MONTREAL – EPDP Phase 2
Monday, November 4, 2019 – 10:30 to 12:00 EDT
ICANN66 | Montréal, Canada

KEITH DRAZEK: Good morning, everyone.

Good morning, everyone. If I could ask everybody to please take your seats so we can begin in two minutes.

Thank you.

Good morning, everyone. Are we ready technically to begin?

Okay. The recording is started. Webcast is ready.

So good morning, all. My name is Keith Drazek. I am the current chair of the GNSO. And I'm very happy to be here with you this morning as your moderator for this session. I'd like to take an opportunity to briefly introduce the panelists for this session. Janis Karklins, who is the current chair of the EPDP Team.

Rafik Dammak is the GNSO Council's liaison.

And Elena Plexida, ICANN org, who has been involved with ICANN's engagement with the European Commission and the European Data Protection Board.

So I'm very happy to be here with you this morning. I'd like to welcome you all to the first plenary session of ICANN66, which will be an update and community engagement on the expedited policy development

process, or EPDP, on gTLD registration data and its phase 2 work in developing policy recommendations around a standardized system for access and disclosure to nonpublic registration data or SSAD. You'll hear quite a few acronyms today. SSAD is the standardized system for access and disclosure to nonpublic registration delta.

I'm going to provide a little bit of context as to how we got here. This EPDP, expedited policy development process, was first chartered by the GNSO, Generic Names Supporting Organization, in July of 2018, following the ICANN board's adoption of a temporary specification on gTLD registration data that enabled contracted parties to comply with existing ICANN contractual requirements and policies while also complying with the European Union's general data protection regulation or GDPR.

In its phase 1 work, the EPDP Team conducted a one-year policy development process to confirm whether or not the temporary specification passed by the board should become a consensus policy.

Following a year of very intensive work, the GNSO Council adopted the phase 1 report during its special council meeting on March 4th, 2019, and at the same time, initiated the commencement of phase 2.

The scope for EPDP phase 2 includes, one, discussion of a system for standardized access and disclosure, the SSAD; two, issues noted in the annex to the original temporary specification that were titled "Important Issues for Further Community Action"; and, three, issues deferred from the phase 1 report, questions including versus legal versus natural persons, redaction of city field, et cetera.

The EPDP Team is currently working to develop the building blocks for the SSAD, standardized system for access and disclosure, that are expected to form the foundation of its initial report, which is expected to be finalized in the next month or two.

With that context, I'd like to kick off this plenary session, which will begin with an update from the EPDP Team chair, Janis Karklins. We will then have a Q&A session following the update and discussion of next steps for the EPDP Team.

Before I hand it to Janis, I'd like to acknowledge the incredible dedication of the EPDP members and the groups you represent. And the ICANN staff supporting this significant and challenging effort, both in phase 1 and the current work of phase 2. You are all a testament to our multistakeholder model of bottom-up consensus policy development, and I thank you in advance for your continued efforts and commitment in this work.

And with that, Janis, I'd like to hand it over to you. Thank you.

JANIS KARKLINS: Yes. Thank you, Keith.

And good morning. It is nice to be back in an ICANN meeting on the stage after, what, nine years this happens. And so, really, that's the -- a very good way to come back.

So let me walk you through a presentation that we have prepared for you explaining where we are standing now with our activities.

So, first of all, for those who are not following closely at the second phase, so we are basically tasked to do three things:

One is to develop a system of standardized access and disclosure to nonpublic registration data, which we call priority 1 issues.

Then, we need to deal with the without standing issues from phase 1, such as legal versus natural persons, redaction of city fields and so on. Then we need to deal with issues not within the annex (indiscernible), the specification for (indiscernible) registration data.

So how we started? We started with developing use cases and going through discussing those use cases in order to build up a better understanding how the SSAD could be developed and how it could function.

So after building up this common understanding of different elements that need to be discussed and factored in, we went to developing building blocks. We agreed that we should build the system as a house, if you wish, using different building blocks. That those different building blocks ultimately would turn into policy recommendations once we will get there.

And then we will put those building blocks in certain order and will issue the initial report, which, in -- according to very optimistic scenario, we are planning to issue in early December this year, allowing the community to provide the good -- or allowing community to have a good reading material for Christmas.

So in problem, we would continue working on priority 2 issues, in other words, leftovers from the first phase, because, of course, the priorities given to SSAD and the bandwidth of the team is limited.

So we also tried to visualize our work how the system would be. And since ICANN lately is in food titles, we thought that it would be appropriate also to go in the same direction, and we visualized SSAD as a hamburger, where you have the demand side, the request of disclosure; then you have supply side, where the data, the private data, sits in; and then you have this middle part, the burger patty, where the magic of disclosure decision is made.

So what is important on this slide is the list of building blocks that you can see on the right-hand side of the slide. They are: criteria and content of requests, purposes of request, user groups, acceptable use policy, retention and destruction of data, accreditation, response requirements, query policy, receipt and acknowledgment, terms of use, financial sustainability, automation, auditing, logging, rights of data subject, and policy principles.

So as you see, there are a wealth of titles. Each of them -- some are bigger; some are -- Of these sections, some are bigger, some are smaller. And currently, we are working on all of them.

So at this moment, I would like maybe to outline a few very fundamental decisions that we have already agreed as a team and building our work on these understandings.

So first and foremost, the objective of SSAD is to provide predictable, transparent, and accountable mechanism for access and disclosure of nonpublic registration data.

Second important understanding is that SSAD must only accept requests for access or disclosure from accredited organizations or individuals. However, accreditation requirements must accommodate any intended user of the system, including an individual or organization who makes a single request.

We also have a full understanding that the automation of SSAD may not be possible in full and that SSAD should be automated as much as it is technically feasible and legally permissible. And where automation is not feasible or possible, then the team would recommend that a baseline is simply standardized.

And, finally, the very important understanding is that accreditation does not mean unlimited automatic disclosure of nonpublic -- nonpublic data. Each request will be treated and considered based on its own method.

So we have already met about 30 times through online meetings. We had also a face-to-face meeting in Los Angeles recently. And during this session, we have sessions -- four sessions where we are discussing further our -- our system.

So if you are interested, the resources -- the current state of all documentation is available on the Web site, as indicated here.

Keith, I would give back the floor to you.

KEITH DRAZEK: Okay. Thank you very much, Janis. And just to remind everybody, we will have a Q&A session following a couple more bits of presentation and update. So we're certainly looking for your input, any questions that you may have. And we will have a series of four or five questions for you to consider when we get to the Q&A session.

So with that, Elena, if I could hand it over to you.

ELENA PLEXIDA: Thank you very much, Keith. Good morning, everyone. And Janis is absolutely right, there is a lot of food in this session. You might have heard of the project team called the Strawberries. We're not responsible for our name, but we make great fun with it.

The Strawberry project was set up with Goran with a very specific task: to draft the paper that would outline a unified access model and bring it forward with the data protection authorities, seeking feedback.

That would, in turn, hopefully help inform the EPDP Team's work as the team is considering its policy options for SSAD.

Seeking this feedback, this guidance from the DPAs is in line with the goal given to Goran by the board to continue to work toward obtaining legal guidance from the DPAs as to whether a UAM is permissible and compliant with GDPR. It is also in line -- We have received several communications addressed to the board and to the org, or to the org, calling for a uniform access mechanism for registration data.

So the paper titled exploring a unified access model for gTLD registration data, was sent to the European Data Protection Board on October 28th. We had the invaluable support of the European Commission, who provided advice to us and helped us formulate the questions included in the paper in the best possible way to solicit as concrete and as many full feedback as possible.

Let me be abundantly clear here: The model the UAM outlined in the paper is a hypothetical one. And as the paper itself notes, assumptions made are for discussion purposes only, and the EPDP Team will make its own policy recommendations.

The paper emphasizes that the structure of the model, if any, will depend on the EPDP Team's recommendations, and only that.

Now, the model outlined in the paper proposes an approach for unified access based on the technical model proposed by the TSG. This proposed UAM would provide the centralized system for access to nonpublic registration data, creating hopefully a transparent and predictable system, both for data subjects whose data might be handled by the UAM and for the (indiscernible), of course.

The model proposes that ICANN org takes on the responsibility associated with a central gateway through which requests for access to nonpublic registration data would be accepted and processed. A requestor would authenticate their identity with an identity provider and the legitimate purpose with an authorization provider. Then the request goes to the central gateway that would approve or deny. If approved, the central gateway asks the relevant gTLD registry or

registrar to provide the registration data requested. It filtered it, the central gateway, and returns the appropriate data subject to the requestor.

In other words, and simple words, in this hypothetical model, it will be the centralized system, not the individual contracted parties that decide whether or not to disclose data and discloses it.

The paper aimed to test the theory that such a system would, indeed, consolidate responsibility related to the processing activity of disclosure in that system so as to be able to have a unified approach.

Therefore, the questions that are included in the paper are about whether the model can ensure that the responsibilities are clearly allocated and defined, and in effect, that the centralized system is responsible under the GDPR for disclosure, and whether at the same time this model would ensure a higher level for protection for data subjects.

Really, in essence, the heart of the questions is about responsibility and the controller (indiscernible) relationship in connection with the joint and several provisions of the GDPR.

Now, what we can expect, we expect hearing the back from the European Data Protection Board. As I said earlier, the paper was forwarded on October 25. In order for the data protection Board to consider the paper during a plenary session, it needs to have the paper well in advance. That said, the November plenary, which is taking place next week, is of course out of the question.

We hope that the December plenary could be possible, and we of course also hope that the Data Protection Board will consider the paper.

As I am concluding I would like to extend our sincere gratitude to the European Commission for its help with this exercise. It's invaluable. And the Strawberry Team is not actively working on anything anymore other than follow-up with the paper, and as Goran reiterated many times, we remain the EPDP team's availability to channel any questions or issues that we might consider need to be channeled to the DPAs as it sees fit or if it sees fit.

Thank you very much.

KEITH DRAZEK: Okay. Thank you very much, Elana. And next on our agenda here, we have an update on expected next steps and timelines. I'll hand it back to Janis. Thank you.

JANIS KARKLINS: Thank you. Thank you very much, Keith.

We started our activities in May, and so for the moment, we're reaching the point when the initial draft report will be put together based on developed building blocks and discussed by the team. I mentioned in the previous intervention that in the best case, the initial report would be published in early December, which then would allow a community to provide input by sometime mid-January. And the team is scheduled

to meet in face-to-face meeting at the end of January. So in that scenario, we would examine all inputs received during the comment period and would start working on final report.

So if we will not be able to produce an initial report in early December, then most likely scenario is that initial report will be published after face to face meeting in end of -- end of January. So -- but that automatically would mean that the final report would not be published before June meeting of ICANN. And that would -- we would not meet the requirement that has been formulated to the team by many parts of community that we need to proceed expeditiously to the development of this standardized system and implement that system as soon as feasible.

So you see the chart which outlines this first scenario, optimistic scenario, which would aim at produce the final report sometime in May.

The question about priority 2 issues. So there are a little bit dependencies that are out of, let's say, scope or control of EPDP team. Some studies have been recommended by the recommendations of the first phase. These studies now are in the phase of implementation. And once we go -- receive that additional material, we'll be able to factor those results in our -- in our decision-making process.

So again, most plausible scenario is that there will be parallel -- sorry, initial report on priority 2 issues at one point. When that will be, for the moment, I cannot say. We would do utmost to produce it more or less in parallel, but as I mentioned, the bandwidth of the team is limited, and also we start feeling certain fatigue. That is accumulated fatigue,

also, from the first phase since many team members continued working on the team also from the phase -- Phase 1.

So this -- this is kind of a maybe not overly definite timeline, but the team does utmost. And I, from my side, also want to use this opportunity and put on the public record my profound gratitude to team members as well as to ICANN staff which is supporting us in activities, because that is an enormous effort that we're trying to make.

So, yes.

KEITH DRAZEK: Thank you very much, Janis, and thanks to everybody.

So the next session will be an interactive Q&A. We're going to put some questions up on the screen. So I will read these questions, and then give you a few minutes to consider them, and then I'll make just some brief remarks, again, about some of the context around one of the things that Janis noted regarding sort of the urgency or the need to work expeditiously here.

But first the questions that we're seeking input around. And these were questions developed by the EPDP team and working with staff to try to generate discussion, to receive input on some key questions that will help them continue to do and to finalize their work.

So the first question: Are there any building blocks that the EPDP team has not considered yet that it should?

Are there any concerns about the preliminary agreements that the EPDP team has reached to date?

Is there anything else the EPDP team should consider with third-party identity providers who would verify the identity of certain categories of users?

What financial considerations should the EPDP take into account for the development and maintains of the System for Standardized Access and Disclosure?

And any other input that will assist the EPDP team in reaching consensus on the policy recommendations?

So while you consider those five questions, and what we will have now is an open mic. People, if you're willing, come to the microphone, ask questions, provide input. We have approximately an hour for this next engagement session. But I'd just like to note that as the GNSO Council was chartering the EPDP team, both for Phase 1 and Phase 2, there was a recognition that users of data, registration data, that had previously been publicly available and accessible, because of the temporary specification and because of the GDPR, were unable and are still unable to access the data in the way that they had, and that requests and access to that data today requires a request to be reviewed and acted upon by registries and registrars, the contracted parties.

And so as the GNSO Council chartered this group, there was a recognition that these third parties, their activities and their interests, were being impacted, and negatively impacted because they no longer

had access to the data that had, for years and years, been publicly available.

So essentially the work of this EPDP, both in Phase 1 and Phase 2, has been and continues to be to try to develop a system that will provide maximum access under the law, within the law, and also allow contracted parties, registries and registrars, to meet their contractual obligations, again, without crossing the line when it comes to regulation and law.

And so that's essentially what the group is working on. The council, in chartering, recognized that there was an urgency and the need, as Janis said, to act expeditiously. And that's one of the reasons the timelines that you've seen around this particular PDP, which is an expedited PDP, have been so demanding. And again, I want to reiterate our appreciation and thanks for everybody that's contributed to this, both from community, the members, and ICANN staff that's supporting it.

So with that, we'll move to the Q&A session. So if anybody would like to provide input, ask any questions, feel free to come of the microphone. I understand we'll also have remote participation available, so if somebody who is not in the room would like to ask a question, feel free to do so, and I will be notified.

So let's open it up. Q&A.

Who wants to go first?

Please.

Thank you. Brave soul.

UNKNOWN SPEAKER: Okay. I'm (saying name) from Tunisia. I would like to congratulate all the team of the EPDP team for all the effort they provided. And I have a question about the following graph provided who provide an overview of the proposed unified model. When looking to this flow or process or graphic, we see a data a lot of centralized system or gateway that are going to manage or give the access to a lot of the data used by CTID. Who would manage the centralized system or gateway?

Thank you.

KEITH DRAZEK: So thank you very much for the question. And just to summarize, I think it was as we talk about a centralized system or a standardized system of access and disclosure, I believe your question was who would operate it; correct? In other words, who would be responsible for -- I think both at the policy level but also the operational level. Did I capture that correctly?

UNKNOWN SPEAKER: The question?

You think that the operator are the -- could manage the centralized option?

KEITH DRAZEK: Yeah, thank you for the question. So I think one of the questions that's before the EPDP team today is a question of the roles and the responsibilities of the various parties. I think that extends to questions of controller, processor, joint controller, as well as the questions around who will actually operate these different components. And so I might hand that to Janis, you know, in terms of where the EPDP team is in that conversation at this point. But I think the answer to your question directly is it's not yet determined.

JANIS KARKLINS: Yeah, Keith, you answered the question. It's not yet determined. So it will be clear once we will establish agreement on the methodology, how the most important part of the system, the decision to disclose, where this decision will be made and by whom.

So I can -- I can maybe repeat what I -- what we concluded during the Saturday's session, that seems to me that the team is converging to understanding that there might be -- might be one central gateway where requests would come in.

So that is probably the only sort of element of this final architecture that I can -- I can say we are leaning towards. So then the question is where the determination would be done. And here you have, in reality, two options, and probably some variations within those options. And the one option would be that the determination is done by one centralized entity at the gateway, or the decision on disclosure is done at each registrar/registry level, and that means there would be then 2,000-plus points of decision-making. So -- But where it is, we have not reached

yet any conclusion, and certainly the advice provided by the European Data Protection Board would inform our own reflection in that respect.

KEITH DRAZEK: Thank you, Janis. And thanks for the question.

Next in line.

UNKNOWN SPEAKER: Hello. My name is (saying name). I'm from Germany, a RALO. I'm speaking on behalf of myself. I was involved in the data protection laws in Germany. I believe to understand that there is a fundamental misunderstanding here regarding the GDPR. You are saying we have to conform the law. That's wrong. It's wrong in the sense that there is no central worldwide law. We have a distributed system of lawful entities, distributed modified during the time so you can't conform every law in the world. So you have simply exact this fact.

So, from this point, I think the only thing you can do in ICANN is to reveal the data you have, you are required to have, that's contractual data. So if you're asking a server for who is responsible for anything, the server has to respond, "I don't know, but I have a contract to a party who knows more than I."

WHOIS iana.org is operating this way. If you ask anything IANA is responsible to the server you get a response saying, "Oh, I am not responsible for. Please ask the WHOIS server of party." This way it is

called thin WHOIS or ultra thin WHOIS if you extend it up to the registrars.

This way you can manage the access through different lawful areas. You can guide a query through different lawful expectations, and you allow the registrars and registries to fulfill their local law without breaching it because they have a contract with ICANN saying, oh, we're collecting all the data worldwide in the central database and we are responsible for everything.

Next point, by making such a contract saying we are collecting the data, in the term of GDPR you are responsible for the data. You are responsible for the reasons why they are collected, how they are operated, how they are stored, how they are accessed, and you are responsible for every bit of data in this database simply by making the proposal how to do this.

The person or the company saying, "We want to do this in this way" is responsible by the law. But you are not obligated to do so.

ICANN is for policy. ICANN is not for operating. So operating such things is far outside of the remit of ICANN. And by breaching this, you are making a lot, a lot of unmanageable lawful implications. You are responsible to fulfill policy -- police laws in various countries because they are not allowed to access data from another country. They can bypass all these international league of nations by simply asking ICANN, "You have the data. Please give it to me." And you have a lot of lobby organizations like (indiscernible) -- organizations say, "Oh, we like to have bulk access."

And the point which is never read by me, I am not reading all the documents but I think it's missed, by doing so, by introducing a thick WHOIS, you transfer the responsibility for the correctness and the collection of data from the registrars and registries to ICANN, lawfully. You are the person who is saying we want to have this data. You are collecting them for us. So you are not responsible anymore by law, the GDPR. Consider this.

KEITH DRAZEK: Thank you very much for the intervention. And I certainly take on board your earlier comments that not all laws and regulations worldwide are the same or could be conformed. I think what we are faced with here today, and have been for the last 18 months or so, actually many more years than that, but the EPDP has been focused on trying to address the fact that existing registry and registrar contracts in the gTLD space essentially became in conflict with the GDPR and with the associated fines within the GDPR construct. And there are provisions in ICANN's bylaws related to the security, stability, and resiliency of the Internet that actually are fairly explicit when it comes to registration data. And those obligations or those requirements have flowed down into registry and registrar agreements. And so we are in a situation where, through this process, we're trying to ensure that the obligations that exist and that the contracts can be updated accordingly to not be in violation of GDPR, but I fully recognize that GDPR is not the only regulation today, and it will not be the only regulation or law in the future.

And so at some point, what we're designing and building here today will need to be available. And I think that's a concern that the community is aware of. I take that on board. And thank you for your other comments. I don't know if anybody else would like to respond or we can move on to the next question.

Okay. Next question. Thank you.

UNKNOWN SPEAKER: Hello. I'm (saying name) from Bangladesh.

I read the interim solution model in May (indiscernible) published.

On behalf of the community, it is really hard to find the interim solution data flow. (indiscernible) stakeholder (indiscernible). For example, as to the (indiscernible).

My comments or position is, if you make in the infographic presentation a blog tag of the data flow in interim compliance model or an upcoming NIST model, which will be updated in upcoming day. So it should be infographic, so we know how the data flow from controller to controller, (indiscernible) provider to (indiscernible) provider, and registry/registrar.

So then the end user community can learn better, understand better. Everything is written in this format, but if you present in the infographic way, how the data will flow, then it will be helpful for the community to understand better what's going on and their understanding of the current position.

Thank you.

KEITH DRAZEK: Thanks very much for that comment. And I think to the extent that the community and this EPDP Team are working on developing the system, I think you're absolutely right that an illustration of the data flow and the roles and the responsibilities of each party, I think, is absolutely critical. So I thank you for your comment. I think you're right, it would help both inform the community about what's being discussed, but it would also help define precisely those roles and responsibilities that are still a subject of discussion.

We look forward to taking that on for perhaps the next one of these sessions.

Next, James.

JAMES BLADEL: Thanks. Hi. James Bladel, a member of the EPDP Team.

But a question specifically for the Strawberry effort. And my question or my concern, based on some of the previous speakers is, are we being, in your opinion, overly specific in attempting to tailor this SSAD system to comply with GDPR when we're seeing other privacy laws arise, including in other population centers, you know, India, Canada, and even California, where ICANN is based, presuming that they have some role as the owner/operator of this hypothetical model, do you believe that feedback from the European authorities will be sufficiently generic

that it can apply to all of those other laws? Or will SSAD have to be smart enough to match jurisdictions of data subjects and requestors? Or are we going to need multiple SSADs that are able to handle any discrepancies in the data protection frameworks?

And I don't know the answer to this question. I just want to know if we're even ready to tackle that yet.

Thanks.

KEITH DRAZEK: Thanks very much, James. I think that's a really, really important question. And whether that can be answered today or not is certainly something I think we need to look into and keep on our radar scopes.

But, Elena, I'd like to offer you the opportunity to respond.

ELENA PLEXIDA: Indeed, as Keith said, it can't be answered today as such, but there may be some key points.

It is in itself a huge challenge to create a system that has to globally operate in so many different jurisdictions.

Just to tell you that, internally, in ICANN org, we are monitoring all privacy regulations that are going on around the globe. We are very lucky -- put it that way -- to the extent that GDPR is sort of setting a standard and it is being followed by other regions in the world. And, indeed, I know that (indiscernible) of the European Commission, for

example, is making a fantastic job, giving know-how to other regions with respect to how GDPR is applied or how it can be applied there.

The real problem would be the moments we might have and legislation that directly opposes GDPR, particularly with WHOIS registration data.

KEITH DRAZEK: Okay. Thank you.

Next in line, James.

JAMES GANNON: Hi. James Gannon.

And two quick points. I want to lend support to the concept of a distributed model. Because I do agree that from a high-level policy decision, talking about GDPR as a basis is, in principle, good. But as somebody who's worked a lot in international organization building privacy programs, the principles are the same, but the operationalization of those principles is often different in different jurisdictions. And we are going to see more of that, particularly if you look at CCPA, which is coming along very soon. You know, that is the same principles, but very different implementation. And trying to build a single, global system that matches that diverse landscape of privacy law, which is only going to get more diverse, is a risky way to go down.

Second point, I just maybe wanted to talk a little bit about the future, and talking to implementation. And I think the concept of utilizing a central authority that looks at identity providers is a good concept in

some ways. But I don't and I haven't heard discussion about who those identity providers are going to be. And I think that's potentially a large hurdle that we haven't really thought through yet, particularly coming from the cybersecurity realm. You know, there is no centralized identity authority to say, yes, this person is a valid cybersecurity researcher; no, this person is not. That doesn't exist in certain areas of industry that would have potentially legitimate access to nonpublic WHOIS data.

But we haven't actually talked about what the implementation of this would look like. That's a big risk for the ICANN org to take, because I think, easily, you can look at two or three years' implementation for the SSAD. And that's a large risk to carry for a number of years.

Has that been thought through yet, you know, how the implementation (inaudible)?

KEITH DRAZEK: Thank you, James.

I think at this stage, the EPDP Team and the community are primarily focused on developing the policies. Implementation is, of course, always in the back of our mind. And I think in order to develop appropriate policies, you need to have a good sense as to what the structure is that you're trying to design against. And, of course, that will factor into and impact the implementation work.

But I think we're still a long way from getting into the details of implementation, that we're still at the stage fundamentally trying to

come up with a model and to develop policies against that model that would be compliant, in this instance, with GDPR.

Janis, would you like to add anything to that?

JANIS KARKLINS: As you said, Keith, the implementation is always in the back of the mind of all team members, and we're discussing different policy options.

So we started by analyzing real-life cases in order to understand how the SSAD may function. And now, when we're talking, like, for instance, yesterday, we were talking about query policy. And the discussion evolved on how that would work in real terms. So -- and based on that conversation, we revisit the initial draft of that initial proposal. And today, we'll be looking further at how that policy recommendation would -- whether that would be acceptable, which was redrafted based on our conversation how that system could work in practical terms.

So this is how the team works. And so I can encourage everyone who wants to follow our conversation to do so remotely. This is always possible.

KEITH DRAZEK: Okay. Thank you, Janis.

I have Kathy next in line. I'd like to check, do we have any remote participation, anybody in queue?

Very good. Kathy, over to you, and then to John.

KATHY KLEIMAN: Thanks, Keith. Kathy Kleiman.

American University Washington College of Law.

I have a question about automation. According to one of your slides, the SSAD must be automated where both technically feasible and legally permissible.

And I wanted to ask about the tension this seems to create with article 22 of the GDPR, which says, "The data subject shall have the right not to be subject to a decision based solely on automated processing, which produces legal effects concerning him." And this could produce significant legal effects.

So I'm wondering what some of the discussions of the EPDP in phase 2 have been regarding the question of access to the data subject's data, and then how to evaluate safeguarding the data subject's rights and freedoms and legitimate interests, which are also part of article 22 of the GDPR.

Thanks.

KEITH DRAZEK: Okay. Thanks very much, Kathy. And I know that that is one of the questions. And I'll hand it to Janis for the actual discussions that are taking place within the EPDP Team. But I know that's one of the topics, this question of automation, to the extent to which things can be automated or could be automated, you know, does that extend to

actual -- you know, the decision-making process or is it something shy of that? But I think the language that you cited in article 29, if I'm not mistaken, is, you know, "to the extent permissible by law" or something to that effect. And so that is definitely an ongoing topic of conversation. But it's also maybe not the direct subject of discussion today, because they -- I'm going to defer to Janis. I'm not sure that they've gotten to that in significant detail yet.

Janis, over to you.

JANIS KARKLINS: Actually, we have. In Los Angeles face-to-face meeting, we had a presentation how big registrar today does this balancing test and what steps need to be -- or the particular registrar is doing in order to -- coming to the decision whether data should be disclosed or not.

So based on that conversation, another team member proposed how that process could look like in SSAD. And that is something that the team will be discussing once we get there. So that is discussed. And so also thinking about automation, probably after -- after a certain period of time, we will be seeing certain patterns. And then decision may be made whether, following those patterns, something -- some more automation could be offered if that is legally permissible.

So there always will be this tension or balancing what is permissible and what is not, and what is feasible and what is not.

And so that is as far as I can say. But the clear understanding is that there will be, certainly, many cases where human intervention will be

needed. And that will be in tension with the scalability of the system. And how that will work, probably system will get smarter after certain time of operations, I would suggest.

KEITH DRAZEK: Okay. So thank you, Janis. And I'm happy to be corrected on that point. So thank you.

Kathy, did you have a follow-up?

KATHY KLEIMAN: Just because of the tremendous human rights implications of the issue, where disclosure of the location of a data subject to a requestor who may be in a jurisdiction which almost by definition makes that disclosure dangerous is just an issue that no automated system is going to pick up, but humans may under the circumstances that we would know and different kinds of current events and other issues.

Thanks.

JANIS KARKLINS: Yeah, this particular issue we discussed maybe a few days ago specifically on those special cases, to protect data subjects based on these exceptional circumstances.

So, again, there is no easy solution for that.

But imagine in the case of distributed model, you would have two thousand -- I don't know -- five hundred places where such a

determination could be made when the request is filed. And most likely, each registrar/registry, if there would be distributed model, would not have at hand either human rights lawyer or data protection expert who could put those things kind of together. And, most likely, that would be a technical guy. And myself, I have been witnessing in the U.N. discussions where communication experts are starting to talk about human rights. So they are in the weeds all the time.

So we really need to factor those different aspects in the policy recommendations. And certainly this is not trivial.

KEITH DRAZEK: Okay. Thank you, Janis. Thank you, Kathy.

And, John, I'll get to you just momentarily.

Just like to remind everybody, we have 35 minutes in this session. This is exactly the type of engagement and input that we were looking for. So, please, if you have questions or comments or any input, please come to the microphone. There's one on each side of the room. And we really do encourage your participation here today.

So, John, over to you.

JOHN LAPRISE: John Laprise, ALAC.

So I'd like to probe Elena a little bit further on a comment she made previously, which is, you know, the nightmare is that we have another

jurisdiction that comes out with rules that are oppositional to GDPR in some fashion.

Now, we're expending a lot of resources, both human and monetary, to develop policy to comply with GDPR. Are we facing the potential of another EPDP in short order if such a jurisdictional conflict comes up? And this goes to some of ICANN's long-term strategic planning initiatives in terms of looking at external risk.

So I'd like to hear from the team what they've been thinking about this potential contingency.

Thank you.

KEITH DRAZEK: Okay. Thank you, John.

And so I'll just open that up.

Elena, if you'd like to respond, or Janis.

This is -- obviously, this question of the potential conflict between what we're designing against now, which is GDPR compliance, and what may come in terms of come into conflict later in terms of other laws and regulations in just different jurisdictions. And I think as somebody noted, even in California with CCPA, there could be some variation.

So I just will open that up in terms of, you know, has the team discussed or considered sort of the need for that variability?

Thank you.

ELENA PLEXIDA: So I think I would answer this question with some of my maybe personal thoughts, if I may.

This would be a risk that might materialize if, and only if, there is no trust in the multistakeholder model, but it will come up with a good solution. And that, I believe, is not the case here.

JANIS KARKLINS: Yeah. At the beginning of our work, we had a discussion, and certainly there is a very good understanding that some new laws could come into force in other countries and that we should -- thinking about the policy, we should think beyond GDPR and make SSAD -- or design SSAD in a way that, in the case of appearance of new data protection laws somewhere else, the SSAD could be modified or application of SSAD could be modified on -- at operational level.

But I must admit that we have not looked at the scenario when another data protection law would contradict GDPR. So I don't recall.

And I am looking to my team members in front of me. Their body language suggests that, no, we have not looked at that scenario.

From other side, I'm not sure whether that is very likely that one data -- personal data protection law would completely contradict another data protection law.

So as a result, I think they will be, anyway, in -- going in the same direction. They may be different -- provide different level of protection.

But whether they would really contradict. If you can give an example that would stimulate our own thinking and understanding. So thank you for rushing to the microphone.

JOHN LAPRISE: So if I can give a hypothetical example, there are certainly jurisdictions where the lawful authorities may want radical transparency. They want everything open to everyone all the time. So they can keep track of things and people. And that would completely go -- oppose sort of like the protections embodied in GDPR. Without getting too specific.

JANIS KARKLINS: But that, in my view, again, I'm not a lawyer but just common sense suggestions that those jurisdictions basically are where we were. There were no any limitations or restrictions in use of WHOIS in terms of accessibility to private data prior to GDPR, and GDPR then introduce the data protection of European data subjects. So -- And probably those were -- data protection laws were not enforced so they would still expect to access data but not those that are fall under GDPR.

We can take it offline --

JOHN LAPRISE: Yeah.

JANIS KARKLINS: -- and discuss it further.

KEITH DRAZEK: Thank you, Janis. And thank you, John, for the question.

So I'll take a moment. We have a few people in queue. We're coming over here next but I'd lake to make a comment first. Just in terms of the EPDP team, its charter, the expectations of the group.

So clearly what we have are, in the ICANN space and referenced in the bylaws and the registry and registrar agreements, is a global policy, something that's intended to be a global policy for gTLDs. And what we're faced with here is a situation where different jurisdictions are coming up with different regulations that are impacting our ability to come up with a globally consistent policy. And that's the challenge before us.

This EPDP team was chartered to first deal with the temporary specification in GDPR and is now tasked with coming up with a standardized system for access and disclosure in the context of GDPR. And if and when it appears that we need -- we, as the GNSO Council, the policy managers responsible for revisiting or taking another look at the changing landscape, then we certainly have the ability to do that. But I take the point, and I think it's an important point, that if we're designing a system today, policies for a system, that will be built and operationalized and will cost resources to operate -- you know, design, operate, manage, and potentially change down the road, that that should be something that's factored into the consideration.

And so I hope that provides a little context in terms of where we are today, what the roles of the GNSO Council in chartering this work is, and that we have the ability to evolve that work as needed.

But I really do appreciate the question, and I think that was an important point.

Next in queue right over here, and then we'll come back to this side.

GREG MOUNIER: Thank you, my name is Greg Mounier. I'm working for Europol, and I'm a member of the Public Safety Working Group.

First of all, I wanted to say that we're very grateful for the work and dedication of the members of the EPDP team. I mean, the time and effort you're spending into this process is really amazing, and we're really hopeful that at the end we come up with a system which balance the interest of everyone and come up with transparency, accountability for (indiscernible) system.

My point is really related to the first point on that slide. In the field of public safety work, most of the domains that we are looking into are registered with privacy and proxy services, and for good reason; because people who have registered those domains with bad intentions want to hide their traces. So that's fair enough.

I've heard as well that globally about 30% of the domains registered today are actually registered with privacy and proxy services. And I'm

looking at our friends from the contracted parties to confirm that type of figures.

But I think it is a pity that 30% of the domains globally are somehow excluded from the system that you come up with, because the decision to disclose is already made by the contracted parties. Because you pay an additional fee, you're not going to -- the contracted parties are not going to release information on those domains. And I think it's a pity that it's excluded from the scope of this system, even though it might balance all the interests.

I don't know if you have any comment on this.

Thank you.

KEITH DRAZEK: Okay. Thank you very much, Gregory. I do not have a response to that at this time, but I am happy to take it offline and follow up. I don't know if anybody else would like to comment on the privacy/proxy service or privacy/proxy registrations at this point. But your point's well taken.

Okay. Thank you.

Okay. Next in line.

GG LEVINE: I'm Gg Levine with the National Association of Boards of Pharmacy and the .PHARMACY registry, and my question is concerning the distinction between natural and corporate persons as discussed in the GDPR. And

I'm just wondering what the discussions have been in the in the EPDP on that distinction.

KEITH DRAZEK: Thank you very much for the question. I think in EPDP Phase 1, the decision at that time, particularly in light of the time crunch if you will, the deadlines that we were facing, externally imposed deadlines, the decision at that time was made to not draw a distinction as it relates to the implementation of the temporary specification in the new policy recommendations. But I would defer to Janis on the question as it relates to ongoing discussions in Phase 2.

So, Janis, the question, natural versus legal.

JANIS KARKLINS: Yeah. This is one of the outstanding questions that falls with the priority 2 bucket. We had, on Saturday, the conversation that ICANN org in terms of reference for the study which was recommended by the Phase 1. The team members provided input to sort of draft terms of reference.

Our understanding is that the study will be made and results may be available, something between three to nine months from now. So depending when -- when these results will be brought to attention of the team, we will be continuing more informed discussion on the topic. And so hopefully we'll come with some kind of recommendations.

I sense that in team, there is divergence of opinions -- or variety of opinions on the topic. And so the study may well inform our conversation.

So -- But that is on the agenda.

KEITH DRAZEK: Okay. Thank you, Janis. And thanks for the question.

I don't want to lose the previous question about the privacy/proxy, and I would like to -- I'm actually curious, because I don't know the answer, if that's a subject that will be discussed or is that a priority 2 item in the Phase 2?

JANIS KARKLINS: No, this is a priority 2 item and is on our agenda as a priority 2.

KEITH DRAZEK: Thank you, Janis. So the clarification there is still a subject for discussion around the privacy/proxy question in the Phase 2 work. priority 2.

Thank you for that clarification.

Chris, over to you.

CHRIS DISSPAIN: Thank you, Keith. Good morning, everybody. Chris Disspain.

What I'm about to say is entirely a personal view and it goes back to the meta question that John asked and acknowledges completely what you're saying about the role of the CPDP. But we do have a situation where governments around the world are creating privacy legislation, and we have a situation where some of that, not all of it but some of it attempts to be extraterritorial and say it's not just within our borders but outside of our borders, and so on, and that's creating major challenges. And we also have a situation where we're -- we're tasked at the moment with doing the work that you've described.

I wonder whether, in parallel to that, we, as a community, shouldn't start thinking about approaching this problem in a slightly different way and actually come to consensus or try to come to consensus on what WHOIS is about, what it's for, and why we need it, what the benefits are. And then instead of creating a system that simply complies with one particular law, we create -- we create a possible policy that says everyone should do this, and then go get our government parts of the community to go to their governments and say write whatever WHOIS laws -- whatever privacy laws you like, but when you do so, in respect to data that is produced on the Internet about who owns domain names, please do it this way. Because not a single one of these governments, I imagine, has WHOIS at the top their list of reasons why they are writing GDPR.

So just a thought that we might want to think about in addition to what we're already doing -- and I have no doubt Goran has something to say about this -- in addition to what we're already doing, actually lifting the

discussion to a higher level and talking about trying to persuade people globally of the importance of the data and how it should be dealt with.

Thanks.

[Applause]

KEITH DRAZEK: Thank you, Chris, and thanks for that comment. And again, sort of what you suggested is outside the scope of this current effort in terms of the team, but I think very important question to be -- to be posed.

Goran, please.

GORAN MARBY: I just want to say I agree with Chris.

Thank you, Chris.

KEITH DRAZEK: Thank you. Thank you, Goran. Thank you, Chris.

Tijani, please.

TIJANI BEN JEMAA: Thank you very much. Tijani speaking from Iraq, but I am speaking on my own behalf.

Thank you very much for all the work you did for Phase 1 and 2. We are doing now for Phase 2. I know it is a lot of amount of time and energy, so thank you.

I have a question for you. In your understanding, who will be the data controller for the registrant data? And who will bear the GDPR fines in case of violation of this regulation?

And more importantly for me and I think for all of us, what will be the role and responsibilities of ICANN?

Thank you.

KEITH DRAZEK: Thank you very much, Tijani. I think those are excellent questions. And I think we have not yet come to a conclusion.

Janis says he has an answer. He's bailing me out. Thank you.

JANIS KARKLINS: Yeah, my answer is I will answer your question the moment the final report will be released.

KEITH DRAZEK: Yeah, thank you, Janis. And thank you, Tijani.

I think these are the open questions. The roles and responsibilities of the various parties involved in this, the definitions of controllership

versus processing or joint controllership, these are the questions of the day.

The EPDP team is working towards developing policies that, in many ways, are dependent upon those answers. And I think that's something that the sooner we, as a community, working with ICANN org and the Board can make some determination there, it would very much help the development of the policy work itself. But it's a question that -- and I'm not a GDPR expert and I'm not a lawyer, but there are questions as to whether there is the ability to share or transfer liability from contracted parties, and specifically registrars, as the closest entity to their customer to third parties, including ICANN as an organization. There are questions about who plays a role in terms of an accrediting body for, you know, if there is going to be a system where you're giving accredited access to certain users, whether you call them trusted notifiers or interested parties who have established their credentials in a trust. There are real questions about, you know, who has what role and who performs those roles. And I think ICANN org is definitely in there somewhere, but it's yet to be determined where and how.

TIJANI BEN JEMAA: Thank you. It's not only about access. It's also about collection of data. It's also about processing the data.

So you are -- you are focused on the SSID. This is very important, but there is also a lot of issues about the collection of the data and processing of the data.

Thank you.

KEITH DRAZEK: Thank you, Tijani. Agreed wholeheartedly.

Next.

PEARSE O'DONOHUE: Hi, good morning. Thank you. My name is Pearse O'Donohue. Member of the GAC, but speaking of behalf of the European Commission.

First of all, Ambassador Karklins, Janis, thank you very much for all the hard work you're doing with the team. And I have to say already that the preliminary recommendations, although they be in draft form, are certainly which the European Commission can fully get behind in terms of the direction that you are taking in Phase 2. So we're really looking forward to an expedited result to that work.

Secondly, in relation to the elements that Elana presented to us from the Strawberry Team, there's just one element where we have a very large question mark and that's in relation to the idea that we may use this unified access model as the return path for the data to be given to the requestor in the sense that there would be a determination at the level of the central portal or gateway as to whether or not that data should, in fact, be transmitted, which would require the collection and processing of the data by the access model. And that actually renders everything even more complex under the GDPR. It would not, at the same time, remove the liability of the data controller, which is the

registrar or the registry. So we would have a question as to whether it is actually worth that added complexity and this added liability, which will actually fall onto ICANN as well as the liability which will continue to apply to the data controller, the other data controller.

But now, having said that, we're not going to anticipate nor does the European Commission in any way influence the position of the European Data Protection Board, so we're happy that that proposal has now been suggested to them, and we will, of course, try to help them speed up their deliberation with regard to that submission. But it is one issue in which we in the European Commission have a significant concern.

There was a question raised about Article XXII with regard to automated processing. I'd just like to point out that that has to be taken in the context of the negotiations of the GDPR, and it's particularly important to note that under that article with regard to automated processing, there are already exceptions, particularly if the data controller is subject to European law or to the law of a member state. So it is not to -- do not assume that there is an automatic interdiction against automated processing. If it is due process, it can, within limited, be considered.

But I actually wanted to come to the wide scope of so many things that have been said already by other participants from the floor which is about the GDPR itself.

I think because it's been spoken about so much, most people understand what its objective is. The GDPR was not, though many of

you may not believe it, did not and was not designed to have other extraterritorial effect in the way that certain other regions of the world framed their legislation, but it clearly does when it relates to the personal data of a European data subject or, and let me be very clear about this, about the data of any individual, no matter where they come from in the world, in that data is stored or processed in the European Union. It applies to all personal data.

So there is some limitation to the scope, but I'd like to turn the conversation around for a moment and say isn't it great that other countries and regions of the world are now having a serious discussion about increasing and improving the level of data privacy. So we're actually quite proud in Europe of having the GDPR as a benchmark. Maybe somebody can improve on it further. That would be great, too. But I do, in that context, nevertheless, fully accept and actually support what has been said and was even said to the GAC yesterday by a representative of the GNSO, which is that this EPDP work and generally the work that's being done in ICANN is not about redesigning or creating another data protection law. It's about simply protecting privacy while, at the same time, ensuring that insofar as it is required, that ICANN and its contracted parties can conform with the GDPR.

So we should look at the positives of this whole discussion and hopefully learn from the GDPR, perhaps learn from some of the mistakes that have been made, but don't in any way assume that there is a negative a priori that anything that is proposed will be attacked simply because it comes from outside of the European Union. That is not the case.

So my final message, I'm sorry for taking so long, thank you very much for all of the work that has been done, and we look forward to a quick result to Phase 2.

Thank you.

KEITH DRAZEK: Thank you very much for that intervention. Very helpful, and we look forward to further engaging with you and others.

Goran wanted to get in briefly in response or in follow-up, and then we'll come back to the other side.

GORAN MARBY: It's a very interesting question the European Commission asked, and it's actually the question 4 we raised to the DPAs as well because we don't have the answer to it.

The other argument to use a more centralized model is actually for security, to make sure that the integrity of the questions goes the right way.

But we don't have the answer to it, and that's why we asked the question specifically to the DPAs.

Thank you very much.

KEITH DRAZEK: Thank you very much, Goran.

Okay. Next in line.

UNKNOWN SPEAKER: (Saying name) again for the record.

You used the term "joint data controller." Let me ground you and remove the hope for this term.

This term is not well defined. It's currently in discussion but the Data Protection Office in Europe, how it will be applied and what it means.

We had this problem at work. We have to work with such issues. And we had the interesting discussion with our data protection officers especially on this term. And they made -- better, they spoiled us with what is upcoming. Joint ownership or joint data controlling is not what it means, the technical terms. The term which mean two parties define the use of the data, and both has the interest in special parts of data use. It's not the case here.

The registries and registrars has no, no interest in publishing data like WHOIS. From their operational model, there is no need to do so. The only need to do so is from the contractual relationships with ICANN.

So the only party defining the use case and the requirements is ICANN. So the whole term "joint data controller" is not applicable for this. Data controllers are not organizations which are operating the technical environment. It's not the heuristical term. It's not -- the technical term of operating doesn't mean it's a heuristical operator. It only means who defines the words in the contract.

So please do not hope that you can go away and put other parties in. It will be your only sole responsibility for all the data if you have it in the contract and the other party can't put it out.

Thanks.

KEITH DRAZEK: Okay. Thank you very much for the comments. And I think -- if I understood you correctly, because, in your view, ICANN is the one setting the rules and making the requirements, that they are essentially the controller, then I think things would suddenly become much easier for us in our conversations, because I think that question of controllership processing, responsibilities and roles, and whether there is a joint controllership relationship or not is one of the things that is still unclear to the group and can certainly serve with clarification.

Okay. We have about ten minutes left. I'm glad to see people are still interested enough to come to the microphones. Please come up. If you want to contribute any questions or comments, please go ahead.

FRED FELMAN: Hi, I'm Fred Felman.

I'm speaking on my personal capacity. And I was thinking back on Chris's remarks, as well as others.

I think there was a lot of work done about the use of WHOIS and the WHOIS RT report in 2012. So we might actually want to think about going back to that and thinking about the uses of that data.

And it seems to me when I look at the work of the EPDP, that a lot of work actually has been done already in a lot of other places. In fact, there was a really excellent event hosted by Intanet (phonetic) yesterday, and where a lot of the processes where people were using in IDK and PIR and other places, dot U.K., to, one, collect this data, use the data, and update abuse.

So it seems to me that reinventing all of this work is maybe a waste of time. And we're 18 months into this. And as we try to develop policy, there are a lot of people who are being harmed in the interim. And we've seen increases in abuse. We've heard from IBM X-Force that blocking is being hindered by a lack of data being available.

So I'd just like to sort of step back and hear from you about how the EPDP will use some of the existing work to actually hasten this process so we may come to a solution more quickly.

KEITH DRAZEK: Okay. Thanks very much, Fred. And, you know, going back to my earlier comments, and Janis's reference to the need to act expeditiously and with urgency, it's certainly the GNSO Council in our chartering of this group for phase 1 and phase 2 recognized the impact on third-party users of nonpublic data, what is now nonpublic data. And there's definitely a recognition that we need to move as quickly as possible. But these are difficult and challenging issues. The EPDP Team right now in phase 2 is on track to deliver its report soon, with a goal of wrapping this up in -- ideally, in May.

I take your point that there are -- there's the view that negative impacts are happening and the lack of access to that data is hindering various groups and people in their work. And we, I think, acknowledged that in the chartering of this group. And we're doing what we can to get this thing moved forward.

I don't know if, Janis, you want to add anything to that.

Okay. Thank you.

Okay. Next in line. Thank you.

NICK WENBAN-SMITH: Hi, everyone. It's Nick Wenban-Smith, Nominet U.K. I'm a data protection officer, and I'm general counsel for the company.

We obviously operate the country code. We have some gTLDs as well for geo-specific regions.

So in the absence of a sort of consensus policy, each registry operator and registrar has had to come up with their own disclosure processes, so there's a patchwork quilt.

And I've got a sort of -- quite a specific question, and it relates to operation, but also risk, because what tends to resort in problems under data protection law is complaints from people's data and the way that's being used. And a lot of people don't really know about the WHOIS. But what our policy is, is when we do disclose people's data, when it is for legitimate purposes being expressed, is we notify the data subject, we notified the registrant that their data is being disclosed.

And that does prompt some complaints. But we think it's the fair and transparent thing to do and we're happy to do it and happy to take on the risk of having the complaints.

And I wondered whether the solutions that you're looking towards would also incorporate such a transparency measure and how that would work and that sort of question. I wonder whether you've gotten into that detail yet.

KEITH DRAZEK: Thank you, Nick.

Janis, I'll hand that one off to you.

JANIS KARKLINS: Yeah, that is under consideration. I cannot give you more details. For the moment, there is no final sort of proposal on the table. But, yes, this is under consideration.

And maybe I can use this opportunity maybe to provide a more clear answer on privacy proxy question.

So I got help in this. And I would say that the disclosure of privacy proxy information has been subject of different PDP, which is currently in implementation. So we need to wait until this implementation is finalized. So the EPDP team in phase 1 already recommended that the privacy proxy registration should be labeled as such in RDAP so that requestor can immediately go to privacy proxy provider instead of going to SSAD and receive information of the privacy proxy provider.

KEITH DRAZEK: Thank you, Janis, for that clarification. Very helpful.

Next in line. We have about four minutes left. Thank you.

UNKNOWN SPEAKER: Frank (saying name) with the Motion Picture Association.

I wanted to sort of kind of give a shoutout to the paper that was sent to the European protection board called the Strawberry Project paper, because I think it would -- I think it's probably going to help the work of the EPDP by sort of clarifying the legal framework around one of the options that was under consideration, kind of solve the chicken and egg situation.

But also from the perspective of, you know, how implementable this system will be eventually. Right now, we have a completely decentralized system that requires every single contracted party out there to have one or more lawyers to process requests, et cetera, create a lot of delays, but a lot of sort of cost for them. For the requestors, a lot of delays as well. A lot of uncertainty. And generally, right now, an incredibly low rate of response to the requests.

So we're very hopeful that quickly, also positively, the European Data Protection Board can provide that kind of guidance that clarifies that, you know, that sort of easier-to-implement, faster, more effective, efficient system can be considered by EPDP.

KEITH DRAZEK: Okay. Thank you very much.

Elena, would you like to respond? Any follow-up on that? I think it was just a recognition that there's hope that the work that you've been doing and that ICANN org has been doing with the Commission and with the Data Protection Board will bear fruit and be productive.

ELENA PLEXIDA: Yes. Thank you.

There were similar interventions by other people today asking what will be the role in the responsibilities of the different actors that we put in place, exactly what we will tie to this paper to ask. Because it's not a clear thing. It's not as easy. And, hopefully, the answer will inform the EPDP as they're considering their options.

Now, whether what we are proposing is feasible, that remains to be seen. It's not straightforward. If it was, we wouldn't be asking the questions. Thank you.

KEITH DRAZEK: Thank you very much. And I think it's important to note here that the work that Elena and her team have been working on with the Commission and the Data Protection Board is meant to inform the work of the EPDP and the bottom-up consensus policy development work that's taking place within this community. So it will be an input to be considered by the EPDP Team, and ideally, we'll get that information sooner rather than later.

So thank you for that.

We are just about out of time. I don't see any additional hands or people at the mic.

Wait a minute. I've got one more, two more. Do we have any remote participation?

Okay. Thank you very much.

Okay. Over to you, Bradley.

BRADLEY SILVER: Hi. Bradley Silver. I'm P counsel for WarnerMedia.

Follow up on questions between potential conflicts between WHOIS policy and other data protection laws.

Obviously, there is a long-standing consensus policy and procedure to deal with conflicts between WHOIS policy and WHOIS obligations and national data protection laws that's been conspicuously absent from discussions over the last few years, because we've been focused on going in another direction.

And I guess my question for those on the panel and potentially more broadly is, how relevant is that long-standing consensus policy and procedure still, given the direction that ICANN has taken in radically revising WHOIS policy in relation to the GDPR, given that it is likely that there will be and has long been contemplated other data protection laws that will conflict with existing WHOIS policy and obligations?

KEITH DRAZEK: Thanks very much, Bradley. That's a great question. I'm afraid I don't have an answer that I'm confident in at the moment to respond at this time. But I think that's one that we can absolutely take offline and come back to you with.

And I don't know if anybody else has a thought on that one or not.

But I think your point's relevant. I mean, to the extent that there's an existing policy that talks about what you do and how do you approach conflicts with -- you know, between the WHOIS obligations and with national laws, I think it's certainly relevant. And we'll take a look at that. And certainly we would look at that at the GNSO Council level. So I'll commit to getting back to you with an answer on that one.

Okay. Thanks.

Okay. Next in line and last before we wrap up. Thank you.

UNKNOWN SPEAKER: I have only just a comment about observer.

As an observer, I have -- I have proved a lot of difficulty. And the phase 2 of the EPDP says I'm not able to join in the work directly, I have only to see this offline.

As a concern, could you please influence the EPDP to give out this opportunity for this last -- this remaining period of EPDP online.

Thank you.

KEITH DRAZEK: Okay. Thanks very much. And I'll be corrected here if I'm wrong, but there is the ability for anybody in the community to actually listen to the meetings and to follow the meetings of the EPDP Team. So there is actually the ability for you to audio cast, to listen and to observe through the audio cast the ability.

And we'd be happy to make sure that that gets publicized and circulated so everybody's aware. And we certainly welcome anybody that wants to observe the work of this group.

And just to be clear, this group was chartered in a very tight frame with very specific responsibilities. And we as the GNSO Council chartered it, essentially, to be a representative model, so the members of the group who participate and contribute directly are representing other parts of the ICANN community and all parts of the ICANN community. So there is a representative structure. If you, through your respective organizations, want to contribute, then, typically, you would do so through your group structures and through the members that your structures have appointed. And we certainly welcome that.

So with that we are over time. I think we need to wrap up. Any final questions, comments from the panelists?

JANIS KARKLINS: No, just confirmation answering the last question. All EPDP Team meetings are live streamed, audio cast. And after the meeting, literally, within an hour, the audio recording is -- the link to the audio recording

is published and everyone can download it. There are no limitations in that respect.

UNKNOWN SPEAKER: But the quality of the sound live streaming is not always good. So I approve really -- I mentioned this to the ICANN staff for several times. So it's -- if it is possible to create, as we did it in the phase 1, a second room in which -- with Zoom, in which you could follow the -- But with the sound live, believe me when I say that there is a lot of difficulty to follow.

KEITH DRAZEK: Okay. Thank you for the comment.

Sorry. Thank you for the comment. And I'll take an action item to work with staff on exploring how to improve the sound quality. I think there's a technical challenge since we moved from Adobe Connect to Zoom and the inability to have two rooms going parallel in Zoom. I'll look into it.

Thanks, everybody, very much appreciate you joining. Thank you for the input and engagement. This won't be the last time that we do this.

Thank you very much to the EPDP Team and staff for everything that you've done to get us to this point. And we look forward to seeing an initial report in the future.

Thanks, all.

[END OF TRANSCRIPTION]