had a lot prepared for that. I'll skip that.

I will just say that the other point that I wanted to make is I know something about this just from the practice of the business that we've been in for 20 years. the effective establishment of that trust happens both on an individual domain basis as well as its scale. This is the concept of searchable WHOIS, which also Lori I believe is going to touch upon.

But, really, when you think about our constituents and network and cybersecurity in IP and brand protection and anti-fraud, it all is related to use cases that we're trying to represent today. Really, there are use cases for both the individual lookup and the information about a domain name that's currently captured in the WHOIS protocol as well as the ability to connect [inaudible] resources – domains, their hosting infrastructure – to that actor in order to establish context and then precipitate whatever kind of legal process, take-down, locking, remediation that you're trying to [inaudible] that you're trying to do on your network, for your users, for your employees, for your brands and IP, and your organization.

So, it is important to talk about that. I'll echo what people have said here. Driving towards this model of how that's going to happen, what's allowed behind the gate, is of primary importance. So, people in those fields can understand their capabilities, what they're going to be able to do going forward after May 25th. Thank you.

LORI SHULMAN: Hello. My name is Lori Shulman and I am the Senior Director for Internet Policy for the International Trademark Association. I want to thank Tim and Claudia for teeing up some large issues that I'd like to address in terms of the gaps in the convergence model and where we feel there is definitely more room for discussion.

There are three key areas. One is including a real e-mail address in front public-facing WHOIS. We feel that's absolutely critical. There is a letter with justification written on behalf of the Coalition for Online Accountability which is an association of content owners and they are members of the International Property Constituency. It's on ICANN's website. I was going to go through the points today, but actually in the interest of time, I'm going to ask those to reference the letter. It is on the ICANN website. Which goes into why it's important to have an actual e-mail address with a real name, something that's contactable that we can get to [inaudible] of whatever services are being offered under a domain name [publicly] for a variety of reasons and I'll just highlight a few.

One, if someone's website is under attack, the quickest way to inform them is through a real e-mail address rather than going through some sort of [inaudible] system.

Secondarily, for those of us who are very much interested in the consumer protection aspects and the applicability of WHOIS, the best way to understand who may be either intentionally or unintentionally creating confusion on the web in terms of the source of a particular good or service under a trademark or content. That source be very readily contacted because not all controversies end in court. A lot of the correspondence and the notice and the take-down and operations to get bad actors off the web is done through WHOIS.

So, the importance of keeping a real e-mail address public-facing we see isn't necessarily precluded by GDPR. This was very well explained to us by our European colleagues.

That being said, Cathrin Bauer-Bulst mentioned and we emphasize the importance of improving accuracy on the WHOIS. We don't see anything in the convergence model right now that talks about accuracy. It's going to take the opportunity to comply with GDPR to essentially close off some data sources that we're used to having and at least those that we have should be much more accurate.

We all know that the WHOIS is notoriously inaccurate, and in spite of the inaccuracies, I've read statistics that say it's 50-75%, depending whose studies you look at. There's still accurate data there, but it would be better now to have even more reliability and accountability as to who is the owner of a domain. It's really that simple.

We're also concerned about bulk inquiries. Bulk inquiries help cybersecurity experts, consumer protection advocates, brand owners, content owners to figure out patterns – important patterns – in what has becoming an exponentially growing problem with phishing, malware, and all the other little [inaudible] that one can encounter. A normal consumer going to a website they think is from some particular source. It's not from a particular source. They provide information. The information then is used for identity theft.

The quickest way to get at solving these problems, from doing the bad acts, is to get to a real e-mail address, accurate information, and then analyzing patterns through bulk access.

Fundamentally, though, this does come down to the gate in question and that has I think also been very well portrayed today, that we're talking about this convergence model at such a high level that we don't understand how access will happen, when access will happen. Will it be only limited to law enforcement? Will it only be limited to lawyers? I've heard there are some models that say let's provide access to IP attorneys. That's great. We welcome that. But, there's a broader universe of interested private parties out there. It's not just IP attorneys. It's private investigators, it's service providers, it's people who have a stake in and an interest in making sure that the Internet is a clean, safe space for consumers. And I'm going to end it right there. Thank you.

BRIAN WINTERFELDT: Great. Thank you so much. Any questions for our speakers? Steve?

STEVE METALITZ: Thank you for the presentations. I want to follow off of Lori's presentation. It also really comes back to the [inaudible] of the third parties who are not [inaudible] possible [inaudible] accreditation, such as [inaudible] being able to contact.

UNIDENTIFIED MALE: Thank you. Among the people who will not be included in any plausible accreditation scenario or consumers around the world who need access to this. But, one other aspect of that is that if these consumers no longer have access to a registrant e-mail address and cannot contact the owner of the domain name in order to determine, as a previous speaker said, whether the crib is defective or who is going to be responsible for the crib, where are they going to turn? I'm assuming they're going to turn to the contracted parties. They're going to be turning to the registrars for this information.

So, one consequence of suppressing public access to registrant e-mail, which is what appears to be in the convergence model is going to be an increased burden on registrars, either to act upon requests that they receive from consumers and from – I'll give another example, investigative journalists. Every day we see stories in the press in the United States anyway, and I'm sure in Europe, where there's a big concern about fake news in social media and so forth. Every day we see stories that clearly are based upon, or in which WHOIS data is used for the investigative journalists. And they will, again, not be – in any plausible scenario, will not be accredited.

So, all these people will be coming to the contracted parties. Are the contracted parties prepared to deal with both a higher volume and the potential liability if they do not actually provide this information to these requestors?

I just wanted to put that perspective in as well.

BRIAN WINTERFELDT: Thank you, Steve. Laureen?

LAUREEN KAPIN: Thanks. Quick question, and this may be for our DPA—

UNIDENTIFIED FEMALE: We can't hear you.

UNIDENTIFIED MALE: Brian, do you hear us?

BRIAN WINTERFELDT: We hear you. I think we're having trouble with Laureen's mic.

LAUREEN KAPIN: Okay. Can you hear me now? Yes. Okay, sorry about that.

Building on the issue of data accuracy – and this may be for our DPA folks – there was mention that the GDPR actually has obligations to correct inaccurate information and that is not clear what this means specifically for registries and registrars.

But, I'm wondering, in terms of standing, is it only … Who has the standing to raise the issue of inaccurate data? It can't just be the registrant because the registrant many times is giving the inaccurate data. So, I'm just wondering if the standings to raise this issue goes to anyone who may be harmed by the fact that the data is inaccurate or it's some other analysis.

UNIDENTIFIED MALE: Normally, it would be the person who is concerned by the data, but that's under data protection law. But, if it's a question of generally inaccurate data, then I would assume that can be raised with the authorities, the regulator. It doesn't have to be the data subject themselves. It's an interesting question. I don't think there would be any block to someone bringing the case forward.

BRIAN WINTERFELDT: Great. Thank you so much. I think that's a super helpful point, and again an issue that we're trying to work through in figuring out what the data accuracy means and who would have the ability to make an objection.

I think this is actually a good segue to our next topic. I want to thank Claudia, Lori, and Tim for providing the perspective of the user with regard to the ICANN convergence model.

One of the challenges that we see moving forward is the creation of a certification or accreditation system. One of the concerns we have with the convergence model is that we see lots of things going dark from a public-facing standpoint and we don't have a clear picture yet of how access is going to be granted and to the extent of information that the people who are granted access are going to have it in terms of both time duration and scope.

So, I wanted to actually turn things over Susan Kawaguchi and Alex Deacon to kick off our discussion on this topic.

ALEX DEACON: Thanks, Brian. Can everyone hear me okay?

BRIAN WINTERFELDT: Yes.

ALEX DEACON: Great. This is Alex Deacon. Hi, everyone. Thanks for joining us. So, [inaudible] stated that its high level goal in these discussions is to maintain to the greatest extent possible the amount of data still available in the public WHOIS system while complying with the GDPR. We agree this is an important goal, but we do understand that some registration information may no longer be publicly available and that some form of gated or tiered access to this data, leveraging the technical capabilities of a protocol like RDAP, for example, will be necessary.

I think when thinking tiered access, there's some things that need to be taken into consideration. I think, first, it must minimize burdens not only on registrars and registries, but also on third parties who have legitimate interest in seeking access to this non-public data.

Second, it must provide for expedited access, reliability and consistency, while still complying with the GDPR.

So, Susan and I have been asked to talk about how the ICANN community should go about designing and eventually implementing systems that will allow access to registration data that is no longer publicly available.

With the May 2018 date quickly approaching, I think we could all agree that we need to be thinking about a phased approach, one that allows us to be up and running at the end of May with an interim process based on self-certification that will ensure continued, yet now controlled, access to important data contained in the WHOIS system.

In parallel, we need to start on the definition of a longer term, more robust accreditation system that can take us and move us forward into the future.

So, I'm going to chat a little bit about requirements for self-certifications that we could use in the interim, and then I'll pass it on to Susan to talk about a longer-term solution, one based on formal accreditation.

In any system based on self-certification, the requestor must certify that it needs access to the data for one of the ICANN-defined purposes. For example, those purposes that have been outlined [inaudible] in ICANN's proposed interim models, which include law enforcement, cybersecurity, consumer protection, intellectual property interest and the like.

A requestor of information must also certify that it will comply with the GDPR when processing WHOIS data it receives. The IPC in one of its comments puts some details around additional requirements for self-certification. They are on the slide. I'm not going to read all of this, but I'll just go through it quickly.

When requesting access to information, we believe that self-certification regimes need to ask for the name of the requestor, need to understand that the requestor – sorry. If the requestor is an individual, the name of that person, the address of the requestor, e-mail address, phone number, and then of course the purpose of the request based on one of the five purposes set forth by the ICANN interim model.

Then, a self-certification model, this requestor would agree under penalty of perjury to several conditions. I won't read these, but you'll see them now up on slide 19. I won't read these. You can take a look at the slide and also the IPC comments.

The bottom line here is that if the requestor properly completes items one through six and affirms to items listed in seven there, then the registrar or the registry should grant immediate access to the non-public data of the requestor.

We think this self-certification process would comply with the GDPR for a number of reasons. First, it limits the use of the data by the requestor to a legitimate purpose and imposes obligations on the requestor to process and use the data in compliance with the GDPR and any other applicable laws.

So, it embraces the principles relating to the processing of personal data set forth in article 5 of the GDP, for example.

Second, because the self-certification affirms in item 7b that the requested data will potentially be used to establish, exercise, or defend a legal claim, either civil or criminal, it serves to relieve the registrar of balancing the interest of the registrant and requestor with respect to the right to object set forth in article 21 of the GDPR.

Finally, we believe it's important to ensure that we all agree up front that the self-certification process is interim and short term. And we would suggest that a date be set, an expiration date for any interim process that may be agreed to be set, for example, end of December 2018 or some other dates to give us incentives to actually come up with a more formal and final accreditation, formal accreditation, process at that date.

So, with that, I'll pass it over to Susan who will talk about the long game here and how we can address a formal accreditation process. Thank you.

SUSAN KAWAGUCHI: Thank you, Alex. We have one question. Steve DelBianco?

STEVE DELBIANCO: In the chat, I placed a question. Can you cite any examples of where a similar form of self-certification such as what you've described is being used by European registry operators today?

ALEX DEACON: Thanks, Steve. We've seen a form of self-certification being proposed in the dot-amsterdam TLD. I believe something similar is outlined for dot-eu. So, these things do exist today and we would build from those and perhaps learn from those in whatever interim self-certification process that we may come up with.

SUSAN KAWAGUCHI: We have another question in the room.

UNIDENTIFIED MALE: Hi, this is [Erongo] with the FBI. I just had a question if you saw this self-certification being applicable at the individual level or if there is a mechanism for having a whole organization in the sense that we would have an issue of each individual investigator need to go through this process just in terms of the expediency for an investigation.

ALEX DEACON: Thanks, [Erongo]. I think clearly that we want to make sure that we meet the requirements, or at least one of the requirements that I stated up front is that it needs to minimize burdens on the registries and registrars. We'll have to process these applications, but also to those who will be taking advantage or using the credentials issued in having access to the data.

So, I think there are ways that we can achieve that and having a single application, for example, for an organization I think is one way to do that.

So, I think we envision that this would work for organizations as a whole and the employees that need access to that information – the investigators, for example – but also to individuals, as the case may be.

UNIDENTIFIED FEMALE: Becky. Another question in the room.

BECKY BURR: Thanks. This is Becky Burr. I think the self-certification question begged that question of how do we get to answers that help us bridge the gap here? I think that if you talk to registries and registrars and other folks, there's a great deal of anxiety about whether a self-certification process would pass GDPR muster.

I understand, on the other hand, why it's attractive and useful from other perspectives. In some way, it would simplify. If it actually worked, it would simplify compliance and the need to create an accreditation system [and the like].

But, the question really is how do we get to some level of clarity with respect to whether it passes muster or not? Because I don't think there's a great deal of confidence that it does.

UNIDENTIFIED FEMALE: Alex, would you like to respond first to that?

ALEX DEACON: Sure. I think it's a great question, and I think in order to understand if something passes muster, we need to, as a community, come together to define what we think it should look like and then ask for input from the DPAs and others who are experts.

It seems to me that is a path forward if we were to do that, but I agree, Becky, ultimately that is the question. Will this pass muster? Given that, we'll put some thought into it, that there will be defined processes and requirements that requestors will agree to handle the data per the GDPR.

I think that leads us – and also the fact that it's interim and that we will eventually be moving on to something more permanent, which perhaps is better, if you will, in the eyes of the GDPR. I think it seems to me that it is definitely possible, but the question I think needs to be asked of those who are kind of in the data protection space to give us guidance there on how to best do that.

SUSAN KAWAGUCHI: I agree that it will be at the best a guess, but we definitely need to balance the GDPR versus consumer protection and it's not sustainable to all of a sudden have no access to those records come May 25th. So, I'm hoping that ICANN can take a stance on this and maybe the authorities in Europe will understand it's a work in progress and we can continually change the model. It's hard for registrars to implement something that's changing on a monthly basis, but hopefully we can all work together toward a model that the authorities can accept.

Then, there's always the risk involved. So, we either have a consumer protection risk or a GDPR fine risk. I have an opinion on which outweighs the other, but I'm not sure that would be agreed upon.

I will takeover here on the long-term requirements for an accreditation model. I think one of the first steps we should do after we've come up with a temporary model for self-certification is actually, as a community, agree on a framework – a document that we all sign on to, similar to what we did with the [PTSAI] in the privacy and proxy specification in the RAA. 2013 RAA, we all signed on to that. Well, registrars signed on to that. It was something we could turn to and say, "Okay, we have this responsibility. We already agreed to this and we need to make this move forward within a timeframe." December 2018 timeframe that Alex was speaking about, that's quite aggressive. Can we get there? But, we should – what we don't want to do is end up with an agreement that times out over the years and we're left with a model that doesn't really work and that the registrars have a hard time implementing.

I think one of our first paths is to develop a very short framework that everyone agrees to.

Part of the details that we need to look at is can we determine organizations within each of our communities that could help with this validation process? Is there a cybersecurity community or group that could actually step forward and say, “Yes, they are a member of our group. We have validated their membership. They are responsible.” Whatever the details are, and bless those individuals or companies to be able to be part of the accreditation and gain access to the WHOIS. It’s been mentioned maybe WIPO or INTA would work in that function for IP and brand owners. Is there a copyright group?

Each of us need to go out to our communities and really think who could stand there and validate for us. Are there other? We also, as a community, need to agree to all those legitimate and lawful purposes for disclosure. There’s been a lot of discussion on that. I’m not sure there’s complete agreement on the actual purposes and the data elements that go along with a disclosure for those purposes. So, we would need to determine the level of access.

There are a few groups out there that are already doing, that were sort of discussed in Alex’s presentation. But, [Digicert] was brought to my attention in that they provide validation of registrants for dot-bank and dot-insurance. Could we take their model and maybe work on that?

So, instead of reinventing the wheel here, I think we should all go out and look at what’s out there, and then also turn to work that we’ve already done as a community or has reviewed as a community.

I won’t go through all these data access principles, but I just pulled these from the EWG report. No surprise. I was on the EWG. This was pretty well thought-out and we’ve discussed some of these in the RDS Working Group. Maybe we can start here. I’m not saying let’s just pick this up and say this is it, but maybe instead of going back to step one and drafting [inaudible] and really discussing it forever, maybe we start with something that's existing out there, something that most of the community is aware of.

I think we've done a lot of the work. We've known this was a problem coming. We've been aware of the challenges and now we have a short timeline to come to terms and propose a model that works for all the parts of the community.

That's about all of my presentation. Any questions or concerns?

PHIL CORWIN: Phil Corwin from Verisign. For clarification, we all understand the interim model is going to be some type of self-certification and I think everyone would agree that we want the permanent model to be adopted as quickly as possible, although I agree with you that December 2018 for having it in effect is "aggressive."

You're on RDS. You're familiar. You were on EWG. I asked [inaudible] ask you and put it out in the room. Once the self-certification model is in place and we're moving within the ICANN community toward creating a permanent model, do you see that happening in terms of ICANN organization talking to the community and proposing something, or through the work of the RDS PDP, or through a CCWG because of governmental involvement?

In other words, what's going to be the institutional form for the past to the permanent model in your mind?

SUSAN KAWAGUCHI: Only my opinion. Please don't make it a PDP. I think we're all on enough PDPs. As part of the GNSO Council, we had a pretty in-depth discussion in January at our strategy meeting about making the PDPs more effective. There are other types of groups that are in the bylaws that we could use, one of which is an expert taskforce or maybe we call it a taskforce only.

So, I think, as a community, we need to explore that. Obviously, everyone needs a voice and needs to be heard. But, we don't have ten years to discuss this. We have a short deadline to figure this out and do it right. And we have the people to do it. I think the community is … Steve Metalitz, please.

STEVE METALITZ: Thank you. Susan, thank you for bringing up the EWG report. This is an incredibly important resource that we can rely on, again, not for the final answer, but for a great starting point. As I recall, at the time the EWG report was released, there wasn't discussion about sending this to the Article 29 Working Party or to DPAs and asking for their feedback on it. And one issue we were [inaudible] in the IPC we were very interested in was their reaction. Did they think this would help address the data protection issues that they were raising? Do we know if that was ever done and did any of the DPAs or the Article 29 Working Party? Maybe we can pose this to the earlier panel from the EDPS and from the Commission. Do we know if they've ever looked at this, at the EWG report? Maybe specifically this aspect of it that you've highlighted here.

I think, again, that could put us ahead of the game if they've already – they've had this report available for three or four years, and hopefully they've come to some views on it.

SUSAN KAWAGUCHI: There has been some calls for ICANN to [submit this] to the data authorities in Europe. In the [inaudible] model, which I worked on with [Fifel Shaw], that was in our opening statement was please send the EWG report over and please let's get a viewpoint on this, because there's a lot of good work in this report.

If you've noted, especially the EC technical input document, they do reference the EWG report on accuracy. From that, I would assume that some of them have seen it and read parts of it. But, no, I don't think – in the [inaudible] request there was no response from ICANN on that.

Recently, on the RDS Working Group, which you may have seen that Rod Rasmussen also suggested the same thing. Let's not reinvent the wheel. Let's look at this and get an evaluation. But, has that happened? Not as far as I know.

ASHLEY HEINEMAN: Hi, Ashley Heineman from NTIA, but also the US GAC representative. I just wanted to make you aware, if you're not already, the GAC did have a conversation with ICANN yesterday in terms of socializing their interim plan. There was this specific task to the GAC, which was basically, one, to provide a listing of all law enforcement and government users anticipated for WHOIS as well as to develop a code of conduct for all other users. GAC input asked as soon as possible.

We're not sure what all this means yet. We haven't had a chance as a GAC to come together and talk about it, but it's certainly a lot for the GAC to do and I suspect at a very minimum that we will have to talk to other users outside of government in terms of what your needs are, what your thoughts are. I just wanted to lay that down in case you weren't aware because I imagine it's going to make us either very popular or unpopular moving forward.

SUSAN KAWAGUCHI: Good to know. Thank you. And we should all work together on this.

CATHRIN BAUER-BULST: Sorry, I disconnected us earlier when I hit the wrong button instead of the mute button. But, just to respond to the question on whether the EWG report was shared with the Article 29, whether they weighed in, I believe it was not. But, on EWG there was also representative of the European Commission and [inaudible] time both [inaudible] provided input that the colleague, [Michael Neber], then conveyed to the EWG to ensure that the proposals in the report were also compliant with the then data protection directives.

So, there were some efforts done on this and I believe this is also reflected in the report, which is why we also refer to it in the Union [positions].

Also, second, what Susan was saying is there's some really excellent details in the report that are worthy of further exploration now.

SUSAN KAWAGUCHI: Thank you, Cathrin, for reminding. [Michael] actually was a great leader in the EWG and provided a lot of input. We appreciated his work.

BRIAN WINTERFELDT: Great. Thank you so much. That was a really great discussion. I want to thank Susan and Alex. I want to thank everyone for all their questions. We have in a couple minutes John Jeffreys and Akram Atallah joining us to talk a little bit more about the convergence model and to answer our questions. I propose maybe we take a two or three-minute break and give our guests a chance to arrive and then we can restart.

STEVE DELBIANCO: We'll start again in one minute. We'll be joined by Akram Atallah, John Jeffrey, and Theresa Swinehart.

Thanks, everyone. Steve DelBianco here with the BC. We're going to pick up again on our agenda. This is a discussion of ICANN's convergence model. I think everyone will want to tune in and pay attention to this since it's coming directly from ICANN's head of the global domains division, Akram Atallah. It's coming also from John Jeffrey, general council of ICANN; and Theresa Swinehart in ICANN management as well.

So, Akram and JJ, my understanding is you’re together in a place. So, we’re going to turn it over to you. We can go as much as 45 minutes, perhaps five minutes longer since I know there will be a lot of questions and we’ll watch that in Adobe. So, Akram and JJ, the floor is yours.

AKRAM ATALLAH: Hello, everyone, and thank you very much for having us on the call. There is a beeping sound. Can we get rid of that? Can you hear me?

[YVETTE]: Hi, Akram. This is Yvette. I’m working on that. My apologies.

AKRAM ATALLAH: No problem.

STEVE DELBIANCO: Akram, if you can endure the high-pitched whine in the ears, we can still understand you, so please proceed while Yvette works this out.

AKRAM ATALLAH: Okay, very good. Well, thanks again for having us here. We have a lot of staff also listening to this call. We wanted to actually take the time to answer any clarifying questions on the model that we are converging toward, and also hear from you your concerns and what transpired yesterday during the discussions with the contracted parties and if there are any outcomes from that, it would be really appreciated if we could hear that from you as well.

John, anything to add?

JOHN JEFFREY: No, not at this time.

AKRAM ATALLAH: Very good. So, we start just by giving a little bit of a story how we got here and then we will go through the model. We'll try to do it quickly so we leave enough time for Q&A.

We set out early on to build a public record of the purpose of the WHOIS so that we can have a legitimate purpose for the collection, for the [inaudible] for transfer and display for WHOIS records. We collected that from the community and we built that record. We put out three different models for the community to comment on and the three models were taking the three different extremes – one that is as close to the current WHOIS with a little bit of compliance to the GDPR, two the other side which is extreme compliance with the GDPR and going away from the model, and then a model in between the two trying to track the needs between the – staying as true as possible to the consensus policy as well as providing compliance with the GDPR.

We collected all the information from the community, all the comments, as well as other models that were suggested by the community. Then, now we're still collecting information and we're collecting into a model … Oh, great. Thank you. That was painful.

So, collecting with a model that is a model for collection of all of the input that we got and there are still now some areas of debate that we are trying to focus on. John will walk us through the model and give us the headlines. Then, we could actually go back to answer questions.

The important thing is that we've been communicating with the DPAs. We've been engaging with the European community as well as the global community to try to explain what the WHOIS is and how it works, and also why we use it and how it is in the public interest to continue to have the WHOIS being public. I think we've done a good job so far. We have communication with the DPAs coming up as well to explain to them this model that we're converging on and see where we go from there.

With that, I'll give it to John.

JOHN JEFFREY: Very good. Steve, please tell me if the right thing to do is to go through our proposed interim model at this point. I know you all have been engaged in discussions yesterday. We don't have the results of that yet and know where you've agreed, so some of these things obviously may be adjusting depending on the outcome of those discussions. Is it your preference that I just go through the proposed interim model that we were talking about before your discussions yesterday? Is there anyone still there?

AKRAM ATALLAH: Did we lose everybody?

JOHN JEFFREY: Maybe the tone went away because no one is there.

[YVETTE]: Hi, everyone. This is Yvette, the host in the room. I can hear you loud and clear. At least we lost the tone. We've got Part A going. So, let me see if we can get everybody's sound back. Part B. My apologies, guys. Working on that.

STEVE DELBIANCO: Akram and John, can you hear this?

JOHN JEFFREY: Yes, we can hear you. Thank you.

STEVE DELBIANCO: Thank you very much. John, before you proceed, Akram, while you described a process that was indeed community public, there have been over the past two weeks very narrowly focused discussions with the contract parties on your convergence model and I believe with a couple of leaders of the IPC. But, to my knowledge, no other members of the ICANN community were dialed up for a discussion, a walkthrough, of the convergence model.

So, I don't think it would be strictly accurate to say that it's been circulated to all, the convergence discussions. This was noted in the Adobe chat. I just note that to suggest that as JJ moves to a discussion of the convergence model, it will be the first time that most people on this webinar will have heard anything about it. So, JJ, what would be so helpful is to walk through, and on each point, we will take questions in Adobe. Please help us understand if you have moved from the ICANN three community models and convergence represents something different. it will help us so much to understand what information or comment or legal analysis you relied upon to tweak what we first saw in early January on the three ICANN models and the convergence models you're describing today. With that, JJ, over to you.

AKRAM ATALLAH: Hi, Steve. Just to answer your original question, yeah, it's very difficult for us to actually do this globally with everybody and still get the work done in such a short period of time. We tried to reach out to as many people as we could to bounce off some of the concepts, and let's remember that this is not a final model. This is a model that we're going to be discussing now and in the future, even after we post it, to see what the feedback is and then we're going to collect as much feedback as we get and then come up with the final. So, this is a draft model for now. With that, I'll give it to JJ.

JOHN JEFFREY: Yeah. And just to further elaborate, it's a draft model and the reason we hadn't gone to publication is because we understand it's a draft or a proposal, not a formal document and not something that we were ready to come out with without engaging further with you, with the contracted parties, with anyone that's willing to talk about it.

And we were well aware of the meeting being scheduled yesterday and had been asked by various leaders to not publish our model until that discussion occurred and there was an opportunity to adjust elements of it. But, I'm happy to go through what we had put on the table, a straw proposal, as a proposed interim convergence model that could be used for compliance and could be used as a discussion point for both these types of discussions as well as for discussions with the DPAs if they were prepared to speak to us.

We haven't spoken to the DPAs about this model, in part because they wanted to hear what the community output was and make sure that we were incorporating that into this model before we brought it to them.

I understand the tone and your frustration, but I hope that you understand we're just trying to work through a process and hope that you will help us in understanding whether this is a good approach or whether there are elements of it that still need to be improved.

So, with that, I don't know what's going to be up on the screen or if you have anything that you can put up, but for those of you who are familiar with the document that we published earlier, which was the non-paper which set out a number of different proposals and gridded them against each other so that you could see how those various elements work, if you're looking at that paper, you can follow along on that. If not, listen and please interject with any questions.

We've broken the models down for understanding the comparatives into a number of different categories. The first category being data collection processing and retention. The second being how it would be applied, applicability. The third being what would appear in the public WHOIS. And then the fourth being what would appear in non-public WHOIS. So, how would non-public WHOIS be approached?

So, I'll start with the data collection and processing and retention. What I'm going to refer to very specifically now is our straw proposal, our interim proposal, that we're hoping to put on the table to talk about.

So, looking at collection from registrant to registrar, we've looked deeply at the full set of data that is being collected now, the full set of thick data that is collected by some of the registrars for registries and we looked at various fields to determine are there individual fields that were being underutilized or that were not being utilized at all? And we identified a field that we couldn't see in the public WHOIS was being utilized. We now understand there's some different input coming back on that and that there is a purpose for its use in the anti-abuse community. So, the registry-registrant ID was a field we saw that wasn't being utilized, but we understand that now may be utilized.

We also understand there's been additional community dialogue about whether various fields are useful and important to collect. So, we're interested in input back from the community on that particular topic.

On data transfer from registrar to registry, and on data transfer to escrow agents, we see both of those being a full transfer of data that is collected. So, if the field is somehow limited by those that are underutilized or not useful, then it would be that data set. If it's the full data set, then that would be the data set that's transferred.

On data retention, as you're all aware, there's been a discussion in the community about can ICANN require retention of the data. In ECO model, for example, it had proposed eliminating ICANN data retention requirement. In the IPC model, it said life of registration plus two years.

In looking across these models and the purpose of retention and looking at that conversations that had occurred on the RAA with registrars and different DPAs relating to WHOIS information in the past, we selected as part of our straw model life of registration plus two years, noting those existing waivers of registrars that have already been preserved.

I'll move forward then to applicability. So, the question is must the model be applied globally or only to the European economic area? When we looked across the various models that had been presented from the community and read the community dialogue, there was a divergence in this approach as well – some, like the ECO model, and a handful of others suggested a global approach. And the IPC, the GAC, and other models said it would be applied only to the European economic area registrants.

We tried to take a middle approach to this looking at the difficulty of determining in many cases who would be a European registrant as opposed to a global registrant. Also, wanting to take into account the fact that there may be businesses, contracted parties, who my have unique business models and only serve non-European registrants. So, we believe that obviously the model must be applied to the EEA for European registrants, but that we would allow for a global approach for those contracted parties who believe that it was too difficult to differentiate between the two. And where there would be an election, as an example, we think this is a starting point for where it would be useful to have a controller agreement in place between the contracted parties and ICANN about how those selections could be made and how choices like applying or not applying the model would be specified.

Moving to the row registrant types affected, here there was a divergence in the models between registrations of natural and legal persons or just natural persons only. Looking across that data, we believe that the registration of natural and legal persons was useful in part because of the use of personally identifiable information sometimes in the legal persons data.

Moving on to what would be presented in the public WHOIS, continue to be presented in the public WHOIS – and we understand this is still part of what is controversial in our proposal and still in discussion. I'll just run through this quickly.

Registrant name in public WHOIS, we think that the registrant organization if it's applicable could and should be published in the public WHOIS, but perhaps not the specific registrant name if it is PII. On registrant postal address in the public WHOIS, we believe that there has to be information provided to identify the jurisdiction where the registrant is – for example, state, province, and country – but perhaps not the street, city, and postal code information which would be considered more directed PII.

On registrant e-mail in the public WHOIS, we saw a solution emerging from some of the various models, the [inaudible] for online accountability model and the ECO model both had a suggestion of creating anonymized e-mail or a web form to contact the registrant. So, we proposed that as a possible solution. We were asking the [inaudible] yesterday's meeting to consider whether that was a useful approach.

On registrant phone and fax and admin and tech contact names, we were saying that not be put into the public WHOIS. On admin and tech contact postal addresses, we were also saying it would not be part of the public WHOIS. On admin tech contact e-mail addresses, we believe that this could also be approached through the anonymized e-mail or web form as opposed to publishing the exact identifying information. On admin tech contact phone in public WHOIS, we believe that could be left out of the public WHOIS. And on the registrar's opportunity to provide opt-in for publication of additional data to the registrant, we believe that's an important element as well as we looked across those fields.

Now, going back through just what's going to be presented in the public WHOIS, an important element of thinking about this is that that is the information that will be publicly displayed, but not just the information that would be available if an accredited party were to obtain access to what is not public. So, these information fields would all be collected still, but they would not be presented in the public WHOIS. It would only be available to those who had some form of approval to gain access to what is behind the firewall or in the non-public WHOIS.

STEVE DELBIANCO: John, before you jump to the non-public—

JOHN JEFFREY: I'm almost finished. It might be useful to just let me go through the last couple of fields and then we could go to questions if that's okay, Steve.

STEVE DELBIANCO: The distinction about what made the cut between public and non-public could enjoy ten minutes of Q&A, and then the non-public information and the access methods could deserve another segment. So, perhaps withhold the non-public and certification discussion and allow to take a few questions if you would on what made the cut between public and non-public.

JOHN JEFFREY: Yeah. If you don't mind, though, let me explain the last part because I think it grounds why we're looking at this the way that we were looking at it in the model.

So, we think self-certification access presents an issue. If we're allowing the choice to go to every registrar and registry about whether they self-certify. If there's some other method of self-certification, it could be considered. But, we think also the creation of the anonymized e-mail address and the web form to be able to contact the registrants and to be able to contact the tech and admin contacts presented an opportunity to provide information directly to those parties, perhaps even instantaneously, the same way you would in e-mailing them.

Then, the last part on accreditation program for access to non-public WHOIS, we think this is a really important part of considering this. Without this part, this would certainly change the approach we have to the rest of the model. We think that it’s very important that there be an accreditation program and then that be done in consultation with the GAC, that we allow for individual countries to provide the GAC a list of authorized law enforcement authorities that would have access, and that the GAC could work with us and the community to develop a code of conduct for non law enforcement agencies to abide by for access to the non-public WHOIS data, and that there could be an opportunity for a centralized accreditation point which would allow registrars and registries to know very quickly whether or not parties that are accredited – for example, many of the parties in the room that have legitimate reasons to want access non-public WHOIS information. If they are accredited, they would have instantaneous access to that non-public WHOIS database.

With that, I’ll pause and we can take any questions.

STEVE DELBIANCO: JJ, thank you. We’ll have a 10-minute question segment on what made the cut and what didn’t and then move on the accreditation certification process for the non-public.

JJ, you noted – and I understand now why you wanted to proceed with the conclusion of your presentation, because you believe that with the addition of an anonymized relay address that the four elements that would be in the public WHOIS would be sufficient, you believe, for most purposes. And just to repeat, it was the registrant’s organization, the registrant’s state and province, and the registrant’s country, plus an anonymized e-mail address that could be used to relay I believe to the registrant. Do I have that right?

JOHN JEFFREY: That’s correct. Well, relay, or you might know more technically than I would. As the lawyer, maybe I should give it to Akram. But, as I understand it, if the approach were anonymized e-mail, I think there’s other potential proposals that are coming up – for example, hashtagged information or information that might allow you to connect different registrants or admin and tech contacts across data fields, or across registration types.

But, if I go back to anonymizing, the concept would be that you’d get a … The same way you might look at … I can’t think of a service now that’s doing it, but there’s a couple of services. We had referenced eBay might be one, Craigslist might be another, where instead of displaying the actual e-mail address, it’s to provide you with a clear e-mail address that is unique to the individual registrant or admin or tech contact, and that if you put that e-mail address in your browser, it would be relayed I believe through the server directly to that party in a matter of less than a second.

That’s the idea, that it would be without showing you the exact address, you could get the e-mail directly to the registrant admin contact or tech contact.

I don’t pretend to have this as a full answer. This is one of the things that we’ve been saying to everyone we talk to. If you have a better way of approaching this, a different approach to this, we're very interested in it and we don't represent that this is the end-all.

STEVE DELBIANCO: Thank you for acknowledging a need which was identified in our gap analysis, the need for correlated or reverse WHOIS lookups. And I think you just articulated that you've acknowledged that need in the sense that this anonymized e-mail contact would be globally unique to each registrant and that would at least create the opportunity for a reverse WHOIS lookup to identify other registrations held by that same registrant, even though that registrants PII isn't displayed in the public WHOIS. Is that your appreciation of the goal?

JOHN JEFFREY: I want to be [inaudible]. This is not my acknowledgement of the need or a decision by me. This is my reference to what we had heard in some of the initial discussions in an understanding that that's the request. So, I'm not an authority or have the authority to change the position. I think what we're asking you to do is provide us with that information that justifies that, and hopefully in your discussions yesterday, that was part of the discussion.

STEVE DELBIANCO: Thank you. Yes. The acknowledgement that the community has requested it is important, but the notion of concepts of having it be a globally unique anonymized information at least holds the potential for satisfying some more of the needs that are there.

JJ, we're going to take a queue on questions for the next several minutes on the public versus non-public cut.

Steve Metalitz, you're in the DC room. You have the mic.

STEVE METALITZ: Yes. You have several questions in the Adobe about this as well. You may not see that. But, on the registrant e-mail, JJ you said you have not reviewed this convergence model with the DPAs and I'm sure you know that most of the feedback you received from the community, at least numerically, stressed the importance of preserving the public access to registrant e-mail that exists today.

You've often said also that ICANN's goal was to maintain as much as possible of the existing WHOIS system while achieving compliance with the GDPR.

Is it safe to assume that you have concluded that including registrant e-mail in the public WHOIS, which so many people rely upon today, have you concluded that that would violate the GDPR? And if so, since you have not reviewed this with the Article 29 Working Party, what is your basis for that conclusion?

JOHN JEFFREY: No. In fact, as you're probably aware, because I think we received an e-mail from you shortly after the discussion when we spoke with the IPC community leaders, there was a suggestion that there might be additional information to show us that it would be consistent with the GDPR to publish that and we asked for additional information to be provided to us. We've heard differing legal opinions on that point and are very interested in additional information.

So, there's no conclusion. As I said at the beginning, what we were trying to look at is across all these data fields, knowing that we would get some things wrong and that this needed to be adjusted. We wanted to put this out as the proposed interim model as a discussion point, so that you could provide this sort of input that would allow us to make sure that we had the community input in before we got to a point where we were publishing it and before we got to the point where we were discussing it with DPAs.

We are concerned, though, that there is a belief that we're going to present a model to the DPAs and we're going to get their blessing and we don't believe that that's the case. We believe we'll have to have a strong set of [inaudible] supporting each of the positions that we take across the model.

One of the things that we're creating right now is what we're calling the cookbook, which is literally looking at each of these issues and going into detail about that to provide the justifications for the various positions that will be taken in that model.

So, no conclusion yet. We're listening. Please provide us with the additional information that you were referring to that you say tells us that it's not illegal to publish that information. That's the kind of information we need in order to put a field into the cookbook.

STEVE DELBIANCO: Thank you, JJ. We next have Brian Winterfeldt and then Laureen. Brian?

BRIAN WINTERFELDT: Thank you again for joining us. Brian Winterfeldt, IPC President. I believe you might have referenced this earlier, but since we're going through which data elements are going to be public versus non-public, I wanted to remind everyone that the IPC had put forward that the registrant city is something that could and we believe should be included in the public portion. And I believe also zip code is something else that may be able to be included at least in part and we'll definitely follow up with you with more feedback on that, but I wanted to put that forward.

STEVE DELBIANCO: Thank you, Brian. Laureen Kapin?

LAUREEN KAPIN: Hi, JJ and Akram. I had the benefit yesterday of also hearing your discussion, participating with the GAC. I actually wanted to follow-up on one of the issues that was raised during yesterday's call. My concern here is that the convergence model appears to go beyond what the GDPR itself requires. It does that in terms of the territoriality and the distinction between natural and legal entities, I.e. the GDPR protects personal information and that's what a lot of its protections are aimed at. But, the convergence model prevents even information relating to legal entities from being disclosed.

We had pressed a little bit on that issue, and Akram, you had I think responded to the question of why aren't you making the distinction in the convergence model in terms of the publication of information relating to legal entities.

For example, an e-mail belonging to a legal entity. I think your response, and please jump in if I've gotten it wrong, was that practically speaking, logistically speaking, it's difficult to distinguish from looking at the WHOIS data fields between a legal entity and a natural entity.

My question is, with that long build-up, couldn't there be a practical way to actually just have a registrant identify by checking a box "I'm a natural box" or checking the other box "I'm a legal person." And separate and apart from the fact that maybe some people will lie about that, wouldn't that be a very easy, simple way to actually resolve that issue and then not have a model that essentially over-complies with the GDPR and instead provides more useful information so that the community that relies on such information to perform many of its public safety functions?

STEVE DELBIANCO: Go ahead, JJ.

AKRAM ATALLAH: This is Akram. Thank you for the question. This is what we're trying to do is we're trying to collect all the information that we can get on this model and try to balance everything we hear. Again, I don't think the idea is for looking at the e-mail address, but the idea is something automated that would actually work because otherwise the WHOIS will not work if everybody has to eyeball every request and every record.

The other concern that we have is how do you deal with the 150 or 160 million records that are already there? So, there are a lot of issues and we're trying to make the implementation feasible as quickly as possible of whatever model we go through.

I appreciate your concerns about not separating the natural from the legal and we will take that into consideration and we'll look at it.

JOHN JEFFREY: And I think, just to reiterate the earlier point that we made when Steve's question came up, there's still – we are still very interested in … You referenced a specific number of things that you believe make the use and publication of that information public and providing us with background support for that, precisely referencing how that would be compliant with GDPR would be very useful to us as we're building the cookbook and considering that.

STEVE DELBIANCO: Thank you, JJ. We're going to cut the queue with the two questions that were raised earlier on the question of what's in the public WHOIS versus private, and then move on to questions that are specifically targeted to the accreditation certification. So, Marilyn, I will ask you to ask your question briefly. Then, Alexander, ask your question. Then, we'll turn to JJ for his answers. Thank you.

We cannot hear you, Marilyn. Alright, let's skip Marilyn and go to Alexander, please.

CATHRIN BAUER-BULST: Sorry, this is Cathrin. I'm abusing Alexander's presence in the chatroom to raise my hand. Hi, Akram and JJ. Thank you so much for joining. This is Cathrin from the European Commission. I just wanted to build on what Steve Metalitz was saying earlier about the rationale for including or not including registrant name and e-mail address in the publicly available WHOIS.

I would suggest that, with all due respect, that in the cookbook, you performed a step that is missing here which is to check what purposes you would be doing this for.

It's very difficult on the basis of just general use cases or the need for need [inaudible] in some part of the community to assess whether this could be publicly available or not.

I think there are a ton of use cases that have already been collected, a lot of evidence in the context of the Expert Working Group report, of the present-day RDS PDP, and also use cases collected this summer as part of this task force that ICANN ran for a brief moment that could allow you to identify the purposes and then see whether on that basis you can identify a legal basis in the GDPR for the public availability.

That's what is sort of missing here and that would be the missing element that also, as a DPA, the first thing I would ask you. Why or why not would you [inaudible]? So, just a suggestion here. Not really expecting an answer. And we're, of course, happy again to support you in this endeavor.

JOHN JEFFREY: Thank you very much for the question or statement. I think there's some interesting elements to what you're saying, so I do want to reply to it. You're in a much more unique position than we are in this in that you're affiliated with the law, the people who are setting the law and the people who will enforce the law. We're struggling with the existence of that law and trying to figure out how to make sure that we in our industry sector are compliant with it.

So, obviously the work that we've done starting last summer and coming through the fall and collecting information about how the different fields are used by different elements of the community, the work that's been done in setting forth the various legal opinions – the external legal opinions – and talking about what we believe is … We took external advice that in some cases we weren't even 100% connected to and consistent with, and then we heard other legal advice from other people on those same elements that you're talking about – about what is legal and what is not.

So, the cookbook is intended to be the culmination of that, to look at how we can justify the positions that we're choosing to take in that compliance model and to be able to defend ICANN's position as well as the community's position and the contracted parties position in publishing or not publishing that information while still trying to maintain the value and purposes of the historical WHOIS that outdates ICANN.

So, anything that you could do to formalize an official position based on what you're saying to say that if you know that answers to the questions, if you have access to people who know the answers to the question and can provide us guidance that would help us, and you could put that in writing to us as a position from your organization, that would be very valuable to us and it would be something that would stop our guessing and speculating and help us understand how to move forward with a compliance model that's actually useful and valuable to our community and to ICANN.

STEVE DELBIANCO: Earlier on the call, we pressed Cathrin and Christian from DPA staff on that very question, and their fair comeback to us was that we would need to present things that are specific in order to even have any expectation of a specific response from DPAs.

Cathrin, a question, follow-up for you is if in fact we dusted off a long list of legitimate use cases for the registrant name and e-mail address to be public, would that be sufficient to have it become public or is there a concern that there might be counter use cases? Use cases where someone does things with that registrant name and e-mail that do not serve a purpose or go against public purposes?

In other words, what is your analysis? Is it the overwhelming quantity of legitimate use cases or is the presence of any illegitimate use going to be defeating what we're after?

CATHRIN BAUER-BULST: Right. I guess that's the million-dollar question. Again, I want to clarify once more because I think JJ and Akram were not around. The Commission as such is not the regulator. Of course, we're happy to facilitate conversations with the regulators, the national DPAs, and we've done so and I understand ICANN is engaging with them.

That being said, I think, Steve, the use cases are a really good place to start because what we would need to do is we then have to distill legitimate purposes from these use cases and then see whether in view of the un-legitimized uses of the WHOIS for things such as spamming and other abuse, whether the public display is proportionate or not, and if there are other means that would achieve the same aim while excluding the un-legitimate use cases.

So, for example, if you have a self-certification mechanism that allows also your normal user or somebody who'd not accredited by some organization to occasionally have access to the WHOIS, then that could be another way of achieving that proportionality while preserving the usefulness.

I come back to my earlier statement that the Devil lies in the details. The best thing would be to set up a number of different options and then to see what really would be most useful for the community and also most proportionate from the GDPR perspective.

There's [inaudible] and both directions are an excellent starting point.

BRIAN WINTERFELDT: Thanks so much, Cathrin.

JOHN JEFFREY: Could I interject with a comment or a question?

BRIAN WINTERFELDT: Of course. Please go ahead.

JOHN JEFFREY: One, Cathrin what you just said is exactly the sort of information that would benefit us to have in writing that would be useful. So, thank you for making the statement. Then, just a question back for Steve. You mentioned there was DPA staff in the room and that you were questioning them earlier. Could you clarify who that is and what their relationship is to the DPA?

STEVE DELBIANCO: Thank you, JJ. We were fortunate to have Christian D'Cunha who was on the phone. He is a staff to a DPA who is part of the Article 29 Working Group.

CATHRIN BAUER-BULST: JJ, we did put that in writing on page three of the Commission comments on the technical model, which was submitted on February 7th. We're of course happy to elaborate on those anytime that would be useful. Thank you.

BRIAN WINTERFELDT: Please go ahead, Cathrin.

CATHRIN BAUER-BULST: [inaudible] just reminded me it might be good to tell you that Christian has left so he can no longer react. He had to go to another appointment.

BRIAN WINTERFELDT: Thank you so much. I think we're going to shift the focus.

JOHN JEFFREY: [inaudible]. My understanding is he's not DPA staff. Can someone check that fact?

BRIAN WINTERFELDT: He's EDPS staff.

JOHN JEFFREY: Okay, thank you.

BRIAN WINTERFELDT: You're welcome. We're going to shift our conversation now from the data that is included and not included. Judging from what's in the convergence model right now, there is very little that is included that will be public-facing, which really brings us to the question of gated access and what model we're going to be looking at for credentialing or accreditation, if the reality is potentially that very little to almost no information is going to be available publicly.

My first question is what is your vision for once someone is credentialed or is granted access? What level of access do you anticipate they would have and what duration of time would you envision that being for?

JOHN JEFFREY: We've only considered two tiers. So, it would be either you're accessing the public WHOIS or you're able to access it with the accreditation, the full set of data.

BRIAN WINTERFELDT: That's super helpful, and that does line up with our prior conversations. I wanted to outline that we've had conversations with the contracted parties where they put a very different vision forward, where they envisioned incredibly limited access, potentially having to do additional verifications upon every single query to the database and having your queries be potentially limited domain by domain. So, that is a bit of a disconnect that we wanted to point out.

Obviously, again very little is going to be public, what the certification or credentialing process looks like and the kind of access that's granted becomes paramount in order for us to function and do our jobs to protect consumers and protect IP assets and for law enforcement and security folks to do their job. I wanted to just put that forward.

JOHN JEFFREY: I want to confirm we've had no discussions that I'm aware of outside of the two tiers.

STEVE DELBIANCO: We are going to take a brief queue because we are running up against the end of the hour. We'll take a brief queue on the questions only pertaining to the gated access, please. So, I see Marilyn Cade and Lori Shulman. Each ask the question and then JJ will reply. Marilyn we do not hear you. We'll move on to Lori Shulman.

LORI SHULMAN: Hello. Am I being heard?

STEVE DELBIANCO: Yes.

LORI SHULMAN: Okay, I'm speeding it up. JJ, thank you and Akram. I just have a question about wording that's confusing me. I see in paragraph two it says "otherwise an accreditation program is necessary to facilitate access to non-public data" and then in paragraph four I see "ICANN is also exploring other accreditation mechanisms for non law enforcement access."

So, I'm kind of trying to figure out, has ICANN committed to providing accreditation mechanisms for non law enforcement access, if that's the case, that you're committed in exploring what will work? I think that's different than just saying exploring, because that doesn't, to me, sound like a commitment.

STEVE DELBIANCO: Go ahead, JJ.

JOHN JEFFREY: [inaudible] and that we don't know what document you're referring. So, you said in paragraph two and paragraph four.

LORI SHULMAN: Yeah. I'm sorry. I'm looking at the overview of ICANN convergence model and on one side it says category. Do you have that? Take a look at this slide, because I do think whatever wording … Seriously. I think the wording is important to understand if ICANN will act commit to an accreditation process.

BRIAN WINTERFELDT: Yes. I think one of the challenges is because the model we're speaking about has not been officially published. Lori is looking at the slide that we put together that summarized the model. Obviously, I think [inaudible] wording.

JOHN JEFFREY: Yeah. Thank you. So, if I understand the question, let me just restate it. Are we committed to an accreditation model or process? Is that the question or is there a different question?

LORI SHULMAN: Yes, that's exactly the question.

JOHN JEFFREY: Yeah. As I said, when we went to that last section in explaining what our model is, we think that accreditation model is critical to the approach that we're taking in our model. Without that, that means that there would be a significant part of the WHOIS that would not be accessible to parties that we understand have an important value in obtaining that information.

STEVE DELBIANCO: Thank you, JJ. The last two questions are Fabricio Vayra and James Bladel. They will each ask a question in the room and then you can reply. Fabricio?

FABRICIO VAYRA: Thank you. Hey, JJ, it's Fabricio from Perkins Coie. I have a quick question about credentialing and accreditation generally. Do you envision that anyone who is credentialed or goes through an accreditation process would then have to go through additional layers, registrar or registry, individually?

Another way to put it, do you envision that the credentialing process allows for registries and registrars to then add their own layers of different terms and conditions, different checkboxes, different basically gating.

JOHN JEFFREY: So, we're trying to stay as close to the community's viewpoints and the value of the WHOIS as possible. So, we understand there's going to be a policy process that will follow from this. We apply what we were given in terms of what the WHOIS policy – small "p" if you were – is. We tried through the use of our approach to this model and through the whole thing to stay as close that as possible, recognizing that there's now a law that is impacting our ability to maintain the former WHOIS, the current WHOIS, and all of its parts.

So, that's the answer I think in part. Then, if I understood your question, you were going beyond that.

AKRAM ATALLAH: I think what Fabricio was asking is will there be a different [inaudible] that the registrars and registries can do in the WHOIS [inaudible] model.

JOHN JEFFREY: So, the question we had before. Is there contemplation of a registry or registrar level of approval beyond the accreditation? And we had not heard that as a proposal from the community. You're introducing that topic to us for the first time. I understand that's from your discussions yesterday.

We've only talked about two layers and our belief is if there's an accreditation program coming into this discussion, our belief is if there's an accreditation program, that would provide you with all access to what isn't published. So, the full set of data fields. And that would be something that you could readily do. With that accreditation, you would be able to access that non-public WHOIS data. That's the approach we've taken all through and we've had no other discussion about that up until this point.

FABRICIO VAYRA: Great. Thank you, JJ.

STEVE DELBIANCO: Thank you. James Bladel?

JAMES BLADEL: Thanks, JJ. Not a question for JJ and Akram, but I just want to back up to something that Brian asked or stated at the beginning of this section. Part of our discussions yesterday, I think we've been – as contracted parties, we're fairly consistent that we don't know how we would operationalize a check of credentials for every single domain name lookup. We don't want that approach. That's cumbersome and clumsy. We'd like to find something in between that and the all-you-can-eat approach to private, gated WHOIS data.

So, I think somewhere in between whether it's per account or some credentials that are valid for a certain period of time and then expire. All of those I think are potentially up for discussion. But, the checking of the credentials for each lookup, I think we agree is unworkable.

BRIAN WINTERFELDT: Great, James. Thank you so much. It's super helpful clarification. I still think it's helpful for JJ and Akram to hear because it's still a little bit different I think than what they're envisioning. I think that's helpful for them to be aware of that.

I wanted to maybe ask or point out a couple of big issues because I think we're almost out of time. One of the issues I know is that in our talks with contracted parties, we know that a lot of them are already coding. We know a lot of them are going to be doing their own analysis of the ICANN model when it rolls out.

What is ICANN going to do if they roll out their interim model and it's not actually adopted by the registries and registrars, or at least many of them decide to adopt their own models?

JOHN JEFFREY: Sorry, we missed part of your question. Do you mind restating it? Sorry, Brian.

BRIAN WINTERFELDT: No, no problem. In our discussions with contracted parties over the past several weeks, we've learned that they have a lot of technical challenges in terms of actually implementing changes to their platforms, which we can all understand and that in many cases things typically require months and months of preplanning and coding in order to actually implement. So, many of them are actually coding as we speak their first launch of what their stab at being compliant is going to be. Obviously, we're still talking about what a model is going to look like, and for good reason. We're still having community discussions. I think we all agree we wish we were having these discussions a year ago, but here we are.

My question is if ICANN rolls out an interim model and registries and registrars decide, because of their own legal advice they're receiving internally or issues specific to their company that they're not going to comply with that model, what is ICANN's approach going to be to that?

JOHN JEFFREY: So, we're going to need help here. Our goal is to not have registrars or registries go black, meaning hide the information that's in WHOIS on the date that it goes into effect. So, we're seeking to provide a model that is approachable, that is capable of being rolled out. And if the model that we have to go to is a model that can't be rolled out, then we will be asking for help from the DPAs and from others to allow that model to roll out in a timeline that would let that happen in a feasible way and seeking some element of having that not be forced into a compliance mechanism where we would have penalties come into ICANN or to the contracted parties.

Now, this is the great problem as we're coming into the final stages of this and it's going to require the community to come together on what the model is and then jointly to be approaching the authorities to ask for forbearance if that's required or for the community to come together on solution that are actually workable and capable of being implemented. I think this is our collective problem as we head into these final months.

BRIAN WINTERFELDT: Great. Thank you so much. Since we are out of time, I did just want to drop in a couple issues that we would love to continue talking with you about and that we plan, hopefully, following up with you in writing.

One of them is bulk WHOIS access and what the future of that looks like and how important that is for a lot of the work that's done for security and stability on the Internet.

Also, data accuracy is an area that we would love to explore more. There are requirements in the EU that data actually be accurate, so our question is how that actually applies to the DNS and registries and registrars. That's something we'll be looking forward to talking to you more about and hopefully providing feedback and input from our perspective as well.

AKRAM ATALLAH: Thank you, Brian, and thank you all for giving us the opportunity to address your questions and we look forward to continue our communication and discussions, and hopefully we can close on this as soon as possible so we can address all the concerns that were outlined here.

UNIDENTIFIED MALE: And just one question. Was there a contemplator approach to providing this where there was convergence yesterday among your groups, and how can we look to seeing that and what's the next steps from your side in terms of providing us with information?

BRIAN WINTERFELDT: Everyone is not even aware there was a very small group that came together – volunteers. It was something that was organized and led by the IPC. We invited a few key other participants from the BC to participate as well, and then we had some folks from the contracted party house. The idea was to get together to talk about convergence model and look for areas of agreement, common ground, hopefully come up with some solutions.

Our goal from that is to hopefully come to you with a communication that will confirm for you where there's areas of agreement and hopefully push some areas forward.

We are going to work I think on some kind of written communication to you and hopefully get that to you fairly quickly.

In addition, I think the IPC and BC plan on following up today's event with a written communication to you that outlined our analysis more deeply on the gap-filling efforts that we think need to be done on the convergence model both in terms of changes we think seem to be elements that are present as well as holes that we think need to be filled for areas that are not contemplated in the model that's been reviewed with us.

So, our hope is to get lots of feedback to you in the next day or so.

STEVE DELBIANCO: You and Akram, when we conclude this session, I'll write to the Business Constituency members about takeaways. I took two major takeaways from your presentation. The first is that the publication of the interim model is not really the interim model. It's a draft that will be published, that will be then further used to solicit input from community members as well as authorities in Europe. That is a little different than what we had expected, but I'm happy to go with that.

The second is that you talk about it as convergence, but to converge, one tries to find common ground among parties with different views. I think you've acknowledged that perhaps there's a subset of decisions that will represent convergence. But, many of the decisions will not be a convergence at all. It will be some sort of a middle ground – I think is the word JJ used. A middle ground between divergent points of view. And that middle ground doesn't represent convergence as much as it does a forced compromise between irreconcilable positions.

So, it will be vital to do what Brian said and for us to provide the kind of evidence that we need to help steer where that points arrives, but as well to recognize that you should identify where you think you found convergence since that'll be the easy stuff, and the harder stuff is where you note a wide divergence and have instead decided to place a compromise or middle ground solution out there for discussion next week.

If you have any reaction to that, please do before we thank the helpers for this session and conclude.

JOHN JEFFREY: Thank you, Steve, for the last comment and thank you for the opportunity to talk to all of you. There's a couple of important points.

One, we'd prefer that there was a community policy that was adopted and that there's no question. We don't have that, unfortunately, so we're now faced with compliance with a law and trying to guide contracted parties through our agreements in some manner to a place where as a controller, as a co-controller, at least of the information, we're put in a position where ICANN is potentially at risk for the decisions that we have to make out of this.

So, I completely agree there are going to be points where we're picking between difficult positions at the end of this, and hopefully we're doing that based on the best input that all of you are providing and an understanding of the position that we're faced with by a law we didn't create and we're still having some ambiguity around in trying to understand.

So, thank you for your patience and we appreciate all of the information that you're providing and the hard questions because I think this is how we get to a point where we're … I hadn't used the [inaudible] model, but I kind of like it because what we're trying to do is really get to a point where the community has given all the input and we're picking the best possible solution for all of us. Thanks.

BRIAN WINTERFELDT: Great. Well, thank you so much. I really want to thank Akram and JJ and Theresa for joining us today and for giving us so much time. I want to thank all of our speakers for joining us today. I want to thank ICANN staff, including Yvette who did a fantastic job supporting us around the globe. I believe we had at one point over 170 participants online alone in addition to the folks in person, in Brussels, and DC.

I want to thank ICANN for supplying us the office in Brussels. Again, this is just a continuation and we want the dialogue to continue going. Please continue to give Steve or I or anyone in the IPC or BC feedback on next steps and any ideas you have so we can keep the conversation and dialogue going.

Thank you, everyone. I wish you a good rest of your day.

[END OF TRANSCRIPTION]